|  |
| --- |
| **Технологии M2М** позволяют собрать и обработать информацию с удаленных объектов и систем (различные проводные и беспроводные датчики) в единый агрегированный поток.  **РАСШИРЕННЫЙ ПРОФИЛЬ** |

1. **ОПИСАНИЕ**

М2М – это сокращение от «machine-to-machine», т.е. «машина-машине». M2М-технология позволяет объединить удаленные объекты и системы для автоматизации бизнес-процессов.

Именно с помощью **М2М-техонологий** наша жизнь становится проще. Сфера применения М2М-техонологий весьма широка. Эта технология настолько прочно вошла в нашу жизнь, что мы уже не мыслим комфортное цивилизованное существование без нее. Платежные терминалы, банкоматы, системы безопасности и контроля, мониторинг транспортных средств и многое другое. Все это работает именно благодаря М2М-технологиям.

Говоря о М2М-технологиях, мы подразумеваем в первую очередь именно беспроводной способ передачи данных. Но M2M широко применяется и для проводных коммуникаций.

Использование **беспроводных М2М-технологий** дешево и технологично. Они позволяют не тратить средства на прокладку кабельной инфраструктуры, сохраняют время и позволяют свести к минимуму человеческие ресурсы. М2М с использованием беспроводных коммуникаций широко распространено на самом высоком уровне: это и безопасность границ, государственные службы спасения и правоохранительные структуры. Беспроводные M2M-технологии позволяют обеспечить быструю реакцию из коммуникационного центра. Также M2M позволяет следить за мобильными объектами - например за передвижением транспорта, нахождением товаров на складе, узнавать о состоянии торгового автомата. Кроме того, беспроводные М2М-технологии с помощью датчиков позволяют следить за механическим напряжением высотных зданий и мостов и многое другое.

**Области применения М2М-технологий**

**М2М-технологии для интернета.** Это наиболее востребованная на сегодня область применения М2М. Практически у каждого в доме есть модем, обеспечивающий связь wi-fi.

**М2М-технологии для автомобилей.** Службы такси и компании, занимающиеся перевозками, массово покупают GPS-трекеры и устанавливают их на свой автопарк. Это устройство помогает рободиспетчеру знать точное местоположение и скорость автомобиля. Это в разы повышает эффективность транспорта.

**М2М-технологии для дома.** С помощью М2М можно удаленно контролировать температуру в доме и обеспечивать его безопасность. Также с помощью М2М-технологий можно контролировать электрическое оборудование в доме. Достаточно отправить смс.

**М2М-технологии для ЖКХ.**Сегодня мы записываем показания счетчиков воды и электричества и подаем эти показания в соответствующие организации. В будущем эти показания будут считываться автоматически и дистанционно. Возможно к этому процессу подключится и банк – денежные средства будут списываться автоматически.

**М2М-технологии для здоровья.**Датчики М2М могут следить за температурой человека, его давлением и пульсом. Также можно узнать местоположение больного. Все это позволяет вовремя принять меры и выслать при необходимости помощь.

**М2М-технологии для автоматизированного учета.**На любом товаре, находящемся на складе, есть электронно читаемая наклейка. Просканировав товар, можно следить за движением товара и остатками. Управление складом с помощью М2М-технологий может быть полностью автоматизировано.

**М2М-технологии для безопасности.** Покинув дачу или собственную квартиру, вы можете с помощью камеры дистанционно следить за безопасностью помещения. При обнаружении движения, датчики немедленно отправят вам смс или ммс с картинкой происходящего.

**М2М-технологии для торговых автоматов.**Оборудование М2М позволяет дистанционно контролировать кофейные автоматы, платежные терминалы, банковские автоматы, охранять это вендинговое оборудование, осуществлять контроль за работоспособностью.

### Способы реализации М2М решений

### **DTMF** - позволяет посылать кодированные сообщения, используя обычные голосовые каналы. Это может эффективно использоваться для нужд охраны (DTMF форматы передачи информации, например, Contact ID), простого дистанционного управления, для контроля за персональной информацией, например, в голосовой почте. Обычно, автоответчик запрашивает пароль для допуска в меню. Это основная М2М возможность, которая используется в большинстве сетей.

