Интернет вещей:
видео, аудио, коммутация

Современный дом немыслим без электронной аппаратуры дистанционного облачного управления через беспроводную сеть. Настройка всей системы занимает считанные минуты, но безупречно работает годами, позволяя вам контролировать важные объекты за тысячи километров. Устройства, описанные в книге, предназначены для управления электрическими приборами через домашнюю или корпоративную Wi-Fi-сеть и используются в сети с общим названием интернет вещей (IoT). Примеры настройки электронных модулей описаны не только для Windows, но и для приложения Android.

Издание предназначено для широкого круга читателей.

ДМК издательство
www.дмк.рф

Интернет-магазин
www.dmkpress.com

Оптовая продажа:
КТК "Галактика"
books@alians-kniga.ru

ISBN 978-5-97060-761-9
9 785970 607619 >

ДМК издательство
ЛАНЬ

Антти Суомалайнен

Интернет вещей:
видео, аудио, коммутация

Антти Суомалайнен

Интернет вещей: видео, аудио, коммутация

ДМК Пресс
издательство
Москва, 2019

УДК 004.738, 004.62
ББК 32.973
С89

С89 Антти Суомалайнен
Интернет вещей: видео, аудио, коммутация. – М.: ДМК Пресс, 2019. – 120 с.

ISBN 978-5-97060-761-9

Современный дом и его обитатели немыслимы без электронной аппаратуры дистанционного облачного управления через беспроводную сеть. Большой дом можно сделать легко управляемым с помощью различных предложенных в книге решений. Настройка всей системы занимает считанные минуты, но безупречно работает годами, позволяя вам контролировать важные объекты за тысячи километров. Устройства, описанные в книге, предназначены для управления электрическими приборами через домашнюю или корпоративную Wi-Fi-сеть и используются в сети с общим названием интернет вещей. Примеры настройки электронных модулей описаны не только для Windows, но и для приложения Android.

Издание предназначено для широкого круга читателей.

УДК 004.738, 004.62
ББК 32.973

ISBN 978-5-97060-761-9

ОГЛАВЛЕНИЕ

Глава 1. Технологии, возможности и перспективы интернета вещей.... 5

1.1. Из истории интернета вещей.... 5
1.2. Технологии IoT.... 7
1.3. Примеры IoT.... 9
1.4. Перспективы для IoT.... 13
1.4.1. Особенности LPWAN.... 14
1.5. Перспективы разработки новых датчиков для IoT.... 15
1.6. Сравнение беспроводных технологий в интернете вещей.... 16
1.7. IoT-архитектура.... 18
1.8. Особенности тестирования IoT.... 20
1.8.1. Инструменты тестирования IoT.... 21
1.9. Облачные технологии беспроводной передачи данных.... 21
1.9.1. Передача файлов в системе интернета вещей.... 22
1.10. Особенности доступа к системе видеонаблюдения через P2P с разным оборудованием.... 25
1.10.1. Принципы подключения P2P-камер видеонаблюдения.... 27
1.10.2. Практическая настройка P2P-камеры.... 28
1.10.3. Особенности настройки Wi-Fi на конкретном оборудовании.... 28
1.11. Актуальные вопросы безопасности в системе интернета вещей.... 30
1.11.1. Протоколы разных стандартов безопасности сети.... 31
1.11.2. Дополнительные методы защиты пользовательской сети.... 32
1.11.3. Практические рекомендации.... 36
1.12. Распределение Wi-Fi-сигнала в системе интернета вещей.... 39
1.13. Особенности Wi-Fi-маршрутизаторов.... 42
1.13.1. Варианты выбора и технические характеристики оборудования.... 42
1.13.2. Минимальные современные требования к функционалу.... 43
1.14. Программная совместимость оборудования в интернете вещей.... 44
1.15. Легитимное использование интернета вещей в беспроводной сети.... 45

Глава 2. Видеокамеры и диктофоны в системе интернета вещей.... 49

2.1. Особенности разных моделей камер и диктофонов в системе интернета вещей.... 49
2.1.1. C11S мини-DVR-камера 1080P Full HD.... 49
2.2.2. Цифровой диктофон IDV Wi-Fi IP P2P HD Pen Recorder Mini Wi-Fi 1080P.... 52
2.1.3. Wi-Fi-диктофон Olympus DM-7.... 53
2.1.4. Wi-Fi-диктофон Olympus DM-901.... 56
2.1.5. Профессиональный цифровой диктофон Edic-mini Tiny B21.... 58

2.1.6. Диктофон с видеокамерой Fortune Fly FTX-360MC-23 69
2.1.6. Профессиональная DMT6-видеокамера, совмещенная с диктофоном 70
2.2. Видеокамеры P2P 74
2.2.1. IP P2P-камера VSTARCAM T6835WIP. Настройки и практическая работа 74
2.2.2. Настройка P2P-камеры 76
2.2.3. Общая информация по приложению IP Camera Super Client 79
2.2.4. Основные программные функции 85

Глава 3. Другие исполнительные устройства в системе интернета вещей 98
3.1. Особенности и возможности исполнительных устройств бытового назначения 98
3.1.1. Интересные вопросы безопасности 98
3.1.2. Варианты совершенствования безопасности системы интернета вещей 100
3.2. Практические модели управляемых электронных устройств в системе интернета вещей 101
3.2.1. Совместимость устройств 102
3.2.2. Принцип работы устройств 102
3.2.3. Как пользоваться? 102
3.2.4. Распространенные ошибки подключения 103
3.3. Совместимые электронные устройства 104
3.3.1. Беспроводная Wi-Fi-управляемая розетка Orvibo WiWo-S20 104
3.3.2. Беспроводная электронная розетка BePlug-15 105
3.3.3. Электронное устройство SWS-A1 109
3.3.4. Электронное устройство DSP-W215 111
3.4. Как практически можно пользоваться описанными устройствами 112

Литература 117
Справочный материал интернета 117

Глава 1

ТЕХНОЛОГИИ, ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ИНТЕРНЕТА ВЕЩЕЙ

В этой главе мы поговорим об истории возникновения, особенностях облачной технологии, возможностях и перспективах интернета вещей, а также о проблемах или сбоях, связываемых именно с этой технологией взаимодействия современных электронных устройств и передачей данных на расстоянии.

1.1. Из истории интернета вещей

Так или иначе, полезные модели (изобретения) всегда с чего-то начинаются, кем-то, пусть даже в непривычных и неусовершенствованных формах, разрабатываются и запускаются в серийное производство. Мало кому верится сейчас, но концепция популярного сегодня интернета вещей предугадана в начале XX века Николой Теслой. Известный физик и, как бы сказали сегодня, талантливый электроник предполагал свойства проникающих радиоволн в роли нейронов «большого мозга», управляющего различными окружающими человека предметами. По замыслу Теслы, инструменты контроля должны умещаться буквально в кармане повседневной одежды. Великий и проницательный изобретатель не был фантастом, он понимал то, что его современники не могли и представить.

Концепция интернета вещей базируется на принципе межмашинного общения: без вмешательства человека электронные устройства «общаются» между собой. Интернет вещей – это автоматизация, но более высокого уровня. В отличие от «умных» домов, узлы системы используют TCP/IP-протоколы для обмена данными через каналы глобальной сети интернет. Рассматриваемый метод коммуникации дает преимущество – возможность объединять системы между собой, строить «сеть сетей», что позволяет изменить бизнес-модели отраслей и даже экономики целых стран.

Спустя 100 лет после Теслы термин интернет вещей ввел в широкий оборот сотрудник исследовательского агентства при Массачусетском технологическом институте Кевин Эштон, предложивший увеличить эффективность логистических процессов без вмешательства человека в производстве: с помощью электронных (радио)датчиков с автономным питанием собирать информацию о наличии товаров на складах и отслеживать их движение к торговым точкам. Каждая метка отправляла в сеть данные о своем местонахождении в каждый момент времени. Использование RFID-меток ускорило реакцию поставщиков и ритейлеров на изменение спроса и предложения: товары не лежали на складе, а отправлялись туда, где они действительно необходимы. Эффект от введения маркировки оценили, и вскоре все поставщики торговой сети производили товары только с радиометками. В наши дни «интернет вещей не только меняет существующие правила, но и формирует новые правила экономики совместного использования» (shared economy), исключая посредников из бизнес-модели.

Менее чем за 20 лет интернет вещей, или Internet of Things (IoT), стал трендом рынка информационных технологий. Аналитики прогнозируют колоссальное количество IoT-устройств через несколько лет – свыше 50 млрд. Развитие производства электронных компонентов позволяет «штамповать» миллионы дешевых чипов для всевозможных устройств. От радиочипов, нанесенных на складские коробки, IoT трансформировался в глобальную «интернетизацию» окружающих нас предметов и воспринимается людьми как глобальная «оцифровка» реальности.

Внимание, важно!

Уже сейчас, говоря об интернете, можно разделять его, разумеется условно, на интернет вещей и интернет людей, то есть получение, анализ информации с целью контроля процессов, передачи данных и управления исполнительными устройствами и всемирную паутину массовой коммуникации, которая подчас «высасывает» не только деньги, но и время. Некоторые пользователи проводят по нескольку часов в неделю в соцсетях, онлайн-играх или на сайтах, покупают в интернет-магазинах вещи, которые не нужны, просто потому, что это легко и доступно, буквально в два клика. В отличие от традиционного «человеческого» интернета, IoT применяется для рационального и практичного подхода. Его ключевая задача – автоматизация, оптимизация, сокращение материальных и временных затрат.

IoT стал всемирным трендом, и скоро возможность «интернетизации» станет обязательным требованием для продуктов и услуг широкого потребления. Новые устройства выходят с конвейера с уже встроенными интеллектуальными и коммуникационными возможностями. И вряд ли кто в точности мог бы предполагать такое прогрессивное развитие технологии еще 20–30 лет назад.

Применение IoT в промышленной индустрии и транспорте сокращает затраты за счет снижения аварийности, уменьшения потерь сырья и количества использованных ресурсов. В сфере энергетики – повышает эффективность выработки и распределения электроэнергии. Интернет вещей экономит не только деньги, но и время: машины заменили человека на рутинной работе и освободили от выполнения рискованных или стандартных задач. Интеллектуальные системы следят за промышленным конвейером, считают товар на складах и регулируют движение вместо человека – в любую погоду, круглосуточно и без выходных.

Кругом людей окружают разнообразные «подключенные» устройства: на улице работают системы безопасности и экомониторинга. Интернет вещей начинает использоваться в быту, в ЖКХ и индустриальной сфере, транспорте, сельском хозяйстве и медицине. Но мало кто вне цеха специалистов задумывается о том, что же на самом деле скрывается за этими двумя направлениями прогрессивного развития общества – интернетом вещей и интернетом людей. В нашей книге мы будем говорить об интернете вещей, поскольку всего знать невозможно и охватить всё также невозможно. Будем конкретны.

1.2. Технологии IoT

IoT (Industrial IoT, IIoT) объединяет концепцию межмашинного общения, использование BigData и проверенные технологии автоматизации производства. Ключевая идея IIoT – в превосходстве «умной» машины над человеком, в точном, постоянном и безошибочном сборе информации.

Технологии, которые присутствуют в IoT, можно рассматривать в нескольких значимых аспектах:

- RFID (радиочастотная идентификация), EPC (электронный код продукта);

- NFC («коммуникация ближнего поля»). Обеспечивает двусторонние взаимодействия между устройствами. Эта технология присутствует в смартфонах и служит для бесконтактных транзакций;
- Bluetooth. Широко применяется в ситуациях, когда достаточно связи ближнего радиуса действия. Чаще всего присутствует в носимых устройствах;
- Z-Wave. Низкочастотные RF-технологии. Чаще применяются для домашней автоматики, управления освещением и пр.;
- Wi-Fi. Самая популярная сеть для IoT (передача файлов, данных и сообщений).

Именно в этом ключе мы будем в дальнейшем излагать материал: прежде всего по теме книги, нас интересуют видеокамеры и аудиодиктофоны – эти инновационные модели, работающие в системе интернета вещей, следовательно, в книге мы будем опираться на все эти пять направлений, особенно на Wi-Fi, Z-Wave, Bluetooth.

Для читателя, не причисляющего себя к разработчикам радиоэлектронных устройств, интернет вещей понятен прежде всего на бытовом уровне – это холодильник, публикующий фото продуктов, к примеру, в Instagram, или стиральная машина, которая «постит» в Facebook: «у меня была сегодня чумовая стирка».

Примерно из 50 млрд ожидаемых подключений менее половины придется на пользовательские гаджеты, которые составляют «customer IoT»: смартфоны и планшеты, диктофоны и камеры, стационарные носимые и возимые датчики различного направления и контроля, в том числе для фитнеса и амбулаторной медицины. Более 15 млрд устройств будут работать в бизнесе и промышленности: разнообразные датчики для оборудования, терминалы для продаж, сенсоры на производственных агрегатах и общественном транспорте. Именно поэтому интернет вещей уже стал инструментом, с помощью которого можно дешево, быстро и масштабно решать конкретные задачи контроля, безопасности, бизнес-задачи в разных отраслях. Интернет вещей повысит уровень контроля качества продукции, выстроит процесс бережливого и экологичного производства, обеспечит надежные поставки сырья и оптимизирует работу заводского конвейера.

1.3. Примеры IoT

Знакомый всем пример – «Яндекс-навигатор». Водители нередко пользуются этим сервисом. Смартфоны и планшеты передают координаты, направление движения и скорость в службу Яндекс, а принятая от пользователей информация анализируется на сервере компании. Получив сведения о заторе, приложение автоматически предлагает водителю варианты объезда и отображает маршрут на экране телефона или планшета. Мобильные устройства, центры обработки данных и приложение Яндекс обмениваются данными без вмешательства человека, являя собой отличный пример интернета вещей. Как результат – водители тратят меньше времени в пробках, выбирая оптимальные маршруты объезда. Искусственный интеллект Яндекса уже пытается перераспределять нагрузку на дорогах мегаполисов. Учитывая накопленную статистику, он предлагает маршруты, которые оптимально загрузят магистрали и минимизируют пробки.

В спорте интернет вещей используют для накопления статистики и анализа данных. Применение IoT-решений разнообразно: от мобильных приложений для любителей утренних пробежек, следящих за расходом калорий, до производительных информационно-вычислительных систем в профессиональном спорте.

Командное IoT-решение отслеживает состояние отдельных спортсменов и всего коллектива. Причем браслеты и брелоки могут быть используемы не только спортсменами, но и для контроля лиц, отбывающих наказание в системе ФСИН, для военизированной охраны объектов – для контроля состояния часового и в других случаях с подобным спектром задач. Информация о перемещении, пульсе считывается датчиками, встроенными в одежду. Координаты и медицинская телеметрия отправляются на облачную платформу, снабжая оперативной информацией руководство и вспомогательные службы команды. Тренер строит тактику игры, не дожидаясь тайм-аута для оценки состояния коллектива, и переигрывает соперников за счет быстрого реагирования на окружающую обстановку. Ранее у тренерского состава и спортивных аналитиков не было иного выбора, кроме как просматривать после игры заметки и десятки часов видеозаписи для оценки поведения игрока на поле и его работоспособности. Теперь информация предоставляется онлайн, и голевой момент

матча всегда можно «вытащить» из хранилища и проанализировать. Интернет вещей обрел популярность не только среди тренеров, но и у медиков – бригады оказания первой помощи мгновенно реагируют на критические показания здоровья подопечных.

Дистанционное снятие показаний со счетчиков водо- и энергоресурсов в домах возможно благодаря IoT-решениям – беспроводной автоматизированной диспетчеризации. В жилищно-коммунальном хозяйстве IoT нашли применение в системах интеллектуальной диспетчеризации – «умных» приборов учета ресурсов. Подключенные к интернету счетчики передают показания в «облако», а диспетчер видит расход воды (электричества, газа) в отдельном доме, квартале или городе. Это дает возможность, не заглядывая в квартиры собственников, в режиме реального времени иметь информацию о потреблении ресурсов, удаленно управлять приборами учета, оперативно выставлять счета жильцам. Без обходчиков, без обработчиков и без временных потерь. За счет точного учета, оповещения о перерасходе ресурсов или авариях подключенные к интернету приборы учета ЖКХ сохраняют до 30% ресурсов в каждом многоквартирном доме. А помимо удобства, дополнительное преимущество для конечного потребителя – сэкономленные на содержании ненужной «прослойки» деньги. Организации, внедрившие IoT-решения для управления многоквартирными жилыми домами, получили эффективный инструмент контроля и учета ресурсов. Такая система автоматизирует трудоемкие операции по сбору и обработке показаний, которые ранее требовали участия половины штата сотрудников. Имея на руках прозрачные данные, управляющая компания выявляет потери и минимизирует расходы на общедомовые нужды (ОДН).

Аналогично – UBER, который за счет концепции IoT исключил таксомоторные компании из бизнес-модели частного извоза. Это дало возможность минимизировать посредников между клиентом и водителем.

Еще один пример. Наиболее продвинутые компании в России (по всему миру это давно вошло в обиход) используют систему для мониторинга влажности, температуры грунта и других характеристик почвы. Она работает как в частных, так и в государственных хозяйствах, где выращивают овощи и фрукты. Датчик, «закрепленный» за отдельным растением или участком с посевами, отправляет информацию на облачный сервер, отку-

да данные поступают оператору, выводя на экран контрольного дисплея состояние саженца (группы растений) и рекомендации по улучшению их плодоносных свойств. Этот комментарий иллюстрирует рис. 1.1.

Рис. 1.1. Датчик контроля роста томата передает данные беспроводным способом на пульт контроля

Как мы поговорили выше, интернет вещей (или IoT) – сеть соединяющая в себе множество объектов: транспортные средства, домашнюю автоматику, медоборудование, микрочипы и т. д. Все составные элементы накапливают и передают данные. Посредством такой технологии пользователь управляет устройствами удаленно.

Примеры IoT-устройств можно рассматривать в нескольких отдельных и связанных единой концепцией группах, таких как:

1) *носимые технологии*.