### **SMS** - сервис коротких сообщений. Там, где операторы сотовой связи предоставляют этот сервис, для пользователей М2М технологий открываются огромные возможности. Главное преимущество SMS - это то, что сообщение может быть передано за миллисекунды и содержать большое количество информации. SMS открывает возможности для большинства фиксированных и мобильных М2М приложений, таких как автоматы розничной торговли, платежные терминалы, коммунальное хозяйство и др.

### **DATA и "Always on" DATA - модемная связь.**Использование коммутируемых каналов для передачи информации ограничена низкой, по сравнению с выделенными каналами "Always on" DATA, скоростью передачи информации. Системы передачи пакетной информации GPRS или CDPD уже доступны и позволяют осуществлять интерактивные коммуникации в реальном времени. "Always on" DATA является ключевым ориентиром в развитии М2М. С развитием GPRS и CDPD стали возможными телемедицина и развлечения.

### **WAP-IP** предназначены для решений человек-машина (man-to-machine), и начинают становиться обычными для электронных заказов, покупок и платежей, объединяя в себе информационный сервис и приложения по управлению и мониторингу. Для автоматов розничной торговли WAP-IP сеть могла бы подготовить платформу для развития охранных и антивандальных систем.

### **3G.**Третье поколение сотовой связи обеспечивает неограниченные возможности в телекоммуникационной среде, когда все машины и оборудование для построения сетей соответствует одному и тому же протоколу.

Технологии 2G/3G/4G сделали возможным появление Интернета Вещей, однако 5G даст старт «тактильному» интернету, состоящему, по сути, из сети датчиков и устройств. Сферами применения таких беспроводных инновационных технологий станут автоматизация производства, управление процессами и робототехникой. Сегодня мы уже видим работу промышленных WiFi сетей, которые используются в самых различных приложениях. Однако уменьшение времени задержки и беспроводные технологии с высокой пропускной способностью могут революционно изменить процесс производства, обеспечив устойчивую беспроводную связь, которая необходима для объединения машин в рамках широкого спектра приложений.

Области применения технологий М2М

В России в настоящее время более 40% sim-карт, при реализации технологии М2М, установлено на транспортных средствах.

Разработке и внедрению данной технологии в транспортную сеть, во многом поспособствовала Федеральная

целевая программа «Развитие транспортной системы России (2010-2020 годы)».

Области применения технологий М2М представлены на рисунке 1.

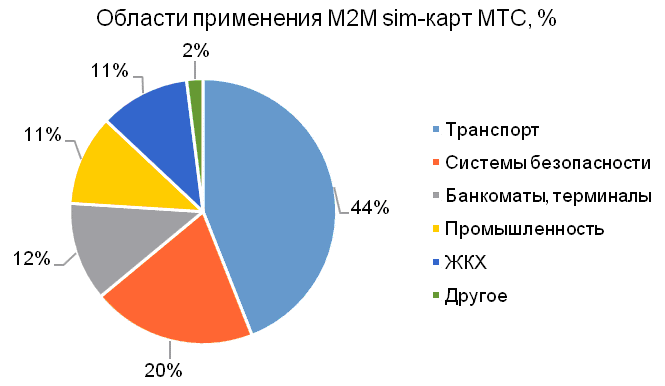


Рис. 1 – Области применения технологий М2М

Мониторинг транспорта

Основные направления применения ─ мониторинг движения и состояния автомобиля (fleet management), общественного транспорта, систем сигнализации.

На предприятиях промышленного сектора число sim-карт МТС выросло на 55 тысяч до 396 тысяч (доля 11%). Наиболее востребованы М2М-сервисы МТС у предприятий нефтегазовой отрасли и энергетики, которым необходимо наладить надежную бесперебойную связь с месторождениями в труднодоступных местах и отдалёнными филиалами.

Число телематических sim-карт МТС в ЖКХ (учет потребления воды, тепла, света в жилых помещениях, установка в лифтах и домофонах) увеличилось на 55 тысяч до 396 тысяч.