   К примеру, фитнес-браслеты Fitbit и умные часы Apple Watch легко синхронизируются с другими мобильными устройствами. IoT-часы и браслеты позволяют оперативно в режиме реального времени собирать сведения о здоровье: частота пульса, активность организма во время сна и др.;

2) *инфраструктура и разработка*.

   К примеру, приложение CitySense в онлайн-режиме анализирует данные об освещении и автоматически включает или выключает фонари. Существуют приложения, которые управляют светофорами или сообщают о доступности парковок;

3) *здоровье*.

   Некоторые системы, которые отслеживают состояние здоровья, используются в больницах. В основе их работы – ори-

ентировочные данные. Эти сервисы контролируют дозировку лекарств в различное время дня. К примеру, приложение UroSense отслеживает уровень жидкости в организме и, если нужно, повысит этот уровень. А врачи узнают сведения о пациентах по беспроводной связи. Рассмотрим пример: медицинская система, которая следит за состоянием здоровья, частотой сердцебиений, содержанием жидкости и отправляет отчеты медработникам. Данные отображаются в системе; доступны архивы. Проанализировав информацию, врачи решают, принимать ли пациенту медикаменты, удаленно.

Интересный симбиоз такой «пахучей» сферы агротехники, как удобрение полей и IoT. Фермер оснастил трактора-распрыскиватели, обслуживающие угодья в радиусе 1 км от станции, решением на базе беспроводных технологий. Водитель-оператор насосной установки удаленно отслеживает и распределяет подачу органических удобрений на поля, а владелец контролирует расход с экрана своего смартфона.

С помощью IoT-технологий операторы морских ветрогенераторов удаленно контролируют износ роторов и турбин, отслеживают их производительность. За счет своевременного обслуживания минимизируется риск остановки «ветряков» и отпадает необходимость в отправке бригад на удаленные морские платформы.

Оборудования на производственных площадках подключили к IoT-платформе, сигнализирующей о необходимости ТО для профилактики возможной поломки. «Проактивный» мониторинг сократил расходы за счет снижения издержек и ликвидации простоев. Традиционно ППР (планово-предупредительные ремонты) требовали остановки производственных линий и организовывались по графику, независимо от того, была в них необходимость или нет. Поэтому важно, чтобы внедрение IoT-технологии позволило проводить упреждающее техобслуживание тогда, когда оно действительно нужно, и ремонтировать оборудование до того, как оно сломается. Интернет вещей обеспечил не только непрерывность производства, но и сэкономил на планировании предупредительных работ (как правило, затраты на планирование составляют 30–40 % от объема ремонтного фонда предприятия).

Кроме того, новые технологии оптимизируют производственный процесс и уберут из него человеческий фактор, а вместе с ним и лишние риски.

Одно из решений в сегменте IoT отслеживает динамику болезни и выздоровления пациентов в режиме 24/7 посредством носимого на теле датчика. Мониторинг происходит в режиме реального времени, начиная от сбора показаний в стационаре и дома, завершая направлением данных лечащему врачу и в лаборатории для анализа и принятия решений. Есть проекты, развернутые в рамках лечебного учреждения и предупреждающие персонал об истощении запаса медикаментов или инструментов.

В обеспечении физической безопасности применение IoT-концепции скорее экзотично, чем привычно. В октябре 2016 года технологию интернета вещей начали использовать военные – для охраны Крымской военно-морской базы Министерство обороны закупило комплекс охраны «Часовой-1». Как уже было отмечено выше, комплекс, в состав которого входят вибробраслеты, гарантирует безопасность бойцов, охраняющих объекты и проверяющих автотранспорт на «блоках». Каждый браслет оснащен датчиком «неподвижности». Как только часовой прекращает движение более чем на 30 с, система посылает на его браслет вибросигнал. Если в течение 15 с после предупреждения боец не «оживет» – в караульном помещении объявляется тревога.

1.4. Перспективы для IoT

Перспективы для развития интернета вещей и новых, с расширенными возможностями протоколов IoT связывают с несколькими аспектами, в числе которых особенности проникающей способности сигнала XNB. Если удастся решить эту проблему в ближайшие годы (а над ее решением работают довольно эффективно), то фундаментом новых масштабных проектов в рассматриваемой теме станет энергоэффективная сеть, удовлетворяющая запросы промышленников, сельхозпроизводителей, государственные компании в масштабности и невысокой стоимости эксплуатации. Интернету вещей сегодня, как воздух, нужен стандарт связи с возможностью широкого территориального охвата, высокой энергоэффективностью, дешевой инфраструктурой и не требующей высоких эксплуатационных расходов. В этом, пожалуй, заинтересованы все стороны. Поэтому можно ответственно заявлять, что будущее IoT-концепции за LPWAN.

1.4.1. Особенности LPWAN

С учетом перечисленных требований и ограничений решением проблемы видится использование технологии на стыке высокой дальности и низкого энергопотребления. Она называется Low-Power Wide-Area Network (сокращенно – LPWAN), или энергоэффективная сеть дальнего радиуса действия. LPWAN разрабатывался специально для межмашинного общения и стал двигателем дальнобойного интернета вещей (далее – ИВ). Отсутствие относительно высоких требований к объему передаваемой информации позволило сконцентрироваться на важных параметрах технологии и обеспечить 50-километровую дистанцию взаимодействия между разнесенными устройствами, высокую энергоэффективность, проникающую способность и масштабируемость. Преимущества LPWAN вписываются в потребности масштабного внедрения IoT в промышленности, транспорте, сфере безопасности и других отраслях. Относительно большой радиус действия, высокая автономность конечных устройств, относительная простота развертывания LPWA-сети и низкая стоимость инфраструктуры дают импульс крупномасштабным проектам и развитию ИВ.

«Дальнобойная» и энергоэффективная LPWAN отлично подходит для IoT как в бытовом, так и в промышленном секторе, где имеется потребность в автономной передаче телеметрии на дальние расстояния, потому что LPWAN гораздо лучше соответствует запросам M2M-сетей, чем ее слабый аналог (в теме передачи данных) сотовая связь – тысячи квадратных километров будут покрыты лишь одной базовой станцией. Построение такой сети проще, а обслуживание – дешевле. Сей подход становится единственной альтернативой в случае, когда датчики разнесены по большой территории. К примеру, счетчики воды в пределах одного квартала или датчики влажности почвы, размещенные сразу на нескольких полях.

IoT проник в недоступные ранее сферы, улучшив качество жизни людей и увеличивая эффективность бизнеса, экономики. Технологии ИВ применяют там, где они выгодны бизнесу и удобны людям.

За счет увеличения масштаба производства и удешевления компонентной базы стоимость «умных» электронных устройств снизится еще более. IoT проник в автомобили, грунт, море и реки, в тело человека. Датчики стали миниатюрными, помещаются в бытовых предметах или продуктах питания. Соответственно, в

перспективе устройства еще уменьшатся в размерах, уменьшится и форм-фактор аккумуляторов, а затем они и вовсе исчезнут – «умные» датчики научатся получать энергию из окружающей среды: от вибрации, света или воздушных потоков, и станут полностью автономными. Если Господь благоволит, то и мы застанем то время, когда интернет вещей станет гетерогенной средой, существующей как живой организм.

Если оставить неблагодарные прогнозы о «количестве устройств интернета вещей к 2020 году», станет ясно, что IoT-индустрия растет. Порядок роста примерно понятен, как и цель – подключение «армии» устройств к интернету.

1.5. Перспективы разработки новых датчиков для IoT

В 2019 году разработчики ставят перед собой следующие перспективные задачи, чтобы обеспечить:

- небольшой объем данных: датчикам и сенсорам не нужно передавать мега- и гигабайты, как правило, это биты и байты;
- энергоэффективность: бóльшая часть датчиков автономна и должна работать годами без смены элемента питания или подпитываясь естественной энергией (солнце, ветер, иные виды альтернативной энергии);
- масштабируемость: в сети должны уживаться миллионы различных устройств, чтобы при необходимости оперативное добавление одного-двух миллионов не вызывало сложностей;
- глобальность: работа на перспективу широкого территориального охвата и, как следствие, передача информации на значительные расстояния;
- проникающая способность: электронные устройства под землей и водой должны передавать сигнал наружу;
- конкурентная стоимость устройств: устройства должны быть относительно дешевы и доступны для пользователя, а готовые решения рентабельны для бизнеса;
- относительная простота: принцип «поставил и забыл»: пользователь выберет понятные и дружелюбные устройства.

Не так давно люди убедили себя, будто бы сети сотовой связи – наиболее перспективные кандидаты на построение развернутой на сотни километров беспроводной IoT-среды. Однако ни стандарт GSM, ни инфраструктура мобильных операторов изначально не создавались для M2M-диалога. Протоколы сотовой связи предназначены для общения людей: этому способствуют большой объем трафика и высокая скорость обмена данными в густонаселенных районах, и это же является проблемой для безупречной качественной связи. Те ошибки или «сбои» аналоговой (речевой) или цифровой связи, которые пусть и скрепя сердце допустимы в общении между частными корреспондентами (в быту), не могут быть признаны приемлемыми в радиоэлектронных устройствах в промышленном производстве с высокими требованиями к техногенной безопасности и (или) передаче данных. К сожалению, в этом вопросе еще не все так гладко, как хотелось бы, ибо ограничить сигнал Wi-Fi с частотой 2,4 ГГц, забить его помехой можно даже на бытовом уровне – такие устройства существуют, – чем привести в полную негодность всю IoT-сеть. Однако и над этой проблемой профессионалы работают, что дает надежду либо на трансформацию протоколов в будущем, либо на обеспечение их безопасности от несанкционированного внешнего воздействия. Подробнее о методах защиты и возможных методах воздействия на сигналы в системе интернета вещей мы поговорим во второй главе книги.

1.6. Сравнение беспроводных технологий в интернете вещей

Разработчики изначально не предполагали возможности обмена небольшими объемами данных между разнесенными «умными» сенсорами. Датчику с Wi-Fi необходимо постоянное питание, а элемент умного GSM-устройства продержится 2–3 недели. Не многие пока готовы ежемесячно менять элементы питания в десятках устройств или монтировать к ним проводную систему питания. Подключение всевозможных устройств к мобильным сетям еще можно представить в населенных пунктах, но за пределами оживленных трасс и урбанизированных территорий протоколы GSM, 3G, LTE не позволяют создавать масштабные IoT-проекты – слишком дорого разворачивать и обслуживать инфраструктуру сотовой сети.

Внимание, важно!

В населенных пунктах с большой плотностью населения (городах, мегаполисах) сотовая связь ограничена низкой проникающей способностью сигнала. А «умные» датчики или счетчики находятся за несколькими стенами, в технических колодцах или на цокольных этажах, где связь GSM может быть неустойчива по определению распространения радиоволн на соответствующих частотах.

В наши дни сложности с компонентной базой ушли в прошлое, появился новый вызов: необходимо объединить миллиарды «умных» приборов в единую сеть. Интеллектуальный станок, датчик температуры масла на промышленном агрегате, смарт-холодильник – всем этим устройствам необходима среда для общения. В противном случае они так и останутся «немыми»: обычным счетчиком или датчиком, отличающимся от своих собратьев только «космическим» дизайном.

К примеру, «Яндекс-навигатор» может работать через GPRS/3G/4G, и пока другая связь для сего приложения не подходит. Можно подключить смартфон к Wi-Fi и запустить «Навигатор», но как только автомобиль отъедет на 150 м от точки доступа – приложение «закончится». А в «умном» доме не «приживутся» автономные GPRS-датчики – через несколько дней активного использования датчиков в них «сядут» батарейки. Поэтому в интеллектуальном жилище лучше всего подойдет энергоэффективный ZigBee.

Действительно, для передачи данных разрабатывалось множество протоколов, но каждый из них был «заточен» под определенную задачу: GSM для голосового общения, GPRS для обмена данными с мобильных телефонов, ZigBee для создания локальной сети и управления «умными» домами, а Wi-Fi для беспроводных локальных сетей с высокой скоростью передачи данных. Все эти технологии интернета вещей могут быть применены для решения нецелевых задач и по-разному с ними справляться. Сейчас разработчики работают над тем, как это все конфигурировать и объединять для взаимодействия именно с высокой степенью надежности.

И наконец, открытый пока вопрос возможности глушения «полезных» сигналов как Wi-Fi, так и GSM, а также спутниковой связи на бытовом уровне. Это действительно проблема, подробно она хорошо описана в современной литературе.

1.7. IoT-архитектура

Существует несколько подходов для тестирования архитектуры IoT.

Необходимо достаточно продуманное оборудование, которое бы отправляло не только уведомления, но и сообщения об ошибках, предупреждения и др. В системе должна присутствовать опция, которая фиксирует события, чтобы конечному пользователю было понятнее. Если такая возможность не предусмотрена, сведения о событиях сохраняются в базе данных. Тщательно проверяется и возможность обработки данных и обмена задачами между устройствами. Необходимо обеспечить юзабилити тестирование каждого из устройств, и желательно при тестах, чтобы тестируемые устройства были портативными.

Безопасность IoT

Данные лежат в основе работы всех подключенных устройств. Потому не исключен несанкционированный доступ во время передачи данных. С точки зрения тестирования ПО необходимо проверять, насколько защищены/зашифрованы данные. Если есть UI, нужно проверить, защищен ли он паролем.

Эффективность и сетевые возможности

Крайне важны возможность подключения к сети и функциональность IoT. Ведь речь идет о системе, которая используется в целях здравоохранения.

Проверяются два главных аспекта:

- наличие сети, возможности передачи данных (передаются ли задания с одного устройства на другое без каких-либо заминок);
- сценарий, когда подключение отсутствует.

Независимо от уровня надежности системы существует вероятность, что статус системы будет офлайн. Если сеть недоступна, сотрудникам больницы или другой организации необходимо об этом знать (уведомления). Таким образом, они смогут следить за состоянием пациента сами, а не ждать, когда система заработает. С другой стороны, в подобных системах обычно присутствует механизм, который сохраняет данные, если это офлайн-система. То есть потеря данных исключается.

Возьмем здесь за пример медицинскую сферу. Необходимо учитывать, насколько решение для сферы здравоохранения применимо в конкретных условиях. В тестировании участвуют от 2 до 10 пациентов, данные передаются на 10–20 устройств. Если вся больница подключается к сети, это уже 180–200 пациентов. То есть фактических данных будет больше, чем тестовых. Также необходимо протестовать утилиту для мониторинга системы: текущая нагрузка, потребление электроэнергии, температура и пр.

Тестирование совместимости

Этот пункт всегда присутствует в плане по тестированию IoT-системы. Совместимость разных версий операционных систем, типов браузеров и их соответствующих версий, устройств разного поколения, режимов связи, к примеру Bluetooth 3.0, крайне важна для IoT.

Пилотное тестирование

Пилотное тестирование – обязательный пункт тест-плана. Только тесты в лаборатории позволят сделать вывод о том, что система функциональна. При пилотном тестировании число пользователей ограничено. Они совершают манипуляции с приложением и высказывают свое мнение. Эти комментарии оказываются весьма кстати, позволяют сделать надежное приложение.

Проверка на соответствие

Система, которая отслеживает состояние здоровья, проходит множество проверок на соответствие. Бывает и так, что программный продукт проходит все этапы тестирования, но проваливает финальный тест на соответствие (тестирование проводит регулирующий орган). Поэтому, целесообразнее проверить на предмет соответствия нормам и стандартам перед стартом цикла разработки.

Тестирование обновлений

IoT – это комбинация множества протоколов, устройств, операционных систем, встроенного ПО, аппаратного обеспечения, сетевых уровней и т. д. Когда происходит обновление – будь то система или что-то еще из перечисленного выше, – требуется

тщательное регрессионное тестирование. В общую стратегию вносятся поправки, чтобы избежать сложностей, связанных с обновлением.

1.8. Особенности тестирования IoT

IoT – это архитектура, в которой тесно переплетаются компоненты ПО и аппаратной части. Важно не только программное обеспечение, но и качество устройств и взаимодействие: датчики, сенсоры, шлюзы, проводка питания и др. Одного лишь функционального тестирования будет недостаточно, чтобы сертифицировать систему. Все составные компоненты взаимозависимы. IoT сложнее, чем отдельно ПО или только аппаратная часть.

Модель взаимодействия устройств

Составные части сети должны взаимодействовать в режиме реального времени или близкого к реальному. Все это становится единым целым – отсюда дополнительные сложности, связанные с IoT (безопасность, обратная совместимость и обновления).

Тестирование данных, поступающих в реальном времени

Получить такие данные непросто. Дело усложняется тем, что система, как в описанном случае, может относиться к сфере здравоохранения.

Сеть IoT обычно состоит из разных устройств, которые управляются разными платформами iOS, Android, Windows, Linux. Тестирование возможно только на некоторых устройствах, поскольку тестировать на всех возможных устройствах практически невозможно.

Доступность сети

Сетевое соединение играет важную роль в IoT. Скорость передачи данных постоянно увеличивается. IoT-архитектура должна тестироваться в различных условиях соединения на разной скорости. Эмуляторы виртуальных сетей в большинстве случаев используются, чтобы разнообразить сетевую нагрузку, возможности соединения, стабильность и прочие элементы нагрузочного тестирования. Но фактические данные – это всегда новые сценарии, и тестировщик не знает, где в будущем возникнут сложности.

1.8.1. Инструменты тестирования IoT

Существует множество инструментов, которые применяются в тестировании IoT-систем. Их классифицируют в зависимости от предназначения.

Особенности программного обеспечения

Wireshark: инструмент с открытым исходным кодом. Используется для мониторинга трафика в интерфейсе, адреса источника/заданного хоста и др.

Tcpdump: этот инструмент выполняет похожую работу. У утилиты нет GUI, ее интерфейс – командная строка. Она дает возможность пользователю высвечивать TCP/IP и другие пакеты, которые передаются по сети.

Особенности аппаратного обеспечения

JTAG Dongle: инструмент, аналогичный отладчикам в приложениях для ПК. Позволяет найти дефекты в коде целевой платформы и показывает изменения шаг за шагом.

Digital Storage Oscilloscope: проверяет различные события с помощью временных отметок, перебои с электропитанием, целостность сигнала.

Software Defined Radio: эмулирует приемник и передатчик для различных беспроводных шлюзов.

Подход к тестированию IoT может отличаться в зависимости от конкретной системы/архитектуры. Тестировать IoT для неподготовленного пользователя непросто, но вместе с тем это интересная работа, благо есть где «размахнуться»: устройств, протоколов и операционных систем множество. Особо интересен тестовый формат TAAS («тесты с точки зрения пользователя»), он позволяет творчески подходить к делу, основываясь на вариативном и опциональном выборе функций, а не просто выполнять формальные требования.

1.9. Облачные технологии беспроводной передачи данных

Доступ через интернет к видеонаблюдению UControl по облачной технологии P2P для пользователя осуществляется бесплатно. Облачная технология P2P (англ. peer-to-peer) создана для удобства

быстрой настройки удаленного доступа к системам видеонаблюдения обычными пользователями-неспециалистами. Используя данную технологию, достаточно подключить рекордер системы видеонаблюдения UControl к сети интернет обычным LAN-кабелем и подождать 1–2 мин. Интернет-подключение будет автоматически настроено, после чего доступ к системе будет возможен из любой точки мира. В отличие от множества других подобных облачных сервисов, технология P2P не требует платы за подключение или обслуживание. Большинство комплектов и рекордеров UControl поддерживает технологию P2P.

Выберите тип устройства, с которого необходимо организовать доступ по технологии P2P, и следуйте инструкции.

1.9.1. Передача файлов в системе интернета вещей

Представим себе конкретный пример. Оба взаимодействующих устройства (ноутбук и телефон) подключены (дома) в сеть к интернету через Wi-Fi-роутер. Как вариант понадобится программа-утилита, не требующая установки и сразу готовая к работе без дополнительных настроек. Переходим на официальный сайт программы HFS (Http File Server) HFS (Http File Server) и в свободном режиме ее скачиваем (Download). После запуска утилиты ее интерфейс прост и понятен, при запуске программатора открывает 80-й порт для доступа по протоколу http.

Все, что нужно сделать, – это перетащить файлы, которые будут передаваться с ноутбука на телефон, в окно программы. Практика такова. Берем телефон и запускаем интернет-браузер. Теперь в адресной строке браузера вводим адрес, указанный в HFS, в конкретном примере это адрес http://192.168.1.35/ или http://192.168.1.0035/. После этого шага можете загрузить эти файлы с браузера в заранее подготовленный сотовый телефон.

Кроме сказанного, безопасности беспроводных сетей уделяют особое внимание. Ведь Wi-Fi является беспроводной сетью с относительно большим радиусом действия. Соответственно, возможный злоумышленник может перехватывать информацию или же атаковать пользовательскую сеть, находясь на относительно безопасном расстоянии. Существует множество различных способов защиты, и при условии правильной настройки можно быть уверенным в обеспечении необходимого уровня безопасности. Разберемся в них предметно.

- WEP – это протокол шифрования, использующий довольно нестойкий алгоритм RC4 на статическом ключе. Существует 64-, 128-, 256- и 512-битное WEP-шифрование. Чем больше бит используется для хранения ключа, тем больше возможных комбинаций ключей, а соответственно, более высокая стойкость сети к взлому. Часть WEP-ключа является статической (40 бит в случае 64-битного шифрования), а другая часть (24 бит) – динамическая (вектор инициализации), то есть меняющаяся в процессе работы сети. Основной уязвимостью протокола WEP является то, что векторы инициализации повторяются через некоторый промежуток времени, и взломщику потребуется лишь собрать эти повторы и вычислить по ним статическую часть ключа. Для повышения уровня безопасности можно дополнительно к wep-шифрованию использовать стандарт 802.1x или VPN.
- WPA – более стойкий протокол шифрования, чем WEP, хотя используется тот же алгоритм RC4. Более высокий уровень безопасности достигается за счет использования протоколов TKIP и MIC.
- TKIP (Temporal Key Integrity Protocol). Протокол динамических ключей сети, которые меняются довольно часто. При этом каждому устройству также присваивается ключ, который тоже меняется.
- MIC (Message Integrity Check). Протокол проверки целостности пакетов. Защищает от перехвата пакетов и из перенаправления. Также возможно и использование 802.1x и VPN, как в случае с WEP-протоколом.

Существует два вида WPA:

- WPA-PSK (Pre-shared key). Для генерации ключей сети и для входа в сеть используется ключевая фраза. Оптимальный вариант для домашней или небольшой офисной сети.
- WPA-802.1x. Вход в сеть осуществляется через сервер аутентификации. Оптимально для сети крупной компании.

Усовершенствование протокола WPA активно происходит все предыдущие годы. В отличие от WPA, используется более стойкий алгоритм шифрования AES – WPA2. По аналогии с WPA, WPA2 также делится на типы: WPA2-PSK и WPA2-802.1x.

Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приемник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi дает свободу при выборе критериев для соединения. Однако сей стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему можно выделить:

- автономные точки доступа (называются также самостоятельные, децентрализованные, умные);
- точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные);
- бесконтроллерные, но притом неавтономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- со статическими настройками радиоканалов;
- с динамическими (адаптивными) настройками радиоканалов;
- со «слоистой» или многослойной структурой радиоканалов.

Беспроводной интернет позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развертывания и/или расширения сети. Места, где нельзя проложить кабель, к примеру вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями. Также такое решение позволяет иметь доступ к сети мобильным устройствам. Для всех Wi-Fi-устройств гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi.

Другим отличительным фактором использования Wi-Fi-устройств и сетей является их доступность в бытовом плане, легкий монтаж и мобильность. Пользователь системы интернета вещей больше не привязан к одному месту и может пользоваться интернетом в комфортной обстановке.

Внимание, важно!

В России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации.

В пределах Wi-Fi-зоны в интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д. Излучение от Wi-Fi-устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона. Поэтому недостатки Wi-Fi тоже имеют место.

В диапазоне 2,4 ГГц работает множество устройств, поддерживающих Bluetooth и др., и даже микроволновые печи, что ухудшает их общую электромагнитную совместимость. Производителями оборудования указывается скорость на L1 (OSI), в результате чего создается иллюзия, что производитель оборудования завышает скорость, но на самом деле в Wi-Fi высоки служебные «накладные расходы». Получается, что скорость передачи данных на L2 (OSI) в Wi-Fi ниже заявленной скорости на L1 (OSI). Реальная скорость зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград, присутствия помех от других беспроводных устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.

Частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы. Во многих европейских странах разрешены два дополнительных канала, которые запрещены в США. В Японии есть ещё один канал в верхней части диапазона, а другие страны, к примеру Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, к примеру Россия, Белоруссия и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или регистрации Wi-Fi-оператора.

1.10. Особенности доступа к системе видеонаблюдения через P2P с разным оборудованием

Для этого потребуется следующее оборудование (вариативно): персональный компьютер или ноутбук, iPhone или iPad, Android-смартфон или планшет.

После подключения системы видеонаблюдения UControl с поддержкой P2P к сети интернет она автоматически посылает сигнал на сервер, который идентифицирует ее по уникальному номеру – MAC-адресу рекордера. Для доступа к системе с компьютера достаточно открыть обычный браузер (например, Internet Explorer) и зайти на сайт сервера. Для доступа с мобильных устройств (iPhone, iPad, смартфоны и планшеты Android) необходимо установить на устройство бесплатную программу из магазина приложений. На сайте сервера (при доступе с компьютера) или в программе (при доступе с мобильных устройств) нужно ввести MAC-адрес рекордера, логин и пароль, после чего будут доступны онлайн-просмотр видео и архивных записей и настройки системы видеонаблюдения.

Для организации удаленного доступа к системе видеонаблюдения UControl без поддержки технологии P2P у интернет-провайдера необходимо подключить одну из двух услуг: «внешний статический IP-адрес» или «внешний динамический IP-адрес». А также произвести настройку перенаправления портов на роутере в случае его использования.

Видеонаблюдение через интернет приобретает все большую популярность, во многом благодаря широким возможностям в сравнении с аналоговыми системами. Как правило, для видеонаблюдения через интернет используют IP-камеры, однако их эксплуатация связана с некоторыми неудобствами, связанными с процессом настройки. Сей недостаток исправлен в новых IP-камерах, работающих по технологии P2P. Пользователи интернета ежедневно сталкиваются с этой технологией, закачивая файлы через торрент или общаясь посредством Skype.

Как это работает?

Аббревиатура P2P обозначает алгоритм «peer to peer», что в дословном переводе обозначает «равный к равному». Пиринговый протокол отличается от привычной клиент-серверной архитектуры отсутствием выделенного сервера, так как каждый узел одновременно выполняет функции как клиента, так и сервера. P2P-архитектура отличается повышенной отказоустойчивостью и более эффективным использованием полосы пропускания. Эта технология является наиболее востребованной для организации удаленного домашнего видеонаблюдения, так как в ней реализована возможность самостоятельной установки без сложных манипуляций с сетевым оборудованием. Возможность работы с

динамическим IP позволяет установить видеонаблюдение в местах, где нет доступа к проводному интернету, достаточно приобрести 3G/4G-модем с поддержкой Wi-Fi и настроить программное обеспечение.

1.10.1. Принципы подключения P2P-камер видеонаблюдения

Камеры P2P начинают работать сразу после подключения к сети интернет, посредством обычного сетевого кабеля или по Wi-Fi. Использование технологии P2P в системах видеонаблюдения позволило существенно упростить настройку оборудования и исключить применение статического IP как обязательного условия для работы всей системы.

По новой технологии видеокамере присваивается специальный идентификатор, который соответствует определенному номеру. При подключении P2P IP-камеры к сети она моментально начинает посылать запрос о готовности, передавая свой уникальный ID.

Установив специальное программное обеспечение на смартфон, планшет или PC, пользователь получает прямой доступ к видеопотоку, сразу же после ввода идентификатора IP видеокамеры. Также реализованы возможность удаленной настройки камеры, непосредственное управление поворотными механизмами и двухсторонняя голосовая связь.

Внимание, важно!

Разрешение сенсора видеокамер может варьироваться от 0.3 до 5 МПс в зависимости от модели (чем больше разрешение, тем выше требования к скорости интернет-соединения). Программное обеспечение для просмотра видеопотока и управления камерами абсолютно бесплатно и доступно для скачивания в Google Play и App Store (планшеты и смартфоны), а также на сайтах производителя (ПО для компьютера). ПО для мобильных устройств позволяет просматривать видеопоток в любом месте, где есть доступ к сети, что является одним из главных преимуществ P2P-технологии.

Оборудование для P2P-видеонаблюдения состоит непосредственно из IP-камеры с поддержкой технологии и специального ПО, устанавливаемого на различные устройства. P2P-камеры

выполняются в купольном или классическом варианте, первый предпочтительнее, так как обеспечивает возможность удаленного управления поворотом и наклоном видеоискателя.

Также выпускаются варианты для уличной и внутренней установки, различающиеся конструктивными особенностями. Камеры, как правило, оснащаются ИК-подсветкой для работы ночью, а также дополнительным слотом для SD-карты, на которую можно записывать видео. Желательно наличие датчиков движения, встроенного микрофона и динамика, существенно расширяющих область применения P2P-камер.

1.10.2. Практическая настройка P2P-камеры

Настройка P2P-видеонаблюдения своими руками не требует сложных манипуляций и занимает немного времени. Порядок действий следующий:

- скачать и установить ПО для работы с камерой;
- установить камеру видеонаблюдения в заранее выбранном месте и подключить напряжение питания;
- подключить видеокамеру к сети интернет, используя кабель LAN или Wi-Fi (в зависимости от используемого оборудования);
- запустить ПО и ввести идентификатор (код на корпусе устройства). При использовании смартфона или планшета можно просто просканировать QR-код.

В программе выбирается камера, и можно приступать к просмотру видео и управлению функциями камеры. Рекомендуется протестировать все доступные функции, включая работу двухсторонней голосовой связи и запись видео на SD-карту. P2P-видеонаблюдение рекомендуется для полноценной замены аналоговых систем, а также для домашнего использования. Популярности технологии способствуют достаточно низкая цена на оборудование и очень простая настройка, что существенно расширяет сферу применения систем видеонаблюдения.

1.10.3. Особенности настройки Wi-Fi на конкретном оборудовании

Главное условие: в помещении должна быть работающая точка доступа Wi-Fi. Радиус действия точки доступа в среднем

20–40 м в зависимости от препятствий и помех. Чтобы подключить ноутбук к сети Wi-Fi, необходимо убедиться, что на вашем оборудовании включен адаптер беспроводных сетей. О его состоянии, как правило, сообщает один из индикаторов на панели ноутбука. На некоторых моделях ноутбуков присутствует отдельная кнопка управления адаптером. Сделано это для того, чтобы в любой момент было возможно выключить Wi-Fi-адаптер в целях экономии заряда аккумулятора. В некоторых моделях кнопка включения/выключения Wi-Fi-адаптера отсутствует, и функцию выполняет сочетание клавиш **Fn**+**Fx**, **x** – в данном случае персональная для всех ноутбуков, обозначается на клавиатуре значком антенны.

Настройка Wi-Fi в операционных системах Windows 7, 8, 10, Vista происходит так. После включения адаптер сам находит доступные сети в радиусе действия. Wi-Fi-сети имеют имя SSID (Service Set Identifier), то есть идентификатор беспроводной сети. Под открытыми сетями понимается возможность подключения без необходимости регистрации и ввода ключей безопасности, однако это не означает, что при подключении к сети сразу появится доступ в интернет. Нередко в общедоступных Wi-Fi-сетях после подключения появляется окно авторизации, через которое можно получить доступ в сеть. Полностью открытые сети, не требующие аутентификации и имеющие свободный доступ в глобальной сети, – нередко результат неграмотной настройки точки доступа, потому что, с одной стороны, использование свободного метода «раздачи» интернета может обернуться непредсказуемыми последствиями для владельцев точки доступа. Но это только на первый взгляд.

С другой стороны, там, где в обществе практикуется большое доверие (не Россия, но страны Европы), нет необходимости создавать избыточные административные барьеры и «следить» за пользователями. В России нашего времени, к сожалению, принят именно первый вариант, когда даже если вы законопослушный гражданин (каких у нас большинство), на всякий случай надо за вами последить – а вдруг вы чего-то «учудите». Такая практика вряд ли может кому-то понравиться, но, к сожалению, мы на ее регулирование влиять пока не можем.

Закрытые точки доступа Wi-Fi для подключения к сети требуют специальный ключ, состоящий из множества знаков. Ключ является основной защитой от несанкционированного подклю-

чения к сети Wi-Fi. Чтобы подключить Wi-Fi, в ноутбуке ничего настраивать не нужно. Необходимо убедиться, что адаптер включен. Включенный адаптер обнаружит беспроводные сети в радиусе действия, если таковые имеются. После этого следует выбрать нужную сеть, используя данные SSID, нажать «подключить». Если сеть закрытая, то система запросит ключ безопасности, а если открытая, то подключится сама, присвоит IP-адрес и сделает ваше оборудование частью локальной сети. В случае успешного подключения необходимо открыть браузер и набрать любой адрес, к примеру «яндекс», и перейти по нему.

1.11. Актуальные вопросы безопасности в системе интернета вещей

Центральной частью любого Wi-Fi-оборудования является так называемая точка доступа или маршрутизатор (Router). И чтобы собрать все эти продукты воедино, производители Wi-Fi-оборудования предоставляют специализированные веб-страницы, благодаря которым пользователи Wi-Fi могут входить в глобальную сеть интернет, используя собственный аккаунт и специализированный особый сетевой адрес. Веб-конструкция защищена экраном-логином (имя пользователя и пароль), который, по идее, должен давать доступ в интернет только зарегистрированным пользователям. Однако по умолчанию логины предоставляются самими производителями Wi-Fi-оборудования, и они известны хакерам в интернете. Следует поменять все эти настройки. В нормально настроенной сети вредный хакер получит «отказ» из-за незнания пароля и к пользовательским данным, хранящимся в памяти ПК, или пересылаемым сообщениям не попадет. Но и это не отменяет возможности взлома устройства из внутренней сети, так что идея поменять пароль – более чем здравая, особенно в том, что касается управления исполнительными устройствами в системе интернета вещей.

Обязательно включите защиту шифрования WPA/WEP. Все виды Wi-Fi-оборудования поддерживают определенные формы шифрования. Сама технология шифрования меняет должным образом все сообщения, которые рассылаются посредством Wi-Fi; наличие данного стандарта шифрования подразумевает, что не

каждый сможет дистанционно управлять вашими исполнительными устройствами. Есть несколько стандартов защиты; пользователю надо найти то, которое будет наиболее эффективно работать с конкретным Wi-Fi-оборудованием. И тем не менее какую бы технологию вы не использовали, все Wi-Fi-девайсы в сети и системе интернета вещей должны поддерживать собственные настройки пользователя. Для начала вполне можно найти и выставить минимальный уровень безопасности в настройках пользовательского Wi-Fi-оборудования. Настраивать стоит WPA, притом очень желательно WPA2-only (шифрование AES). Остальные варианты (WEP и WPA с шифрованием TKIP) подвержены ряду неприятных уязвимостей. WEP вообще очень легко взламывается, и его эффективность чисто символическая. Защитит только от совсем ленивых «взломщиков».