Динамика использования М2М sim-карт МТС по отраслям, % представлена на рисунке 2.

В течение нескольких лет большая часть m2m-устройств будет использовать сети на базе 2G и 3G, так как m2m-решения, применяемые сегодня в развивающихся сегментах, таких как ЖКХ, «умного страхования», потребительская электроника, не требуют высоких скоростей. Технологии сетей LTE активно развиваются и в будущем будут применимы ко всем m2m/IoT – сегментам.

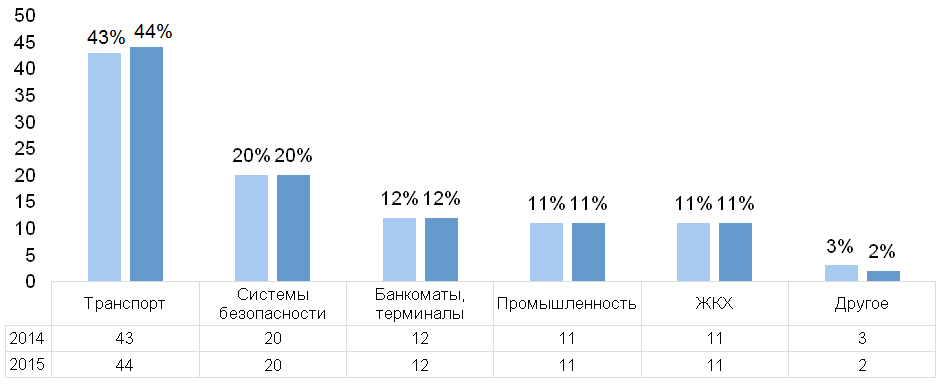


Рис. 2 – Динамика использования М2М sim-карт МТС по отраслям, %

Структура сети

Взаимодействие основных функциональных модулей базовой сети М2М, платформы IMS, интерфейсов сети М2М (mla,mld) и внутренних интерфейсов (ISC,Gm) базовой сети М2М, а также устройств М2М/М2М-шлюзов показано на рисунке 3.

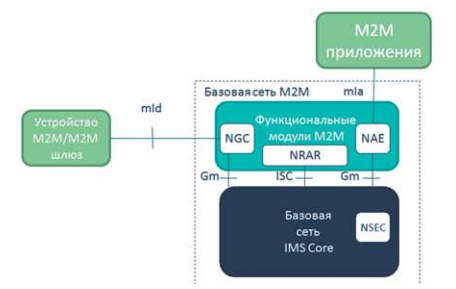


Рис. 3 – Взаимодействие основных функциональных модулей базовой сети М2М

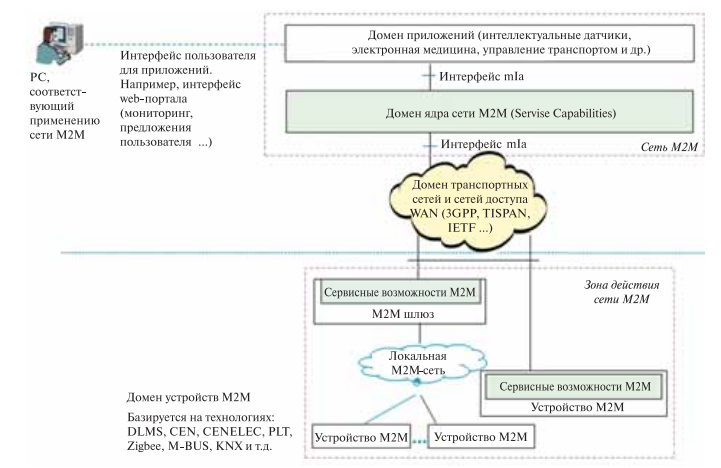
Интерфейсы mIa, dIa, mId сети М2М на основе принципов открытых интерфейсов обеспечивают взаимодействие между доменом приложений и базовой сетью М2М, между прикладным и функциональным уровнем домена устройств М2М, между устройствами М2М и шлюзом М2М соответственно. Типовая функциональная архитектура и интерфейсы сети М2М показаны на рис. 4. 