1.11.1. Протоколы разных стандартов безопасности сети

- EAP (Extensible Authentication Protocol). Протокол расширенной аутентификации. Используется совместно с RADIUS-сервером в крупных сетях.
- TLS (Transport Layer Security). Протокол, который обеспечивает целостность и шифрование передаваемых данных между сервером и клиентом, их взаимную аутентификацию, предотвращая перехват и подмену сообщений.
- RADIUS (Remote Authentication Dial-In User Server). Сервер аутентификации пользователей по логину и паролю.
- VPN (Virtual Private Network) – виртуальная частная сеть. Протокол был создан для безопасного подключения клиентов к сети через общедоступные интернет-каналы. Принцип работы VPN – создание так называемых безопасных «туннелей» от пользователя до узла доступа или сервера. Хотя VPN изначально был создан не для Wi-Fi, его можно использовать в любом типе сетей. Для шифрования трафика в VPN чаще всего используется протокол IPSec. Он обеспечивает практически стопроцентную безопасность. Случаев взлома VPN на данный момент неизвестно. Рекомендуется использовать эту технологию для корпоративных сетей.

1.11.2. Дополнительные методы защиты пользовательской сети

Фильтрация по MAC-адресу – важное звено в обеспечении безопасности работы. MAC-адрес – уникальный идентификатор устройства (сетевого адаптера), «зашитый» в него производителем. На некотором оборудовании можно задействовать данную функцию и разрешить доступ в сеть необходимым адресам. Это создаст дополнительную преграду взломщику, хотя не очень серьезную – в принципе, MAC-адрес можно подменить. Приватное скрытие SSID обеспечивает сети еще большую безопасность.

SSID – это идентификатор беспроводной сети. Большинство оборудования позволяет его скрыть, таким образом, при сканировании всех доступных беспроводных сетей вашей сети видно не будет. Это не слишком серьезная преграда, если взломщик использует более продвинутый сканер сетей, чем стандартная утилита в Windows.

Запрет доступа к настройкам точки доступа или роутера через беспроводную сеть реализуется следующим образом. Активировав эту функцию, можно запретить доступ к настройкам точки доступа через Wi-Fi, однако это не защитит пользователя от перехвата трафика или проникновения в сеть. Поэтому неправильная настройка оборудования, поддерживающего даже самые современные технологии защиты, не обеспечит должный уровень безопасности сети. В каждом стандарте есть дополнительные технологии и настройки для повышения уровня безопасности, которые опытный пользователь умело применяет на практике, не манкируя обеспечением безопасности собственных данных.

На промышленном уровне суперсовременные технологии Wi-Fi предлагаются пока ограниченным числом поставщиков. Так, несколько лет назад компания Siemens Automation & Drives предложила Wi-Fi-решения для своих контроллеров SIMATIC в соответствии со стандартом IEEE 802.11g в свободном ISM-диапазоне 2,4 ГГц, обеспечивающим максимальную скорость передачи данных. Технологии применяются для управления движущимися объектами и в складской логистике, а также в тех случаях, когда по какой-либо причине невозможно прокладывать проводные сети Ethernet. Использование Wi-Fi-устройств на предприятиях обусловлено высокой помехоустойчивостью, что делает их применимыми на предприятиях со множеством металлических кон-

струкций. Wi-Fi-электронные устройства не создают существенных помех для узкополосных радиосигналов. Технология находит широкое применение на удаленном или опасном производстве, там, где нахождение оперативного персонала связано с повышенной опасностью или вовсе затруднительно.

К примеру, для задач телеметрии на нефтегазодобывающих предприятиях, а также для контроля за перемещением персонала и транспортных средств в шахтах и рудниках, для определения нахождения персонала в аварийных ситуациях.

На рис. 1.2 представлена иллюстрация организации сети Wi-Fi.

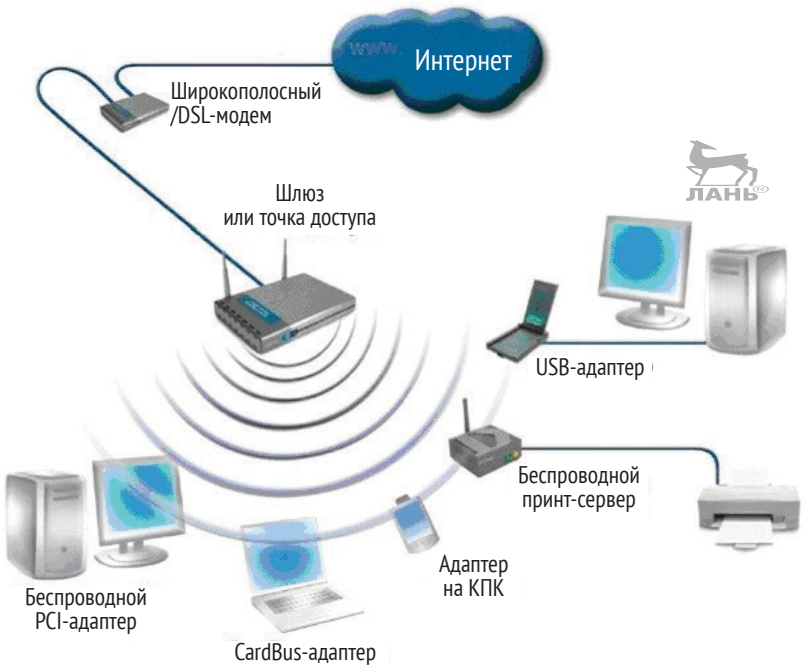

Рис.1.2. Организация сети Wi-Fi

Перспективно Wi-Fi и подобные ему технологии со временем могут заменить сотовые сети, такие как GSM. Препятствиями для подобного развития событий в ближайшем будущем являются отсутствие глобального роуминга, ограниченность частотного диа-

пазона и ограниченный радиус действия Wi-Fi. Более правильным выглядит сравнение сотовых сетей с другими стандартами беспроводных сетей, таких как UMTS, CDMA или WiMAX. Тем не менее Wi-Fi пригоден для использования VoIP в корпоративных сетях или в среде SOHO. Первые образцы оборудования появились еще в начале 2000-х, а 10 лет назад серийно вышли на широкий рынок. Тогда такие компании, как Zyxel, UT Starcomm, Samsung, Hitachi, и многие другие представили на рынок VoIP Wi-Fi-телефоны по «разумным» ценам. В те далекие годы ADSL ISP провайдеры начали предоставлять услуги VoIP своим клиентам (ISP XS4All). Когда звонки с помощью VoIP стали очень дешевыми, иногда бесплатными, провайдеры, способные предоставлять услуги VoIP, открыли новый рынок – услуг VoIP. Телефоны GSM с интегрированной поддержкой возможностей Wi-Fi и VoIP стали выводиться на рынок, и потенциально они планировались такими, чтобы заменить проводные телефоны. Но сегодня непосредственное сравнение Wi-Fi и сотовых сетей нецелесообразно по целому ряду причин. Телефоны, использующие только Wi-Fi, имеют очень ограниченный радиус действия, поэтому развертывание таких сетей обходится очень дорого. И тем не менее подобное развертывание может быть наилучшим решением для локального использования, к примеру в корпоративных сетях. Однако устройства, поддерживающие несколько стандартов, могут занять значительную долю рынка. При наличии в конкретном месте покрытия как GSM, так и Wi-Fi, экономически более выгодно использовать Wi-Fi, разговаривая посредством сервисов интернет-телефонии. К примеру, программное обеспечение – клиент Skype давно существует в версиях как для смартфонов, так и для КПК.

Всех пользователей Wi-Fi сегодня условно можно разделить на категории:

- linus – выделяющие бесплатный доступ в интернет;
- bills – продающие свой частотный диапазон;
- aliens – использующие доступ через bills.

Таким образом, система аналогична пиринговым сервисам. Несмотря на то что FON получает финансовую поддержку от таких компаний, как Google и Skype, лишь со временем можно уточнить, будет ли эта идея действительно работать.

У данного сервиса есть три основные проблемы. Первая заключается в том, что для перехода проекта из начальной стадии в основную требуется больше внимания со стороны общественности и СМИ. Нужно также учитывать тот факт, что предоставление доступа к интернет-каналу другим лицам может быть ограничено вашим договором с провайдером. Поэтому провайдеры пытаются защитить свои интересы. Так же поступят звукозаписывающие компании, выступающие против свободного распространения MP3, MP4 и других новейших стандартов.

Внимание, важно!

По ряду причин в России основное количество точек доступа сообщества FON расположено в Московском регионе. Посему говорить о распространении и какой-либо перспективе развертывания системы по всей стране, полагаю, преждевременно.

Wi-Fi совместим с игровыми консолями и КПК и позволяет вести сетевую игру через любую точку доступа или в режиме точка–точка. Все игровые консоли нового поколения имеют поддержку стандартов Wi-Fi IEEE 802.11g. Пока коммерческие сервисы пытаются использовать существующие бизнес-модели для Wi-Fi, многие группы, сообщества, города и частные лица строят свободные сети Wi-Fi, часто используя общее пиринговое соглашение, для того чтобы сети могли свободно взаимодействовать друг с другом, а также широко применяя возможности Wi-Fi в ограниченном пространстве для управления бытовыми приборами в системе интернета вещей, о чем я подробно расскажу в следующих главах.

Одна из конкретных возможностей – ячеистая сеть. Схема создания ячеистой сети (mesh-network) с использованием оборудования Wi-Fi предполагает следующие уточнения.

OLSR (en) – один из протоколов, используемых для создания свободных сетей. Некоторые сети используют статическую маршрутизацию, другие полностью полагаются на OSPF. В Израиле разрабатывается протокол WiPeer для создания бесплатных P2P-сетей на основе Wi-Fi. Несколько лет назад в Wireless Leiden разработали собственное программное обеспечение для маршрутизации под названием LVrouteD для объединения Wi-Fi-сетей, построенных на полностью беспроводной основе. Большая часть

сетей построена на основе ПО с открытым кодом или публикует свою схему под открытой лицензией (превращает любой ноутбук с установленной Mac OS X и Wi-Fi-модулем в открытый узел Wi-Fi). Также следует обратить внимание на netsukuku – разработку всемирной бесплатной mesh-сети.

Внимание, важно!

Любопытно, что во многих странах мира уже обеспечивают свободный доступ к хот-спотам Wi-Fi и доступ к интернету через Wi-Fi по месту жительства для всех. Такие системы работают и на транспорте. Свободный Wi-Fi можно «получить» на АЗС почти по всему миру, в том числе в России, в кафе, в университетах и некоторых основных школах, в метро, библиотеках и в других местах. Интересную особенность на этот счет я заметил в Финляндии, где в муниципалитетах имеют большое количество свободных хот-спотов Wi-Fi по всей территории страны. «Раздатчик» доступа Wi-Fi находится в здании администрации муниципалитета или в местной библиотеке, а зона его охвата составляет 1,5 км в радиусе. Это реальный пример в коммуне Раутьярви. Разумеется, жители и гости территории ничего не платят за пользование открытым доступом к глобальной сети, организованное таким образом. Услуга предоставляется за счет муниципалитета. «Минусом» данной и подобного рода организации является незащищенность доступа, то есть шифрование WEP сегодня настолько небезопасно, что его можно признать как вовсе открытый канал связи. Это значительно расширяет возможности использования системы интернета вещей хотя бы в части ее дистанционного управления.

Почему так происходит? Возможно, в данном случае провайдеры строят свободные хот-споты Wi-Fi и хот-зоны. Они считают, что свободный доступ привлечет новых клиентов и инвестиции вернутся.

Огромными возможностями такое решение обладает в части темы нашей книги, когда (рассмотрено в следующих разделах) с помощью развернутой сети Wi-Fi и планшета (КПК) можно осуществить дистанционное управление всем, чем угодно, в системе интернета вещей. Предостережения на этот счет также читайте далее.

1.11.3. Практические рекомендации

Подключите «адресный фильтр MAC». Каждый элемент Wi-Fi-оборудования имеет особый идентификатор, который называется физическим адресом, или адресом MAC. Маршрутизатор

Wi-Fi-оборудования хранит в себе MAC-адреса всех тех девайсов, которые подключены. Это означает, что конкретные устройства предлагают пользователю ту опцию в виде ключа в MAC-адресах оборудования, которая позволяет подключаться к сети только проверенным девайсам. Рассмотренная особенность защиты пользовательского оборудования не такая сильная и мощная: хакеры и их специальный софт с легкостью обманывают MAC-адреса. Так что эта защита работает только против начинающих любителей взлома… И тем не менее ограничивать MAC-адреса и отключать SSID малоэффективно. Для более опытных не является проблемой посмотреть сниффером IP и выставить правильный, аналогично и MAC-адреса, ETS.

Следующим шагом поменяйте дефолтные SSID. Маршрутизаторы для своей работы используют SSID (Service Set Identifier). Производители поставляют свое оборудование с одними и теми же настройками SSID. К примеру, SSID для Linksys часто будет означать и «linksys». Конечно, если кто-то и будет знать SSID, то это не будет означать, что сосед незамедлительно влезет в сеть, но это будет началом возможного процесса… Кому это надо?

Поэтому когда находится дефолтный вариант SSID, то хакер лишний раз убеждается, что пользователь данной Wi-Fi-сети является неопытным пользователем и в его систему можно вмешаться для управления его исполнительными устройствами в системе интернета вещей. Здесь нужно помнить одно: когда вы будете конфигурировать свою Wi-Fi-сеть, то незамедлительно поменяйте дефолтные SSID.

Отключите передачу SSID. Маршрутизатор в Wi-Fi обычно передает имя сети (SSID) в эфир через регулярные интервалы. Эта особенность была спроектирована для тех случаев и мобильных «горячих» портов, когда Wi-Fi-клиенты могут входить и выходить из зоны действия их собственной сети. Но у себя дома функция роуминга полностью бесполезна, и это все серьезнейшим образом повышает тот риск, что в вашем районе кто-то другой сможет воспользоваться всей сетью. Именно такая ситуация описана выше на основе практического опыта в Финляндской республике. Важно иметь в виду, что в большинстве Wi-Fi-маршрутизаторов есть особенность отключения данного роуминга через панель администратора.

Следующим шагом отключите автоматическое соединение, чтобы не подключаться через открытый Wi-Fi. Почему это важно?

Соединение через открытые Wi-Fi-«горячие» порты или через маршрутизатор потенциального соседа приведет к повышению риска собственного компьютера. Несмотря на то что в нормальном состоянии это не позволено, но все же все компьютеры имеют те настройки, которые позволяют подсоединяться к таким портам в автоматическом режиме, не уведомляя о том пользователя. Поэтому данную настройку следует отключить.

Установите статические IP на все девайсы. Большинство домашних Wi-Fi-линий использовало динамические IP-адреса. DHCP-технология в наше время является наилучшим решением по этой части. Однако не все так просто: именно это удобство позволяет хакерам перехватывать ваши сигналы, которые могут с легкостью получить статический IP из канала вашего DHCP.

Что же делать?

Как вариант следует отключить DHCP на пользовательском маршрутизаторе и поставить вместо него фиксированный IP; но затем также не стоит забывать сконфигурировать каждый девайс оборудования надлежащим образом. Другое дело, что не все провайдеры позволяют это сделать. Приходится выбирать... Как вариант используйте секретные IP-адреса (к примеру, 10.0.0x), чтобы предотвратить подключение компьютеров напрямую из интернета.

Активируйте Firewall'ы на каждом компьютере и на самом маршрутизаторе. Современные маршрутизаторы уже содержат в себе встроенные Firewall'ы, но всегда существует опция для их отключения. Убедитесь, что на маршрутизаторе Firewall включен. Для более существенной и дополнительной протекции следует инсталлировать персональный Firewall на каждый компьютер, который непосредственно соединен с самим маршрутизатором.

Местонахождение самого маршрутизатора и безопасность всей сети – следующий важнейший вопрос, который будет рассмотрен ниже. В нормальном состоянии (их сила) Wi-Fi-сигналы должны немного переходить границу дома, квартиры. Некоторое количество сигнала, которое утекает через ваш порог, – это нормально, но не есть хорошо, если сигнал уплывает и дальше: всегда есть вероятность перехвата вашего сигнала и его использование. Wi-Fi-сигналы частенько достигают соседних домов и далее, на улицу... И когда будете инсталлировать свою домашнюю Wi-Fi-систему, то следует помнить, что местонахождение самого

маршрутизатора играет не самую последнюю роль. Попробуйте найти ему место посередине комнаты, а не возле окна, что также позволит минимизировать утечку сигнала.

Выключайте свою линию, если не пользуетесь ею долгое время. И вот почему: еще одним решением является выключение сложного оборудования, когда вы вообще не пользуетесь им. Это резко снижает взлом и возможное несанкционированное управление вашими исполнительными устройствами в системе интернета вещей. Естественно, довольно непрактично выключать его очень часто, но во время своих путешествий и продолжительной отлучки (уехали в командировку) отключение оборудования является наилучшим выходом.

Диски компьютера не любят постоянный цикл: включение/выключение, но для широкополосных модемов и маршрутизаторов все это не так уж страшно. Если у пользователя есть всего один маршрутизатор на всю линию компьютеров (Ethernet), то имеет смысл отключить всего лишь широкополосный Wi-Fi-маршрутизатор вместо отключения всей компьютерной сети. Это поможет предохранить пользовательские компьютеры и информацию.

Проектирование Wi-Fi-сетей имеет свои особенности. Нередки такие случаи, когда после отключения трансляции SSID смартфон и планшет не могут к ней подключиться. Хотя при изменении настроек были в сети. Для этого есть функция – «подключиться к скрытой сети». Вводите свой пользовательский SSID и пользуйтесь.

1.12. Распределение Wi-Fi-сигнала в системе интернета вещей

Все возможные варианты реализации раздачи Wi-Fi с ноутбука или ПК, включая способы настройки стандартными средствами Windows 10, а также с помощью специализированных программ, рассмотреть в пределах одной книги невозможно, поэтому обратимся к наиболее популярным вариантам, прошедшим испытание временем.

Вариант № 1. Раздача Wi-Fi с помощью командной строки и встроенной команды `netsh` в ОС Windows 10.

Требования: компьютер 1, подключенный к интернету (LAN, Wi-Fi, 3G…), наличие Wi-Fi-модуля, установленная ОС Windows 7 и выше, а также компьютер 2 со встроенным Wi-Fi-модулем.

В этом случае относительно простая сеть (ad-hoc mode) в режиме точка–точка не подходит для соединения с устройствами, не поддерживающими работу с ad-hoc-сетями (к примеру, планшет либо телефон на базе OS Android).