Рис. 4 – Типовая функциональная архитектура и интерфейсы сети М2М

Интерфейс mIa сети М2М обеспечивает взаимодействие приложения M2M с функциональными модулями сети M2M или домена приложений.

Интерфейс dIa сети М2М обеспечивает взаимодействие приложения M2M, активированного в M2M-устройстве, и доступ к функциональным модулям этого M2M-устройства или M2M-шлюза, а также взаимодействие приложения M2M, активированного в M2M-шлюзе, и иметь доступ к функциональным модулям этого M2M-шлюза.

Интерфейс mId сети М2М обеспечивает взаимодействие M2M-устройства или M2M-шлюза с модулями основных функций M2M в сети и доменом приложений. Интерфейс mId использует функции присоединения базовой сети в качестве своего базового уровня.

Сервисные функциональные характеристики базовой сети М2М реализуются в виде соответствующих функциональных модулей, которые определены стандартом ETSI на функциональную архитектуру сети М2М.

Наиболее важными функциональными модулями, обеспечивающими возможности управления сетью М2М, реализация которых требуется в базовой сети М2М на платформе IMS, являются модули NAE, NGC, NRAR и NSEC.

Интерфейс ISC сети М2М обеспечивает обмен данными, присоединение сервера приложений и доступ к услугам M2M, а также доступ к информации и использование функциональных возможностей базовой сети IMS Core.

Интерфейс Gm сети М2М, выполняющий аутентификацию и авторизацию различных приложений M2M-устройств, а также сетевых приложений, используется для реализации ряда функций базовой сети M2M. Он связан также с базовой сетью IMS через ISC- интерфейс в целях обмена информацией с приложениями M2M-устройств через модуль NGC. Обмен информацией базовой сети M2M SC с сетевыми приложениями осуществляется через модуль NAE.

Модуль NAE (Network Application Enablement) обеспечивает взаимодействие приложений M2M на уровне сетевого домена и домена приложений М2М, а также:

- открывает доступ приложений М2М к функциональным модулям базовой сети М2М по интерфейсу mIa;

- обеспечивает скрытность топологии функциональных модулей SC и адресов NAE, выдавая только необходимую для работы приложений М2М;

- обеспечивает регистрацию приложений М2М в соответствующих функциональных модулях SC;

- обеспечивает аутентификацию и авторизацию приложений М2М через модуль безопасности, а также проверяет наличие соглашения у провайдера приложений М2М и его уровень взаимодействия с функциональными модулями SC;

- проверяет через интерфейс mIa возможности применения функциональных модулей SC и выдает отчет об ошибке при невозможности маршрутизации к другим функциональным модулям.

В дополнение к своим главным функциям модуль NAE обеспечивает межсетевое взаимодействие базовой сети IMS Сore через интерфейс Gm для авторизации и аутентификации только сетевых приложений. Кроме того, использование интерфейса Gm предполагается для поддержки файловой системы FFS.

Модуль NGC (Network Generic Communication) обеспечивает установление транспортных сессий и их последовательное прекращение в случае неподтверждения установленных ключей безопасности. Установление ключей безопасности осуществляется модулем безопасности NSEC и используется для формирования ключей конкретной сессии.

Типовая сессия на уровне приложений между M2M-устройством/ M2M-шлюзом и модулем NGC базируется на протоколе HTTP. В некоторых случаях сессия с данными о безопасности (Secure Data Session) может базироваться на протоколе TLS-PSK.

Кроме того, модуль NGC:

- обеспечивает шифрование/интегральную защиту данных для устройств M2M и M2M-шлюзов;

- устанавливает туннели безопасности сессий от M2M-шлюзов и M2M-устройств, если приложение требует установления туннеля безопасности (например, туннель между домовым шлюзом и одним из функциональных модулей);

- предоставляет средства для транспортировки сообщений между следующими элементами сети М2М: устройствами M2M, шлюзами M2M, функциональными модулями базовой сети М2М, приложениями M2M, входящими в сетевой домен и домен приложений; идентифицирует всех адресатов, передающих сообщения модулю NGC, на основе использования индивидуальных уникальных идентификаторов.