Эта сеть используется в основном для обмена данными между ПК в отсутствие возможности использовать точку доступа. Суть метода состоит из нескольких практических шагов.

1. Открываем **Пуск → Панель управления → Центр управления сетями и общим доступом → Настройка общего подключения или сети**.
2. Выбираем **Настройка беспроводной сети компьютер–компьютер**, жмем **Далее**. Задаем на латинице имя сети и ключ безопасности, жмем **Далее**.
3. Открываем **Пуск → Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера**. Выбираем сеть с доступом в интернет и заходим в **Свойства**. Затем следует переход на вкладку **Доступ** и разрешающая команда к общему доступу. На другом компьютере ищем созданную нами сеть и подключаемся.

Вариант № 2. Раздача сигнала Wi-Fi с помощью командной строки и встроенной команды `netsh` Windows 10 для подключения сети компьютер–устройства с Wi-Fi.

Требования: компьютер 1, подключенный к интернету (LAN, Wi-Fi, 3G…), наличие модуля Wi-Fi, драйверы которого поддерживают Virtual Wi-Fi, установленная Windows 10 максимальная либо Windows 8 R2, второй ПК или (другие устройства) с наличием модуля Wi-Fi.

Этот вариант позволяет подключать устройства через точку доступа (Access Point-AP) на основе программной технологии Virtual Wi-Fi. В основе данной технологии реализуется программная точка доступа (Software Access Point – SoftAP), к которой можно подключить ноутбук, телефон (поддерживается OS Android), фотоаппарат, принтер и другие девайсы.

1. Нажимаем **Пуск**, в строку поиска вводим **cmd**, открываем командную строку от имени администратора.
2. Вводим в командную строку следующую команду:
   `netsh wlan set hostednetwork mode=allow ssid="HomeWi-Fi" key="123qwe123456" keyUsage=persistent`

   где:

   `ssid="HomeWi-Fi"` SSID – идентификатор сети (имя сети), в нашем примере: **HomeWi-Fi**;

   `key="123qwe123456"` – ключ безопасности (пароль), в нашем примере: **123qwe123456**.

   Далее нажимаем **Ввод**.
3. Затем запускаем сеть командой (также вводим в командную строку) `netsh wlan start hostednetwork`, после чего в списке сетевых подключений видна вновь созданная сеть **HomeWi-Fi**.

Для того чтобы предоставить доступ в интернет другим устройствам, подключаемым к созданной сети, необходимо выполнить «Шаг 3», описанный в варианте № 1.

В варианте № 2 присутствует особенность, заключающаяся в том, что при выключении раздающего ноутбука или ухода в сон запуск сети из командной строки необходимо будет выполнять снова. Чтобы это не делать каждый раз, просто скачайте startWi-Fi.bat-файл и перетащите его в **Пуск → Все программы → Автозагрузка**.

Таким образом мы настроили раздачу Wi-Fi с ноутбука на другие устройства.

Внимание, важно!

Нелишним будет приобрести автономную Wi-Fi-точку доступа, которая избавит пользователя от множества проблем с подключением различных устройств. При недостаточном уровне сигнала используйте внешнюю Wi-Fi-антенну с большим коэффициентом усиления.

Вариант № 3. Раздача Wi-Fi при помощи программы для раздачи Wi-Fi с ноутбука.

Требования: согласно варианту № 2.

Такой вариант реализует возможность создания точки доступа на основе варианта № 2, используя лишь графические оболочки программ. В свободном доступе имеется огромное количество программ для раздачи Wi-Fi с ноутбука или ПК, поэтому описывать настройку каждой нет смысла.

1.13. Особенности Wi-Fi-маршрутизаторов

Сегодня роутер – одно из самых популярных устройств среди пользователей интернета. Рынок предлагает широкую линейку роутеров на любой вкус. Какой роутер лучше выбрать для домашнего пользования? На этот вопрос дать однозначный ответ довольно трудно. Различные типы роутеров, основные факторы, на которые необходимо обратить внимание при выборе домашнего Wi-Fi-модема, – все это те важные аспекты, без которых правильный выбор затруднен.

1.13.1. Варианты выбора и технические характеристики оборудования

Роутер или (иначе) маршрутизатор – это устройство, с помощью которого компьютер, смартфон, планшет или другое оборудование объединяются в общую беспроводную сеть, а затем соединяются с интернетом. Маршрутизаторы практически одинаковы, а соответственно, если нет разницы, то зачем платить больше. Но в действительности подобное рассуждение является широко распространенным заблуждением.

Относительно дешевые роутеры комплектуются более дешевыми компонентами, имеющими меньший срок службы, заниженные показатели ключевых параметров и т. д. Даже среди проверенных брендовых моделей встречаются модемы, не всегда отличающиеся хорошим качеством. Так, к примеру, широко известен бренд D-Link, выпускающий большое количество бюджетных модемов. Однако в его линейке далеко не все маршрутизаторы могут похвастаться безупречным качеством и надежной работой. В отличие от D-Link, очень хорошие и высокоскоростные роутеры выпускаются под брендом Linksys. Но за качество, предоставляемое этим брендом, придется заплатить существенно большую сумму.

По авторской практике Zyxel (не имелась в виду реклама ни одного производителя) не самые дешевые роутеры, но обладающие высочайшим качеством и надежностью и TP-Link (производство недорогих, но очень качественных модемов). Какой Wi-Fi-роутер лучше приобрести для дома, решать пользователю, но перед принятием решения безусловно необходимо обратить внимание на технические характеристики модемов.

1.13.2. Минимальные современные требования к функционалу

Первое, на что необходимо обратить внимание, – это оперативная память модема; чем она выше – тем лучше. Кроме этого, следует обратить внимание на мощность модема и количество имеющихся антенн. Далее стоит взглянуть на протоколы, поддерживаемые модемом (PPTP, L2TP, PPPoE). Главное, чтобы он поддерживал тот протокол, который будет использовать пользовательский провайдер. Сегодня высокоскоростные роутеры поддерживают большинство используемых протоколов. Кроме этого, роутеры различаются WAN-портом, с помощью которого происходит подключение к сети: Ethernet, ADSL, USB 3G.

Стандарт Wi-Fi 802.11n поддерживает максимальную скорость подключения, в отличие от стандартов 802.11b или 802.11g. Ниже представлены три модема, имеющих различные типы подключения к сети: роутер с ADSL-портом, роутер с Ethernet-портом, USB-порт. Первый вариант сегодня встречается довольно редко, разве что в таких организациях, как Ростелеком.

Итак, современный роутер должен поддерживать такие возможности и иметь следующие (минимальные) характеристики:

WAN-порт:	Ethernet, USB 3G, 4G
Наличие интерфейсов:	RJ-45 (10BASE-T/100BASE-T) – 5 портов; USB 2.0 тип A – 1 разъем; RP-SMA (подключение внешних антенн Wi-Fi) – 2, 3 розетки
Стандарты беспроводной сети:	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Поддерживаемые протоколы:	PPTP, L2TP, PPPoE
Поддержка IPTV:	есть

Функции безопасности:	наличие встроенного межсетевого экрана (SPI) с защитой от DoS- и DDoS-атак. Возможность блокировки доступа в интернете по MAC-адресу, IP-адресу, URL, TCP/UDP-порту
Функции брандмауэра:	наличие встроенного межсетевого экрана, NAT
Дополнительные функции:	возможность подключения хотя бы 4G-модема и максимальный радиус сигнала до 300 м

Внимание, важно!

При этом лучший роутер – тот, у которого существует достаточный запас по мощности. Не забывайте также о том, что скорость передачи Wi-Fi через роутер, каким бы «навороченным» он ни был, все одно будет меньше, чем при подключении кабеля интернет-провайдера к ПК напрямую. Таким образом, передача по Wi-Fi для бытового пользователя представляет собой лишь некое комфортное времяпрепровождение. О вопросах безопасности для здоровья и информационной безопасности – по этой теме – мы поговорили выше. Поэтому в этой книге мы рассматриваем разные возможности подключения устройств в системе интернета вещей и – во второй главе – способы управления по этой сети в системах интернета вещей, и тем не менее это далеко не лучший способ организации связи именно в бытовых условиях, где люди находятся большую часть дня, в том числе принимают пищу и спят.

О внешней блокировке управления исполнительными устройствами

Существует несколько способов блокировки Wi-Fi-сетей, и чем слабее роутер (мощность его сигнала), тем легче блокировать. В быту для этой цели достаточно применить простейшие «глушилки» из КНР, к примеру те, что описаны в [5].

1.14. Программная совместимость оборудования в интернете вещей

Примерно с 1998 года операционные системы (далее – ОС) семейства BSD (FreeBSD, NetBSD, OpenBSD) работают с большинством адаптеров. Драйверы для чипов Atheros, Prism, Harris/

Intersil и Aironet (от соответствующих производителей Wi-Fi-устройств) обычно входят в ОС BSD начиная с версии 03. Адаптеры производства Apple OS X (прежнее название – Mac OS X) поддерживались изначально с системы Mac OS 9. Примерно 20 лет прошло с тех пор, как все настольные компьютеры и ноутбуки Apple Inc. (и телефоны iPhone, плееры iPod Touch, планшетные компьютеры iPad) штатно оснащаются адаптерами Wi-Fi, сеть Wi-Fi, таким образом, является основным решением Apple для передачи данных и полностью поддерживается OS X. Возможен режим работы адаптера компьютера в качестве точки доступа, что позволяет при необходимости связывать компьютеры Macintosh в беспроводные сети в отсутствие инфраструктуры. Darwin и OS X, несмотря на частичное совпадение с BSD, имеют свою собственную, уникальную реализацию Wi-Fi.

В ОС семейства Microsoft Windows поддержка Wi-Fi обеспечивается, в зависимости от версии, либо посредством драйверов, качество которых зависит от поставщика, либо средствами самой Windows. Про Microsoft Windows XP поддерживающую настройку беспроводных устройств говорить не стану, поскольку устарела. Она включала в себя довольно слабую поддержку, но значительно улучшилась с выходом Service Pack 2, а с выходом Service Pack 3 была добавлена поддержка WPA2. Microsoft Windows Vista содержит улучшенную, по сравнению с Windows XP, поддержку Wi-Fi. Microsoft Windows от 7 версии и выше поддерживает все беспроводные устройства и протоколы шифрования. В ОС Windows 7 и 8 уже создана возможность создавать виртуальные адаптеры Wi-Fi, что теоретически позволяет подключаться не к одной Wi-Fi-сети, а к нескольким сразу. На практике в Windows 10 также поддерживается создание только одного виртуального адаптера при условии написания специальных драйверов, что полезно при использовании компьютера в локальной Wi-Fi- и одновременно в Wi-Fi-сети, подключенной к глобальной сети интернет.

1.15. Легитимное использование интернета вещей в беспроводной сети

В России легитимное использование Wi-Fi регулируется правилами и требованиями, выработанными Роскомнадзором. В соответствии с решениями Государственной комиссии по радиочас-

тотам (ГКРЧ) от 7 мая 2007 г. № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия» и от 20 декабря 2011 г. № 11-13-07-1 использование Wi-Fi без получения частного разрешения на использование частот возможно для организации сети внутри зданий, закрытых складских помещений и производственных территорий в полосах 2400–2483,5 МГц (стандарты 802.11b и 802.11g; каналы 1–13) и 5150–5350 МГц (802.11a и 802.11n; каналы 34–64). Для легального использования внеофисной беспроводной сети Wi-Fi (к примеру, для радиоканала между двумя соседними домами) необходимо получение разрешения на использование частот (как в полосе 2,4 ГГц, так и 5 ГГц) на основании заключения экспертизы о возможности использования заявленных РЭС и их электромагнитной совместимости (ЭМС) с действующими и планируемыми для использования РЭС.

Радиоэлектронные средства подлежат регистрации в Роскомнадзоре в соответствии с установленным порядком, см. постановление № 539 – порядок регистрации РЭС. В соответствии с постановлением Правительства Российской Федерации от 13 октября 2011 г. № 837 «О внесении изменений в постановление Правительства Российской Федерации от 12 октября 2004 г. № 539» не подлежат регистрации, в частности (из пп. 13, 23, 24 приложения):

- пользовательское (оконечное) оборудование передающее, включающее в себя приемное устройство, малого радиуса действия стандартов IEEE 802.11, IEEE 802.11.b, IEEE 802.11.g, IEEE 802.11.n (Wi-Fi), работающее в полосе радиочастот 2400–2483,5 МГц, с допустимой мощностью излучения передатчика не более 100 мВт, в том числе встроенное либо входящее в состав других устройств;
- пользовательское (оконечное) оборудование передающее, включающее в себя приемное устройство, малого радиуса действия стандартов IEEE 802.11a, IEEE 802.11.n (Wi-Fi), работающее в полосах радиочастот 5150–5350 МГц и 5650–6425 МГц, с допустимой мощностью излучения передатчика не более 100 мВт, в том числе встроенное либо входящее в состав других устройств;
- устройства малого радиуса действия, используемые внутри закрытых помещений, в полосе радиочастот 5150–5250 МГц

с максимальной эквивалентной изотропно излучаемой мощностью передатчика не более 200 мВт;
- устройства малого радиуса действия в сетях беспроводной передачи данных внутри закрытых помещений в полосе радиочастот 2400–2483,5 МГц с максимальной эквивалентной изотропно излучаемой мощностью передатчика не более 100 мВт при использовании псевдослучайной перестройки рабочей частоты.

Кстати, даже для дистанционного управления различными моделями используется два участка диапазона 35 и 40 МГц, причем в диапазоне 40 МГц каналы для управления наземными и летающими моделями совпадают, а диапазон 35 МГц предназначен только для управления летающими моделями. Сетка частот имеет шаг 10 КГц, начинается с частоты 35,0000 МГц и заканчивается частотой 35,3000 МГц. Каналам присвоены номера с 60 по 90. В диапазоне 40 МГц шаг также равен 10 КГц, начинается с частоты 40,665 МГц и заканчивается частотой 40,985 МГц. Номера каналов соответственно с 50 по 92. К примеру, во Франции для этой же цели используется участок диапазона 41,0000–41,2000 МГц, каналы начинаются с «нулевого» и заканчиваются «двадцатым». Для модуляции используется узкополосная ЧМ с девиацией 2,5 кГц. Кодирование информации производится изменением длительности канального импульса относительно средней его величины, примерно равной 1500 мс. Эта длительность может несколько отличаться у разных производителей аппаратуры (Graupner, Futaba/Hitec, Multiplex, JR/Airtronix). Для уменьшения ширины спектра излучаемого передатчиком сигнала производится искусственный завал фронтов управляющих импульсов на входе модулятора. До недавнего времени использовались две несовместимые системы передачи управляющей информации: PPM и QPCM. У каждой из них есть свои достоинства и недостатки. В последнее время эти системы активно вытесняются с рынка передатчиками, работающими в диапазоне частот 2,4 ГГц и имеющими полностью цифровой протокол передачи данных.

Юридический статус Wi-Fi различен в разных странах. В США диапазон 2,5 ГГц разрешается использовать без лицензии, при условии что мощность не превышает определённую величину, и такое использование не создаёт помех тем, кто имеет лицензию. В разных странах мира существуют определенные требования

к организации сетей Wi-Fi и безопасности доступа пользователей. К примеру, в Украине использование Wi-Fi без разрешения Украинского государственного центра радиочастот возможно лишь в случае использования точки доступа со стандартной всенаправленной антенной (< 6 дБ, мощность сигнала ≤ 100 мВт на 2,4 ГГц и ≤ 200 мВт на 5 ГГц) для внутренних (использование внутри помещения) потребностей организации (решение Национальной комиссии по регулированию связи Украины № 914 от 06.09.2007). В случае использования внешней антенны необходимо регистрировать передатчик и получить разрешение на эксплуатацию радиоэлектронного средства от ДП УДЦР. Кроме того, для деятельности по предоставлению телекоммуникационных услуг с применением Wi-Fi необходимо получить лицензию от «НКРЗІ». В Белоруссии действует специализированная Государственная комиссия по радиочастотам (ГКРЧ). На основе постановления Министерства связи и информатизации Республики Беларусь от 26.08.2009 № 35 «Перечень радиоэлектронных средств и (или) высокочастотных устройств, не подлежащих регистрации» оборудование Wi-Fi не требует регистрации, при условии что его параметры удовлетворяют следующим требованиям: абонентские станции широкополосного беспроводного доступа, использующие полосы радиочастот 2400–2483,5 МГц, 2500–2700 МГц, 5150–5875 МГц и не использующие внешних антенн (антенн, устанавливаемых вне зданий и сооружений), а также абонентские станции широкополосного беспроводного доступа сети электросвязи общего пользования, использующие полосы радиочастот 3400–3800 МГц, 5470–5875 МГц.

Глава 2

ВИДЕОКАМЕРЫ И ДИКТОФОНЫ В СИСТЕМЕ ИНТЕРНЕТА ВЕЩЕЙ

В этой главе поговорим о принципах и практических примерах подключения видеокамер в системе интернета вещей, рассмотрим несколько моделей камер и снабдим описание простыми и понятными иллюстрациями.

2.1. Особенности разных моделей камер и диктофонов в системе интернета вещей

2.1.1. C11S мини-DVR-камера 1080P Full HD

Мини-DVR-камера 1080P Full HD имеет также диктофон с инфракрасной Wi-Fi-камерой с передачей сигнала на мобильный телефон или иное оборудование пользователя. Внешний вид устройства представлен на рис. 2.1.

Рис. 2.1. Внешний вид C11S мини-DVR-камеры 1080P Full HD

Технические характеристики

Объем встроенной памяти:	4 Гб
Формат записи:	WAV сбалансированный
Форматы воспроизведения:	WAV

Внешний микрофон:	имеется
Размеры (Ш×В×Г), мм:	11,5×2,5×1,4
Система поддержки Wi-Fi:	iOS 6.1 и выше, Android 4.0 и выше
Операционная система:	Windows ME/2000/XP/2003/ Vista/Win7–Win10; Mac OS 10.4
Тип батареи:	Li-ion-батарея высокого качества
Функция Wi-Fi:	передача изображения и управления
Дополнительно:	голосовая активация; встроенный динамик; возможность подключения внешней памяти; пульт дистанционного управления

Особенность устройства в том, что оно функционально может быть использовано как HD-диктофон с управлением по Wi-Fi. Уникальный дизайн внешнего вида, внешний слот для карт TF, возможности скрытого ношения и эксплуатации HD-камеры с разрешением 1080P, в формате HD MOV с кодированием H.264, записывает аудио и видео одновременно. При этом разрешение видео составляет 1920×1080 30 кадров/с, 1280×720 – 60 кадров/с. Разрешение фото: 4032×3024 точек на дюйм. То есть полное HD 1080P с выходом HDMI.

Настройка

Нажмите кнопку **POWER** для включения видеорегистратора (загорятся синий и красный диоды, когда красный погаснет, а синий останется все время гореть – устройство готово к работе).

Нажмите кнопку «записи/остановки» (находится на верхней части устройства), чтобы начать запись видео (красный диод начнет медленно мигать).

Нажмите еще раз кнопку «записи/остановки», чтобы закончить запись видео (красный диод быстро мигнет 3 раза).

Кнопка **MODE** переключает режимы записи:

- обычный режим записи видео;
- звуковой режим записи видео.

Нажмите кнопку **MODE** (красный диод начнет быстро мигать – устройство в звуковом режиме записи).

Когда звук превысит 60 дБ, устройство автоматически начнет запись видео. Длительность записи 2 мин, если через 2 мин будет тишина, то устройство сохранит записанный файл. Если будет звук, то запись будет продолжаться.

Для настройки даты и времени необходимо создать в корневом каталоге карты памяти файл с именем TAG формата txt. В этом файле необходимо указать дату и время, например 2019/02/23, время должно быть написано с новой строки, к примеру 13:00:00.

Сохраните этот файл, при запуске устройство запомнит дату и время.

Если устройство включено и в течение 45 с не происходит никаких действий, то оно автоматически выключится для сбережения энергии.

Устройство можно использовать как веб-камеру. Для этого установите драйвер с диска. Установочный файл называется SPCA1528_V2220_MSetup.exe. После установки на рабочем столе появится иконка Amcap. Подключите устройство через USB-кабель, нажав кнопку **MODE**, перейдите в режим веб-камеры. Запустите Amcap и можете использовать устройство как веб-камеру.

На рис. 2.2 представлен вид Wi-Fi-камеры, закрепленной на штативе.

Рис. 2.2. Вид камеры на штативе в режиме эксплуатации

На рис. 2.3 представлен вид камеры со стороны кнопок управления.

Рис. 2.3. Вид камеры со стороны кнопок управления

2.2.2. Цифровой диктофон IDV Wi-Fi IP P2P HD Pen Recorder Mini Wi-Fi 1080P

Внешний вид устройства представлен на рис. 2.4.

Рис. 2.4. Внешний вид цифрового диктофона IDV Wi-Fi IP P2P HD

Технические характеристики

Внутренняя память:	1 Гб
Формат видео:	MP4
Изображение:	H.264

Разрешение видео:	1920×1080 30 снимков/с
Формат камеры:	JPG
Поддержка Wi-Fi:	iOS 6.1 выше
Система:	Android 4.0
Носитель информации:	микро-SD максимум 128 Гб с поддержкой SD TF
Функции Wi-Fi:	передача изображения, имеется пульт дистанционного управления
Длина световой волны:	940 нм
Инфракрасный объектив (мм):	3.6
Формат камеры:	JPG
Система поддержки:	Windows ME/2000/XP/Win7–10 Mac OS 10.4
Зарядное напряжение:	DC 5 В
Средство интерфейса:	мини-USB «5 штырей»
Тип батареи:	Li-ion, емкость 560 мА
Размер (Ш×В×Г), мм:	115×25×14

Особенности устройства – соединение IP P2P Wi-Fi поддержки и запись голоса, позволяет реально дистанционно контролировать запись голоса и видео через телефон с системой Android 4.0 или iOS с поддержкой Wi-Fi: iOS 6.1 и выше.

2.1.3. Wi-Fi-диктофон Olympus DM-7

Диктофон Olympus DM-7 оборудован Wi-Fi-модулем, что позволяет управлять диктофоном дистанционно. С помощью нового бесплатного приложения от Olympus для устройств на базе iOS или Android можно делиться файлами или выгружать их в Dropbox. Функция «Визуальный индекс» позволяет связать фотографии, сделанные во время записи, с аудиофайлами и, используя их в качестве индексных меток, выделить особенно значимые места. Кроме того, устройство имеет 2-дюймовый цветной ЖК-дисплей с высоким разрешением и интуитивным меню, голосовое управление с функцией распознавания текста, а также поддержку формата аудиокниг Daisy.

Устройство представлено на рис. 2.5.

Наиболее совершенная модель DM-7 представляет собой цифровой диктофон нового поколения и свидетельство приверженности производителя к передовым технологиям. Впервые обору-

дованный модулем Wi-Fi, он помогает организовать запись звука. Подключение к смартфону осуществляется через Wi-Fi и позволяет удаленно управлять диктофоном, благодаря чему достигается наилучшее качество записи, кроме того, пользователь может делать фотографии на смартфоне и прикреплять их к временной шкале как визуальные указатели. Наилучшее качество записи гарантировано расположенными под углом 90° стереомикрофонами с низким уровнем шума, которые могут записывать звук со всех направлений. Переработанный пользовательский интерфейс стал наглядным благодаря цветному экрану, графическим иконкам и интуитивному дизайну, а также удобнее за счет функции прокрутки. Максимальное удобство использования достигнуто внедрением поддержки голосовых команд для управления диктофоном, а функция TexttoSpeech преобразования текста в голос получила поддержку форматов txt, html, doc.

Рис. 2.5. Внешний вид диктофона Wi-Fi модели Olympus DM-7

Общие и технические характеристики

Тип диктофона	цифровой
Производитель	Olympus, модель – DM-7
Поддержка карт памяти	SD
Тип памяти	встроенная и внешняя
Объем встроенной памяти	4 Гб, возможно использование в качестве Flash-накопителя данных
Поддержка форматов	MP3, WMA, WAV
Дисплей	
Тип дисплея	ЖК
Дисплей	2" (дюйма)
Разрешение дисплея	176×220 пикс.
Интерфейсы	
USB	2.0
Выход	аудио/наушники
Вход микрофонный	есть
Подключение к компьютеру	есть
Мультимедиа	
Встроенные динамики	есть
Мощность динамика мВт	280
Моно/Стерео	стерео
Запись	
Формат записи	MP3, PCM, WMA
Диапазон частот записи	40–13 000 Гц
Функция активизации по голосу	есть
Изменение чувствительности микрофона	есть
Запись с разным качеством	есть
Максимальное время записи	850 часов
Количество папок	5
Питание	
Тип элементов питания	Li-ion 1 шт.
Запись по таймеру	есть
Индикатор оставшегося времени записи	есть
Индикатор заряда батареи	есть
Зарядка от USB	есть

Дополнительно	
Диаметр динамика	20 мм
Конструкция	
Материал корпуса	металл
Ширина	51 мм
Высота	115 мм
Толщина	17 мм
Вес	105 г

2.1.4. Wi-Fi-диктофон Olympus DM-901

Компания Olympus выпускает диктофон DM-901 в продолжение бизнес-серии DM. Отличительной особенностью является поддержка сетей Wi-Fi, которая позволяет производить удаленное управление диктофоном со смартфона или планшета. Благодаря функции «визуальный индекс» можно использовать фотографии, снятые на смартфон или планшет во время записи, в качестве меток, связав их с аудиофайлами, чтобы выделить самую важную информацию. С помощью бесплатного приложения для Android или iOS можно получить доступ к индексным меткам через смартфон или планшет, чтобы затем быстро найти необходимые отрезки записи. Также приложение позволяет загрузить необходимые файлы с диктофона на смартфон, а затем переслать их или выложить в Dropbox. Связь посредством Wi-Fi осуществляется в формате P2P, а непосредственно передача файлов – через специального клиента на Android 4.0 и выше.

Внешний вид устройства представлен на рис. 2.6.

Общие и технические характеристики

Частотный диапазон при записи	
в формате MP3 256 Кбит/с	40 Гц – 20 кГц
в формате MP3 128 Кбит/с	40 Гц – 17 кГц
в формате PCM 48 кГц	40 Гц – 23 кГц
в формате PCM 44.1 кГц	40 Гц – 21 кГц
в режиме WMA HQ	40 Гц – 13 кГц
в режиме WMA LP	40 Гц – 3 кГц
Режимы записи:	собрание, конференция, лекция, диктовка, распознавание речи
Кнопки:	режим записи, громкость, 3 программируемые кнопки

Рис. 2.6. Внешний вид диктофона DM-901

Битрейт и частота
- PCM: 44.1–48 кГц / 16 бит
- MP3: 44.1 кГц / 128–256 Кбит/с
- WMA: 8–44.1 кГц / 8–32 Кбит/с

Динамик: встроенный, диаметром 20 мм, мощностью 280 мВт

Микрофон: встроенный

Flash-память: встроенная 4 Гб. Поддерживает 5 папок для диктофонных записей; до 999 файлов в папке

Продолжительность записи
- в режиме WMA LP: 850 ч
- в режиме WMA HQ: 218 ч

в формате MP3 128 Кбит/с:	55 ч
в формате MP3 256 Кбит/с:	27.5 ч
в формате PCM 44.1 кГц/16 бит:	5 ч
в формате PCM 48 кГц:	4.6 ч
Голосовая активация записи:	есть
Стандарты Wi-Fi:	IEEE 802.11g, IEEE 802.11b
Поддерживаемые карты памяти:	SDXC, SDHC, SD до 64 Гб
Разъем:	3.5 мм для подключения наушников, разъем 3.5 мм для подключения микрофона, USB 2.0
Питание:	Li-ion-аккумулятор 3.7 В
Емкость аккумулятора:	925 мА/ч
Ресурс аккумулятора:	29 ч записи в режиме WMA LP или 29 ч воспроизведения WMA LP через наушники
Поддержка ОС:	Windows 8/7/Vista/XP, MAC OS X
Язык меню:	русский
Размеры (Ш×В×Г), мм:	51×115×18
Вес:	105 г
Дополнительно:	поддерживается дистанционное управление записью со смартфона по Wi-Fi

2.1.5. Профессиональный цифровой диктофон Edic-mini Tiny B21

Профессиональный цифровой диктофон Edic-mini Tiny B21 – рекордсмен Книги рекордов Гиннесса. В нем сконцентрировано все, что нужно для работы, и ему не требуется подключение никаких вспомогательных устройств и аксессуаров. Встроенный микрофон обладает чувствительностью до 9 м, автономность устройства до 60 ч (при использовании воздушно-цинковых батарей). Отличительные особенности устройства представлены далее:

- размер: 40×15×8 мм;
- вес: 6 г (без батарейки);

- время работы в режиме записи: до 60 ч;
- встроенный объем памяти: от 300 до 1200 ч.

Внешний вид устройства показан на рис. 2.7.

Рис. 2.7. Внешний вид миниатюрного цифрового диктофона Edic-mini Tiny

Особенности модели

Edic-mini Tiny B21 – первый диктофон в семействе нескольких родственных моделей, которое развивается по сей день. Модель B21, разработанная в 2007 году, проста и лаконична, как и положено классике, легка и мала, но при этом сочетает все необходимые характеристики профессионального устройства. Диктофон выпускается в нескольких цветах, что дает возможность сделать выбор, наиболее соответствующий вкусу конкретного пользователя. Благодаря миниатюрным размерам и малому весу (всего 6 г) это электронное устройство удобно носить с собой постоянно: оно не мешает движениям ни в кармане брюк, ни в маленькой сумочке. При этом всегда готово к работе и поможет не упустить важные жизненные ситуации, зафиксировав их.

Основное достоинство Edic-mini Tiny B21 в том, что этот диктофон исключительно прост в эксплуатации. Для работы он не требует подключения никаких дополнительных аксессуаров и даже не имеет для этого соответствующих разъемов, что позволяет ему оставаться компактным и легким.

Назначения клавиш в кратком формате представлено на рис. 2.8.

Рис. 2.8. Назначение клавиш диктофона Edic-mini Tiny

На рис. 2.9 представлена принципиальная электрическая схема миниатюрного диктофона.

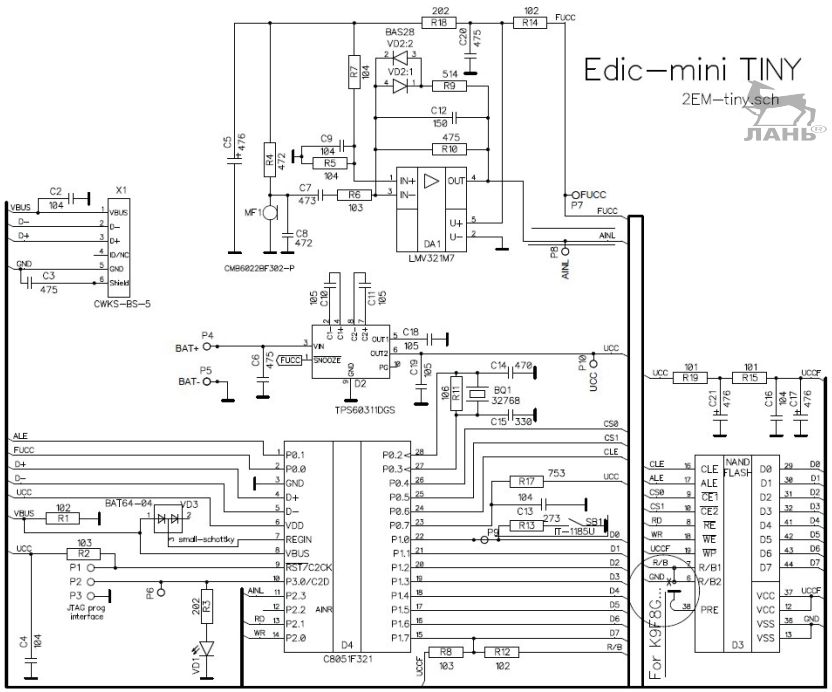

Рис. 2.9. Принципиальная электрическая схема миниатюрного диктофона Edic-mini Tiny

Профессиональный цифровой диктофон Edic-mini Tiny B21 оснащен микрофоном высокой чувствительности (позволяющим качественно записывать звук с расстояния до 9 м), что обеспечивает профессиональное качество записи до 600 ч. Устройство имеет 4 режима сжатия, голосовую активацию, таймер включения в назначенное время и цифровую подпись созданного файла.

На рис. 2.10 представлена монтажная схема диктофона.

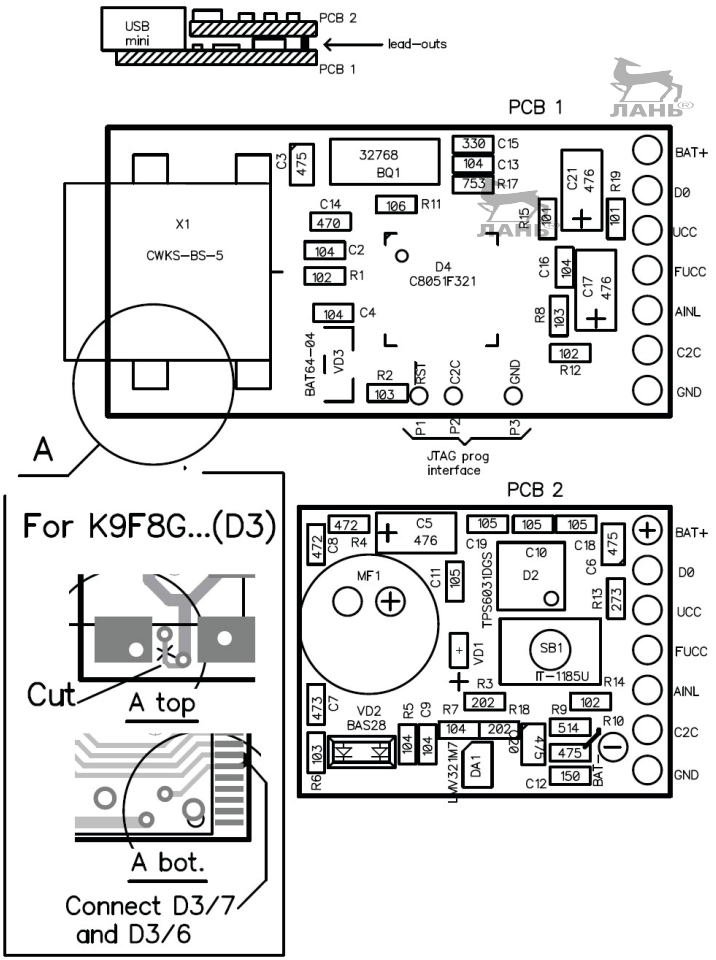

Рис. 2.10. Иллюстрация монтажной схемы профессионального диктофона Edic-mini Tiny

Два элемента питания типа AG13 (диаметр 11.6×5.4 мм) в устройстве меняются за считанные секунды, поэтому не придется тратить время на зарядку аккумулятора, и пользователь не будет зависеть от того, заряжен аккумулятор или нет. Готовясь к важному мероприятию, уместно взять в запас пару новых элементов питания, и тогда цифровой диктофон проработает столько, сколько нужно; вы сможете вести запись до тех пор, пока не кончится свободная память в диктофоне.

Внимание, важно!

Перед сменой батарейки диктофон необходимо обязательно выключить, иначе можно испортить файл текущей записи или повредить память.

Комплект поставки

- Цифровой диктофон
- USB-кабель
- 2 элемента питания (AG13 d 11.6×5.4 мм)
- Краткая инструкция по эксплуатации

Дополнительные аксессуары для диктофонов серии Edic-mini Tiny: выносной микрофон с компрессором (±6 дБ), программируемый выносной микрофон с АРУ (Edic-mini Tiny, Tiny16).