В дополнение к своим главным функциям модуль NGC обеспечивает функцию услуг присоединения при межсетевом взаимодействии базовой сети IMS Сore через интерфейс Gm. В этом случае он работает как устройство разрешения доступа.

Весь обмен между приложениями M2M-устройств и базовой сетью M2M SC осуществляется через модуль NGC.

Модуль NRAR (Network Reachability, Addressing and Repository) входит в состав домена сервис-провайдера услуг М2М и обеспечивает:

установление соответствия между именами M2M-устройства или M2M-шлюза или группы M2M-устройств/M2M-шлюзов и установление сетевых адресов маршрутизации устройств M2M или M2M-шлюзов;

установление статуса достижимости для присоединения устройств M2M или M2M-шлюзов;

получение запросов от других функциональных модулей и уведомление о доступности устройства M2M или получении им нового адреса (как следствие его мобильности), изменение совокупности приложений для устройств M2M согласно регистрируемой информации;

получение другими модулями базовой сети М2М адресных материалов и статусов достижимости для присоединения устройств M2M или M2M- шлюзов;

создание групп M2M-устройств, стирание и составление списков устройств M2M и M2M-шлюзов, входящих в соответствующие группы.

Модуль NRAR в дополнение к своим главным функциям обеспечивает функцию маршрутизации в сети M2M для поддержки межсетевого взаимодействия IMS Сore посредством интерфейса ISC.

Модуль NSEC (Network Security) обеспечивает безопасность сети М2М на уровне сетевого домена и домена приложений и выполняет:

регистрацию устройств M2M на уровне сервисов через аутентификацию ключей об обслуживании на основе соглашений;

управление обменом ключами обслуживания между устройствами M2M/M2M-шлюзами и модулем NSEC;

аутентификацию приложений до предоставления ими услуг;

взаимодействие M2M-сервера аутентификации (MAS) для получения данных об аутентификации, необходимых для выполнения аутентификации устройств M2M или M2M-шлюзов и управления ключами обслуживания.

Взаимодействие устройств М2М может происходить как с использованием, так и без использования базовой сети М2М и шлюзов М2М.

В первом случае абонентское устройство сети М2М представляет собой также точку взаимодействия интерфейса mId домена M2M-устройств, соединяющего M2M- устройство/M2M-шлюз и базовую сеть М2М.

Во втором случае абонентское устройство сети М2М представляет собой также точку взаимодействия интерфейса mIa домена M2M-устройств между приложениями и функциональными модулями, поддерживающими основные функции сети М2М на местном уровне. Интерфейс mIa в этом случае используется также для взаимодействия с локальной сетью устройств М2М.

Каждая услуга M2M идентифицируется в базовой сети М2М, построенной на основе платформы IMS, при помощи идентификатора IMS-услуг (ICSI). Приложения M2M домена приложений и приложения устройств M2M идентифицируются на основе идентификаторов IMS-приложений (IARI). Для опознавания и регистрации устройства М2М в базовой сети M2M оно должно быть конфигурировано при помощи одного идентификатора частного пользователя (Private User Identity – IMPI) и одного идентификатора общественного пользователя (Public User Identity – IMPU), который определяет индивидуальный сетевой номер устройства М2М (ID).

Идентификатор IMPU используется для идентификации информации, поступающей от устройства М2М (например, данные аутентификации) и сохраняемой в подсистеме IMS Core базовой сети.

Идентификатор IMPU используется также базовой сетью M2M SC для запросов при присоединении и взаимодействии с устройством М2М.

Базовая сеть M2M использует подсистему IMS для регистрации сетевых приложений. Для этого базовая сеть M2M поддерживает взаимосвязи между модулями приложений M2M (используя их для приложений M2M). При этом каждому модулю присваиваются свой идентификатор IMPI для идентификации и идентификатор IARI для обеспечения взаимосвязи между модулями соответственно. Кроме того, каждому сетевому приложению, чтобы быть зарегистрированным в подсистеме IMS Сore, должен быть назначен идентификатор IMPU, а функциональные модули базовой сети M2M поддерживают взаимосвязь между индивидуальным номером ID приложения M2M, его идентификатором IARI и назначенными ему идентификаторами IMPI и IMPU.

Идентификатор IMPU приложения M2M используется функциональным модулем NGC для формирования запросов на присоединение к соответствующим приложениям M2M, так как модуль NGC обеспечивает хранение и установление взаимосвязей между приложениями услуг M2M, определяемых посредством приложений устройств M2M, и соответствующим идентификатором IMPU для целевых сетевых приложений M2M.

Стандартизация технологий М2М

Европейской комиссией были выпущены несколько директив и мандатов, стимулирующих его развитие.

В структуре главного европейского органа по стандартизации в области телекоммуникаций – Европейского института стандартизации электросвязи (ETSI) в 2009 г. был создан технический комитет ТК М2М, в сферу ответственности которого входят: сбор и спецификация требований к технологиям и услугам M2M; создание и поддержание работоспособности архитектуры высокого уровня «end-to-end» для сетей M2M; определение ниш в существующих стандартах ETSI, не охватывающих требования к сетям М2М, и разработка этих дополнений; обеспечение роли ТК М2М как главного центра экспертизы ETSI в области сетей и услуг M2M; координация деятельности ТК M2M и других технических комитетов ETSI.

1. **БИЗНЕС-ПОТЕНЦИАЛ**

С уверенностью можно утверждать о дальнейшем бурном темпе роста М2М-технологий в нашей стране в ближайшие годы. Прежде всего потому, что растет число отраслей, где применяется М2М. И этому немало способствуют кризисные явления в экономике, т.к. М2М-технологии позволяют сократить издержки.

1. **БАРЬЕРЫ**

Одним из направлений деятельности крупнейших операторов России может стать приобретение статуса сервис-провайдера услуг М2М. Наличие в сетевой инфраструктуре оператора платформы IMS позволит достаточно быстро и эффективно разворачивать сети М2М, управлять трафиком и обеспечивать нумерацию и адресацию устройств М2М на основе функциональных возможностей IMS. Однако несовершенство нормативной базы в области регулирования сетей и услуг М2М, многоуровневая система управления сетью в ЕСС России, ограниченность частотного ресурса, выделяемого для операторов связи, подключающих и создающих сети M2M-устройств, оказывают негативное влияние на рынок услуг М2М в России. Для преодоления факторов, сдерживающих развитие этого рынка, сегодня необходимо принятие ряда решений ГКРЧ РФ по нелицензионному использованию радиочастотного спектра, открывающему беспроводному М2М-оборудованию дорогу на российский рынок; создание нормативно-правовых актов по сертификации оборудования и построению сетей М2М; разработка Правил нумерации и адресации устройств М2М и Правил оказания услуг в сетях М2М.

1. **ЗНАЧИМОСТЬ ДЛЯ РАЗВИТИЯ БИЗНЕСА**

Сегодня М2М-технологии позволяют бизнесменам не тратить средства на прокладку кабельной инфраструктуры, сохраняют время и экономят человеческие ресурсы. Операторы предлагают своим бизнес-клиентам выгодные и удобные М2М-тарифы. Благодаря округлению трафика до одного килобайта стоимость обслуживания удаленных устройств сводится к минимуму, а простота подключения, качественный контроль работы оборудования и единая стоимость трафика на территории России делает использование сервиса выгодным и удобным.

Несомненно, М2М-технологии являются перспективными в плане долгосрочных вложений с большой окупаемостью и долговечностью.

1. **ИСТОЧНИКИ**

*1. Росляков, А.В., С.В. Ваняшин, Гребешков А.Ю.,* Интернет вещей:учебное пособие. - Самара: ПГУТИ, 2015. – 200 с.

*2. Тихвинский В.О.* Перспективы и мо- дели услуг в сетях M2M //Мир связи: Connect. ‒ 2011. ‒ № 11.

3. http://www.corp.mts.ru/telematika/services/manager\_m2m/