Технические характеристики устройства

Габаритные размеры:	40×15×8 мм
Вес:	6 г (без батареек)
Материал корпуса:	пластик (черного, серого или красного цвета)
Источник записи:	встроенный микрофон
Воспроизведение записей:	через ПК
Подключение к ПК:	USB 1.1 (до 0.7 МБайт/с)
Индикатор работы:	светодиод
Управление:	1 кнопка
Режим записи:	моно
Формат аудиофайла после конвертации:	WAV
Аудиокодек:	10-разрядный

Способ сжатия:	без сжатия; u-Law; ADPCM 4-битный; ADPCM 2-битный
Частоты дискретизации:	5,5 кГц; 8 кГц; 11 кГц, 16 кГц, 22 кГц
Встроенное усиление:	отсутствует
Температура эксплуатации:	от 0 до +40 °С

Память

Носитель информации:	встроенная Flash-память
Объем памяти в часах (8 кГц, в 2-битном ADPCM):	300 ч (2 Гб)

Питание

Источник питания:	батарейка типа G13-A (или LR44 – алкалиновая; Pr44, Za675 – воздушно-цинковая)

Время работы от элемента питания

В режиме записи (частота дискретизации: 8 кГц, без сжатия):	от батарейки G13-A до 10 ч, от воздушно-цинковой батарейки до 60 ч
В режиме записи с VAS, при акустическом сигнале ниже порогового:	от батарейки G13-A до 40 ч, от воздушно-цинковой батарейки до 240 ч
В дежурном режиме	до 2 месяцев

Частотные характеристики

Чувствительность встроенного микрофона:	до 9 м
Отношение сигнал/шум:	–64 дБ
Полоса пропускания при записи:	100–10 000 Гц

Дополнительные функции

Система голосовой активации VAS

Защита записи паролем

Таймер ежедневный и однократный

Возможность использовать в качестве Flash-диска

Линейная или кольцевая запись

Система цифровых маркеров (для определения несанкционированного редактирования записи)

Речь идет о самом маленьком в мире диктофоне, что зафиксировано отдельным свидетельством в Книге рекордов Гиннеса (см. рис. 2.11).

Рис. 2.11. Иллюстрация самого маленького в мире диктофона

Цифровые записи, сделанные на диктофонах Edic-mini Tiny, защищены от подделки специально разработанной системой цифровых маркеров. Передача информации в новых версиях может проходить по Wi-Fi, что вполне соответствует работе в системе интернета вещей.

Внимание, важно!

Для реализации этого свойства необходима прошивка версии не ниже 11.1. Информацию о ней можно посмотреть с помощью встроенной программы RecManager в окне **Проводник**, кнопка **Свойства файла**.

Что такое прошивка? Это встроенная программа, по которой работает цифровое устройство. Прошивка хранится в энергонезависимой памяти диктофона. Необходимо ли обновлять прошивку или RecManager? Если диктофон работает корректно и исполь-

зуемое программное обеспечение вас полностью устраивает, прошивку и RecManager менять не обязательно. Исключения составляют те случаи, когда фирмой-производителем обнаружены критические ошибки в существующем ПО, однако со временем меняются требования потребителей к функциональности выпускаемой продукции. Учитывая замечания и рекомендации клиентов, фирма дорабатывает и обновляет ПО к наиболее востребованным изделиям, расширяя тем самым их функциональные возможности.

Маркеры – это незаметные для пользователя опознавательные знаки, которые проходят через всю запись и позволяют определить целостность записанной речевой информации. С помощью этих знаков можно выяснить модель диктофона, на котором была сделана запись, его серийный номер, дату и время начала записи, а также была ли предпринята попытка ее модификации.

Работа с таким диктофоном – важный шаг для более широкого применения цифровой записи в качестве доказательства в суде, который дает возможность использовать диктофон как неподкупного свидетеля, который точно и объективно зафиксирует на электронный носитель все разговоры и звуки в радиусе 9–12 метров, сохранит их на любое время и никогда не изменит показания в суде.

Режимы записи

С помощью диктофонов Edic-mini Tiny можно вести как линейную, так и кольцевую запись. В режиме линейной записи количество и длительность сообщений ограничены объемом свободной памяти. Кольцевой способ позволяет не останавливать запись. Когда в диктофоне заканчивается свободная память, диктофон просто начинает замещать старые данные новыми. Таким образом, в памяти всегда содержатся самые свежие записи.

Защита и передача записанной информации

Для защиты информации в диктофонах Edic-mini Tiny можно установить пароль, запрещающий другому пользователю доступ к содержимому и настройкам диктофона. Каждая запись, сделанная диктофонами Edic-mini Tiny, имеет метку времени и даты начала записи, снабжается «цифровой подписью», которая позволяет определить, на каком именно диктофоне производилась запись и производилась ли модификация записанного файла.

Запись по таймеру

Запись диктофонами Edic-mini Tiny может производиться автоматически. Для этого в диктофоне предусмотрены 2 таймера: ежедневный (задается время начала и конца записи) и однократный (задается дата-время начала и дата-время окончания записи).

Активация голосом

Диктофоны Edic-mini Tiny оснащены системой голосовой активации (VAS – voice activation system), позволяющей снизить расход памяти и тем самым увеличить реальное время записи, а также потребление энергии от источника питания. При выгрузке записей в ПК длительность пауз может восстанавливаться (в виде тишины) либо пропускаться в зависимости от сделанных установок.

Flash-диск

Диктофоны Edic-mini Tiny могут работать в режиме flash-диска, что позволяет использовать их для хранения и переноса любых данных. Возможно одновременное использование диктофона как для записи сообщений, так и в качестве Flash-диска.

Управление диктофонами Edic-mini Tiny простое. Оно осуществляется одной кнопкой или переключателем, в зависимости от модели. Индикация режимов работы диктофона осуществляется при помощи светодиода. Диктофоны Edic-mini Tiny подключаются к USB-порту компьютера при помощи кабеля, входящего в комплект поставки.

Программное обеспечение диктофонов – программа RecManager (работает под управлением ОС Windows Vista, XP, 7(32x, 64x), 8, 10) – позволяет:

- сохранять записи на диске ПК в виде стандартных звуковых файлов;
- настраивать различные параметры диктофона;
- осуществлять защиту доступа к настройкам диктофона с помощью пароля;
- производить обновление программного обеспечения;
- использовать диктофон как Flash-диск.

Правовая информация

Часть 4 статьи 29 Конституции Российской Федерации гарантирует гражданам РФ право «...получать, передавать, производить и распространять информацию любым законным способом», ст. 46 Конституции гарантирует «судебную защиту прав и свобод», ст. 14 Гражданского кодекса РФ допускает самозащиту гражданских прав.

Устройства аудио- и видеозаписи, дистанционного контроля и управления предназначены для помощи гражданам РФ в реализации своих прав на получение информации согласно ч. 4 ст. 29 и получение и фиксацию доказательств для суда согласно ст. 46 Конституции РФ, а также на реализацию права на самозащиту гражданских прав. Необходимость получения и фиксации информации в качестве доказательства возникает часто, особенно в России нашего турбулентного времени, в которой не до конца налажена работа правоохранительных органов, а судебная власть исторически продолжает защищать исполнительную власть, а не закон (к примеру, практикующим автомобилистам известна расхожая фраза «у суда нет оснований не доверять показаниям работника ГИБДД»).

Представленные в настоящей главе устройства могут быть полезны для охраны имущества, для получения и фиксации доказательств при дорожно-транспортных и иных происшествиях, спорах с недобросовестными представителями власти, фиксации устных договоренностей в бизнесе, судебных процессов и т. д.

Внимание, важно!

Вместе с тем автор и редактор считают необходимым предупредить о незаконности приспособления устройств аудио- и видеозаписи для попыток негласного получения защищаемой законом информации: личной и семейной тайн, тайны информации, передаваемой по сетям связи, коммерческой, банковской и государственной тайн.

О практической стороне дела рассказываю далее.

Как аналоговые, так и цифровые диктофоны – это средство, возможность, механизм для тех или иных действий, а система интернета вещей при ее активации в режиме передачи-приема беспроводным дистанционным способом записанной информации (в том числе информации, передаваемой в режиме реального

времени) лишь расширяет уже известные возможности применения этого типа электронных устройств, в том числе для возможной фиксации доказательств в сложных жизненных ситуациях (вымогательство, шантаж, защита прав детей и т. д.). Несмотря на уникальные технические характеристики видеокамер и диктофонов (минимальный размер, высокая акустическая чувствительность, большая автономность и т. д.), функционирующих в системе интернета вещей, они не являются «специальными техническими средствами для негласного получения информации (СТС НПИ) и разрешены к свободному обороту и использованию. Такие диктофоны соответствуют не только требованиям законодательства (отсутствие камуфляжа под предметы иного функционального назначения), но и расширенным требованиям ФСБ (см. ниже). Дополнительно ко всем требованиям все диктофоны имеют надпись, указывающую их предназначение (диктофон), и световую индикацию записи.

Ранее ФСБ исследовала более 50 моделей различных устройств на предмет отнесения к СТС НПИ (однако активность органов в этом вопросе закончилась в 2011–2012 гг., и в последнее время ФСБ уже не проводит подобных исследований), поэтому мы хорошо разбираемся в данном вопросе. Обращаем внимание, что продающиеся на рынке диктофоны китайского производства часто не соответствуют требованиям законодательства, и их приобретение, хранение и использование может привести к нарушению ст. 138.1 УК РФ и ответственности до 4 лет лишения свободы. Будьте осторожны и благоразумны.

Еще один правовой вопрос – как придать аудио- и видеозаписи статус документа, приобщить ее к делу, добиться, чтобы в суде эта запись была принята в качестве доказательства и сыграла решающую роль в защите интересов?

Юридические рекомендации таковы.

- Занесите в раздел «Особые отметки» всю информацию о том, когда, при каких обстоятельствах и каким оборудованием была сделана запись.
- С одной стороны, вы должны приложить запись в качестве доказательства к акту, но делать это небезопасно, ваша запись может и пропасть. Поэтому лучше не отдавать ее в чужие руки, а в этот же день положить в банковскую ячейку – будет документальное доказательство ее неприкосно-

венности. Или сразу идти прямиком в суд и приложить ее там в качестве доказательства, так будет надежнее. И главное, не затягивайте с этим процессом, т. к. в судебной практике есть примеры, когда видео не принималось именно из-за давности сделанной записи.

Внимание, важно!

Итак, необходимо отразить в протоколе факт ведения вами видео-, звукозаписи, отметьте это в разделе «Объяснения». После того как произвели запись, ни в коем случае не изменяйте ее, не «нарезайте», не компонуйте и т. д. Сделайте копию записи (с пометкой – когда, с помощью чего, кто изготовил).

Далее необходимо подать в суд ходатайство о просмотре/прослушивании и приобщении к материалам дела аудио- или видеозаписи, указать, кем, где, когда, с помощью чего производилась. Пояснить, какие подлежащие установлению обстоятельства дела содержит запись. В приложении не забудьте указать запись, количество экземпляров, носитель. Имейте в виду, может так случиться, что в суде нет технических средств для просмотра, прослушивания записи, тогда аппаратуру придется нести с собой. При этом предварительно узнайте, требуется ли написать заявление на пронос техники, если да, то подготовьте.

Если суд откажет в просмотре/прослушивании записи, то в материалах дела останется письменное ходатайство. Так будет зафиксировано, что ваше право на предоставление доказательств нарушено (ст. 25.1 КоАП РФ). Судья обязан вынести на ходатайство определение с указанием мотивов отказа. Данное определение отдельно обжалованию не подлежит, но в жалобе на постановление вы можете его (определение) оспаривать.

2.1.6. Диктофон с видеокамерой Fortune Fly FTX-360MC-23

Устройство под управлением Wi-Fi Fortune Fly FTX-360MC-23 представляет собой портативную Wi-Fi-мини-камеру 1080P HD со встроенной памятью 128 ГБ и Tf-диктофоном. Внешний вид устройства представлен на рис. 2.1–2.3 (имеет такой же внешний вид, как и ранее описанная модель).

По сути, это 1080P HD-мини-камера скрытого ношения, с поддержкой видеозаписи в режиме реального времени и записи голоса, ИК ночного видения, позволяющей делать снимки в реальном времени и видеосюжеты, а затем транслировать их по каналу Wi-Fi.

Технические характеристики и особенности

Функция:	диктофон и мини-скрытая видеокамера
Угол обзора широкоугольного объектива:	170°
Датчик активации:	CMOS
Корпус:	антивандальный
Видеокамера с разрешением	1080P, Full HD 1080P
Емкость аккумулятора:	1200 мА/ч
Запись видео:	5 ч
Запись голоса:	20 ч
Конфигурация видео:	H.264
Локальное хранилище:	поддержка 128 ГБ MicroSD-карты, поддержка для просмотра онлайн (просмотр воспроизведения видео на телефоне от TF-карты)
Напряжение питания:	DC 5 В, 1 А
Вес изделия:	90 г

Дополнительно:

функция обнаружения движения;
функция автоматического сохранения записи перед выключением питания;
поддержка Windows, iOS и Android телефонов;
модель имеет функцию автоматического выбора времени «день/ночь»: IR-CUT автоматически переключается;
конструкция магнита для легкой установки.

2.1.6. Профессиональная DMT6 видеокамера, совмещенная с диктофоном

Устройство, внешний вид которого представлен на рис. 2.12, представляет собой мобильный видеорегистратор с управлением и передачей данных по Wi-Fi с 1296 P Full HD-качеством записи видео.

Отличительные особенности устройства

- Объектив 140°;
- время записи 8 ч;

Рис. 2.12. Внешний вид видеокамеры-диктофона DMT6

- камера 23 Мп;
- две ИК-подсветки;
- индикация работы (звук и вибрация);
- 2М ударопрочный, 5М водонепроницаемый корпус (военный стандарт);
- уникальная фронтальная кнопка для записи;
- 5 светодиодных индикаторов: индикатор питания, индикатор зарядки, индикатор записи звука, индикатор состояния записи, GPS-индикатор состояния;
- Drop и Doc для зарядки отдельного аккумулятора и установленной батареи одновременно;
- дополнительно 2 элемента питания, каждая батарея обеспечивает работоспособность до 6.2~6.6 ч;
- поддержка до 64 ГБ памяти.

Особенности Wi-Fi-Live Streaming

Устройство можно подключить к мобильному телефону и ноутбуку для загрузки видео или просмотра видео в режиме реально-

го времени. Есть видеошифрование и USB-интерфейс на камере. Пользователь может установить устройство на doc-станцию и входной пароль на программное обеспечение для чтения данных внутри камеры. Эта функция может безопасно защитить накопленные данные.

Технические характеристики и особенности устройства DMT6

Основные

Датчик:	5MP CMOS
Чипсет:	Ambarella A7LA55
Разрешение видео:	2304×1296 P при 30 fps; 1920×1080P при 30 fps; 1280×720 при 30 fps и 60 fps; 848×480 при 30 fps
Формат видео:	H.264. MOV
Аудиовход:	Встроенный микрофон
Формат аудио:	WAV
Воспроизведение аудио:	Встроенный динамик
Водяной знак:	Идентификатор пользователя, datetime Stamp
Камера:	20 Мп; поддержка режима разрыва (3 или 5 изображений)
Формат изображения:	JPEG
Snap shot:	Дает возможность одновременно снимать фотографии во время записи видео
Емкость внешней памяти, вариативно:	16 Гб / 32 Гб / 64 Гб
Одна кнопка записи:	Поддержка, управление
ИК-подсветка:	2 ИК-светодиодные подсветки, 15 м расстояние записи, в отсутствие дневного света

Видео/обзор изображения

Экран:	2 дюйма TFT-, ЖК-дисплей высокого разрешения
Аудио и видео, фотовоспроизведение:	Поддерживает

Видеовыход:	HDMI 1.3
Передача видео:	USB 2.0
Камера	
Угол объектива:	Широкий угол обзора 140°
Водонепроницаемый уровень:	IP65
Клипса:	Металлический зажим с 360° вращения
Ptt	Доступно подключение к различным типам радиоприемников
ИК Вкл/Выкл:	Автоматически контролируется фоторезистором
Аккумулятор	
Тип:	Съемный Li-ion-аккумулятор 2000 мА/ч
Время зарядки:	100 мин
Предупреждение о низком заряде батареи:	Звуковой сигнал оповещения
Другие	
Номер ID:	Включает 6-идентификационный идентификатор устройства и 6-разрядный идентификатор службы безопасности
Защита паролем:	Пароль администратора для удаления файлов
Функция предварительной записи:	5–30 с
Post-функция записи:	10/20/30 с
Режим серийной съемки:	1/3/5 фотографий, снятых непрерывно
Размеры:	84×60×32 мм
Вес:	160 г
Рабочая температура:	–40 ~ +60 °C
Температура хранения:	–20 ~ +55 °C
Аксессуары	
Стандартная комплектация:	USB-кабель, зарядное устройство, инструкция, универсальный металлический зажим, CD, 2 аккумулятора, Drop in Dock

Дополнительные аксессуары	Встроенный GPS, встроенный Wi-Fi, опциональный чип A2 без 1296P видео, внешняя камера, эполеты клипсы на автомобильное лобовое стекло, ptt-кабель

2.2. Видеокамеры P2P

2.2.1. IP P2P-камера VSTARCAM T6835WIP. Настройки и практическая работа

Поворотная IP P2P-камера, внешний вид которой представлен на рис. 2.13, обладает многими преимуществами, существенно отличающими ее от аналогичных моделей, так как:

- легка и проста в установке и наладке за счет применения инновационной программы Plug and Play;
- вся техподдержка и документы доступны на русском языке;
- просматривать изображения, или управлять настройками, или качать информацию можно удаленно при помощи ноутбука или телефона;
- имеет Wi-Fi-антенну;
- запись ведется на SD-карту 32 Гб.

Внешний вид камеры представлен на рис. 2.13.
Устройство имеет следующие возможности:

- использование динамического IP-адреса за счет поддержки P2P;
- возможность отличного обзора – поворотный механизм обеспечивает наклон на 120° и поворот на 350°;
- качественная съемка ночью за счет автоматического включения инфракрасной подсветки на расстоянии до 10 м;
- благодаря встроенному высокочувствительному микрофону есть возможность передачи не только изображения, но и звука.

Дизайн камеры Vstarcam T6835WIP оригинален, камера выполнена в белом цвете и внешним видом напоминает мини-робота.

Рис. 2.13. Внешний вид камеры Vstarcam T6835WIP

Технические характеристики IP P2P-камеры

Видео

Матрица:	CMOS, 1/4 0,3 мегапикселя
Объектив:	3.6 мм
ИК-подсветка:	максимальное расстояние до 10 м
Сжатие видео:	MJPEG
Разрешение:	VGA (640×480) при режиме 1–30 к/с, QVGA (320×240) при 1–30 к/с
Объем видеопотока:	128~4096 Кбит/с
Настройка видеоизображения:	контрастность, яркость, насыщенность, оттенок

Запись

Носитель:	карта micro-SD объемом до 32 ГБ, класс не менее 10
Сервер:	FTP (только 2-й поток)
Электронная почта:	отправка фото по факту события (срабатывания сенсора/движения в зоне ответственности) на e-mail

Аудио	
Аудиовход:	1 канал линейный вход (разъем типа «джек» 3.5 мм) и 1 канал внутреннего микрофона – 48 dB
Аудиовыход:	1 канал линейный выход (разъем типа «джек» 3.5 мм) и внутренний динамик (8 Ом, 1 Вт)
Частота дискретизации:	8 кГц, 16 бит
Сжатие аудио:	ADPCM/32 кбит/с
Сеть	
Ethernet (LAN):	10Base-T/100Base-TX, разъем типа RJ45
Wi-Fi:	802.11n: до 150 Мбит, 802.11g: до 54 Мбит, 802.11b: до 11 Мбит
Протоколы:	TCP/IP, HTTP, TCP, ICMP, UDP, ARP, IGMP, SMTP, FTP (только 2-й поток), DHCP, DNS, DDNS, NTP, UPnP, PPPoE Поддержка P2P – работа без статического адреса
Питание	
Напряжение питания	5 ± 0.3 В
Потребляемая мощность	3,5 Вт – 7 Вт при включении поворотного механизма и подсветки
Масса	1200 г
Размер упаковки (д×ш×в)	200×120×179 мм

Комплектация: камера, блок питания, антенна Wi-Fi 2 дБ разъем SMA, кронштейн, клиентское программное обеспечение для просмотра и настройки камер Vstarcam для Windows – IP Camera Super Client (рус).

2.2.2. Настройка P2P-камеры

Устройства единого модельного ряда PnP IP/сетевая камера с Wi-Fi T – серия моделей T7838WIP, T7833WIP, T7850WIP, T7838WIP, T7815WIP, все они настраиваются по аналогии. Существует два вида настроек – быстрая и основная.

В режиме «быстрая настройка» подключите камеру к роутеру с помощью сетевого кабеля. Убедитесь в том, что индикатор питания на роутере горит (роутер подключен к сети электропитания), а также что роутер подключен к сети интернет.

Внимание, важно!

Перезагрузить IP-камеру со сбросом к заводским установкам можно кнопкой **Reset**, которая находится внизу камеры (зависит от модели).

Просмотр изображения возможен через мобильный телефон, коммуникатор или планшет на Andriod. Установите приложение P2PCam264, для этого зайдите на сайт http://cd.gocam.so с помощью браузера телефона, планшета и следуйте инструкциям ниже.

Далее потребуется считать QR-код и установить приложение для P2P-камер, что имеется в открытом доступе. Приложение «VsCam» появится в списке приложений при успешной инсталляции.

Затем запустите приложение и нажмите **Добавить** для добавления камеры.

Нажмите **Скан** (Scan), после чего поднесите камеру вашего смартфона к наклейке камеры (находится внизу камеры, на ней написан UID). Характерный звук «бип» означает, что сканирование UID прошло успешно. Также вы можете нажать поиск для поиска камеры через локальную сеть по следующему алгоритму:

- «Имя пользователя» – по умолчанию это admin-пароль – 888888;
- The default password is: 888888;
- The default user is: admin.

Следующим шагом введите камеру в режим просмотра видео.

Настройка Wi-Fi осуществляется так.

Нажмите на значок справа от камеры для настройки камеры. Нажмите **Настройки** (Setting) и **Настройки Wi-Fi** (Wi-Fi Setting), откроется список доступных сетей. Выберите нужную Wi-Fi-сеть, введите пароль для доступа к сети и нажмите **OK**. После этого отключите сетевой кабель от камеры, камера будет перезагружена и автоматически соединится с Wi-Fi-сетью.

Внимание, важно!

Если у камеры есть функция управления поворотом, то можно просто провести по экрану для управления камерой.

Просмотр через устройство Apple

Установите приложение VsCam с сайта http://cd.gocam.so, используя веб-браузер телефона, и следуйте инструкции, используя удобный способ – сканирование QR-кода или обыкновенную установку приложения для просмотра P2P-камер.

Приложение «VsCam» будет доступно на рабочем столе после успешной инсталляции. Затем запустите приложение и нажмите **Добавить** (ADD) для добавления камеры.

Нажмите **Скан** (Scan), после этого считайте UID камеры (поднесите камеру телефона к наклейке с задней стороны камеры). Характерный звук «бип» будет означать, что UID считан успешно.

Также вы можете нажать кнопку **Поиск** для добавления камер по локальной сети в автоматическом (нажмите кнопку +) или ручном режиме. Имя пользователя по умолчанию – admin-пароль 888888.

Wi-Fi-настройка осуществляется по аналогии с описанным выше.

Нажмите на кнопку со стрелкой правее камеры, далее нажмите **Настройки** (Setting) и **Настройки Wi-Fi** (Wi-Fi Setting), откроется список доступных сетей. Выберите нужную Wi-Fi-сеть, введите пароль для доступа к сети и нажмите **OK**. После этого отключите сетевой кабель от камеры, камера будет перезагружена и автоматически соединится с Wi-Fi-сетью.

Внимание, важно!

Если у камеры есть функция управления поворотом, то можно провести курсором по экрану для управления камерой.

Просмотр на компьютере или ноутбуке

Зайдите на сайт http://cd.gocam.so для загрузки клиентского программного обеспечения. После установки на рабочем столе появится иконка, откройте ее двойным кликом мыши. Нажмите **Добавить камеру для подключения камеры по LAN**. Для добавления камеры по LAN нажмите кнопку **Найти** (Find). Для добавления камеры через сеть интернет введите UID камеры (UID камеры указан на наклейке с обратной стороны камеры). Для добавления камеры в ручном режиме – логин – admin-пароль 888888.

Нажмите **OK**, чтобы подтвердить добавление камеры. Раздел **Настройки Wi-Fi** отвечает за настройку камеры через беспроводной интернет. Затем нажмите 2 раза на IP-камеру **IP Camera**, чтобы просмотреть видео.

Для получения более подробной информации зайдите на сайт http://cd.gocam.so.

2.2.3. Общая информация по приложению IP Camera Super Client

IP Camera Super Client – это комплексное программное обеспечение для просмотра и управления IP-камерами. Основные преимущества данных устройств – это:

- просмотр нескольких камер одновременно (до 81 камеры);
- управление функциями поворота и приближения (PTZ);
- управление записью и тревогой;
- разграничение прав пользователей.

Расширенный набор функций

1. Просмотр до 81 камеры в одном окне.
2. Поддержка работы и записи по расписанию, по тревоге, отправка тревожных снимков и уведомлений.
3. Поддержка русского, английского, французского и испанского языков.
4. Удобный интерфейс просмотра и сортировки тревожных сообщений.
5. Поддержка воспроизведения видео с компьютера или ноутбука.
6. Поддержка включения тревоги по датчику движения.
7 Поддержка отправки тревожных сообщений вручную или автоматически.

На рис. 2.14 вы увидите начальное окно – иллюстрацию программной установки камеры на компьютер.

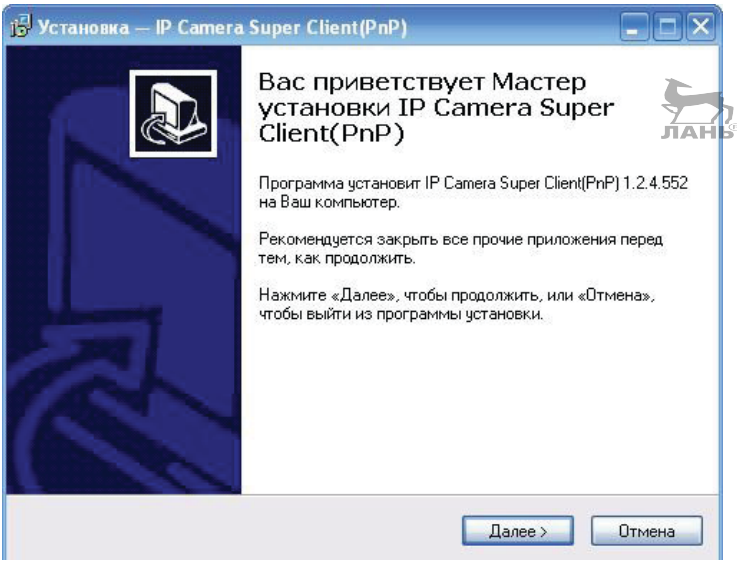

Рис. 2.14. Иллюстрация программной установки камеры на компьютер

На рис. 2.15 представлено окно следующего шага установки.

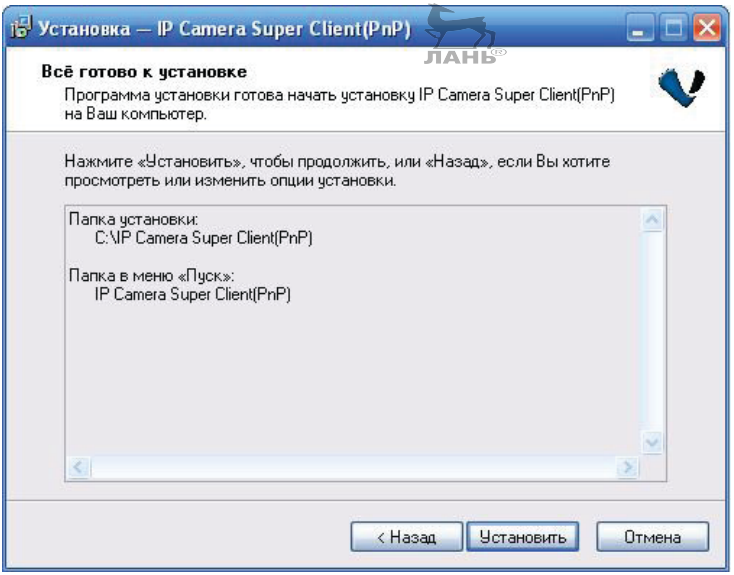

Рис. 2.15. Следующий шаг установки оборудования

На рис. 2.16 представлено окно выбора языка (установки).

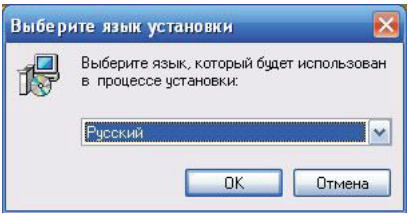

Рис. 2.16. Иллюстрация окна выбора языка

Внимание, важно!

Если будет появляться другая информация или вопросы при установке, нажмите **Применить**. По завершении установки на рабочем столе появится соответствующая иконка.

На рис. 2.17 представлено окно выбора папки установки драйвера управления камерой на ПК.

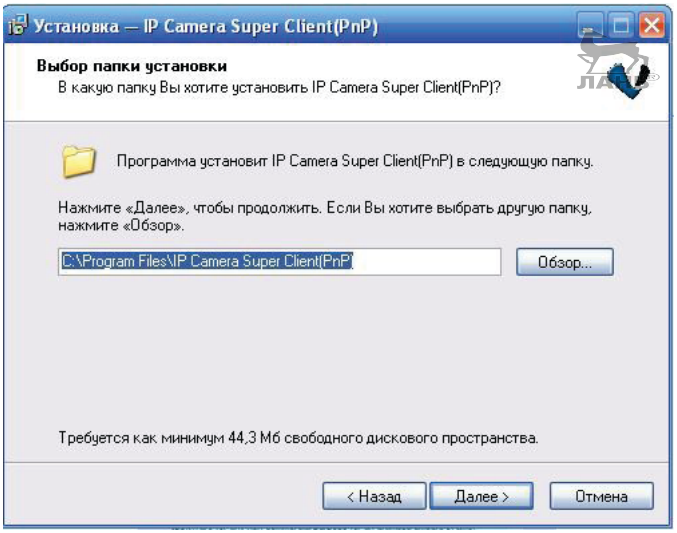

Рис. 2.17. Окно выбора папки установки драйвера управления камерой на ПК

На рис. 2.18 представлена иллюстрация промежуточного шага распаковки файлов.

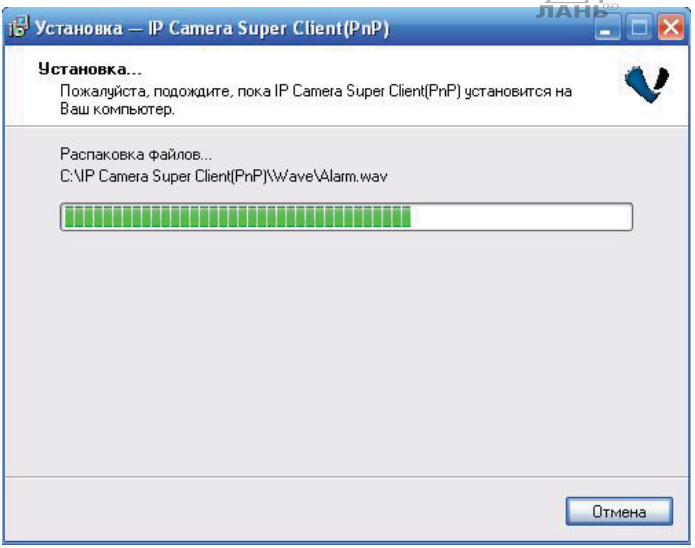

Рис. 2.18. Иллюстрация распаковки файлов

На рис. 2.19 представлено окно завершения установки программного обеспечения для камеры на компьютер.

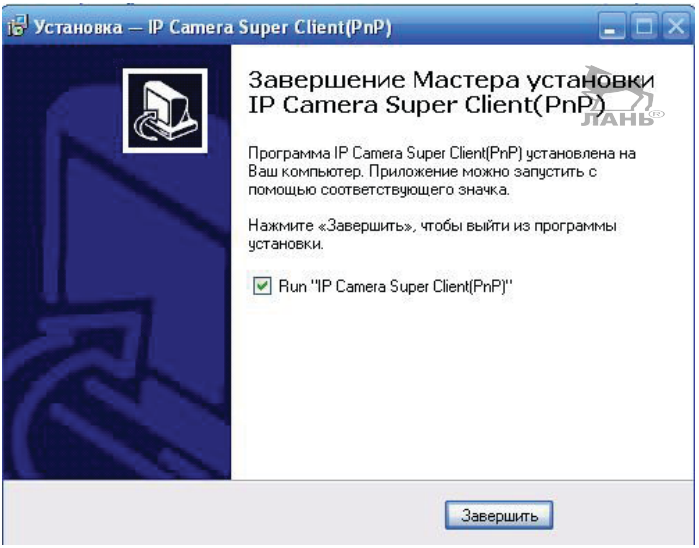

Рис. 2.19. Иллюстрация завершения работы **Мастера установки** оборудования

Настройка пути для сохранения файлов

Дальнейшая настройка оборудования осуществляется после запуска программы драйвера на ПК и уже программными средствами, то есть путем нажатия «кнопок» курсором по открывающимся окнам программы. Для установки пути сохранения файлов нажмите кнопку настройки, что иллюстрирует рис. 2.20.

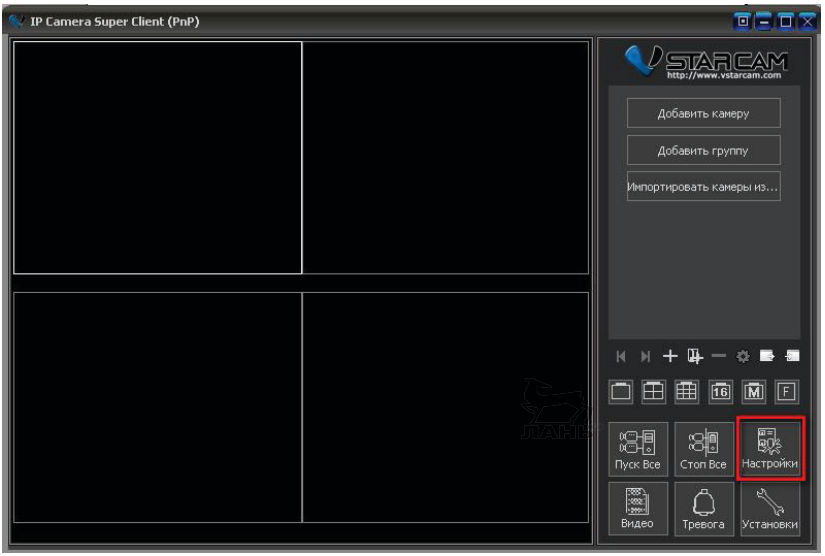

Рис. 2.20. Иллюстрация выбора пути сохранения файлов и кнопки **Настройка**

Добавить или удалить путь

Вы можете добавить несколько путей для сохранения видео. Для этого зайдите в раздел **Путь для хранения записей**. Если пространство в указанном месте заканчивается (если, например, указан определенный жесткий диск), то система автоматически начинает сохранять данные по второму пути (см. рис. 2.21).

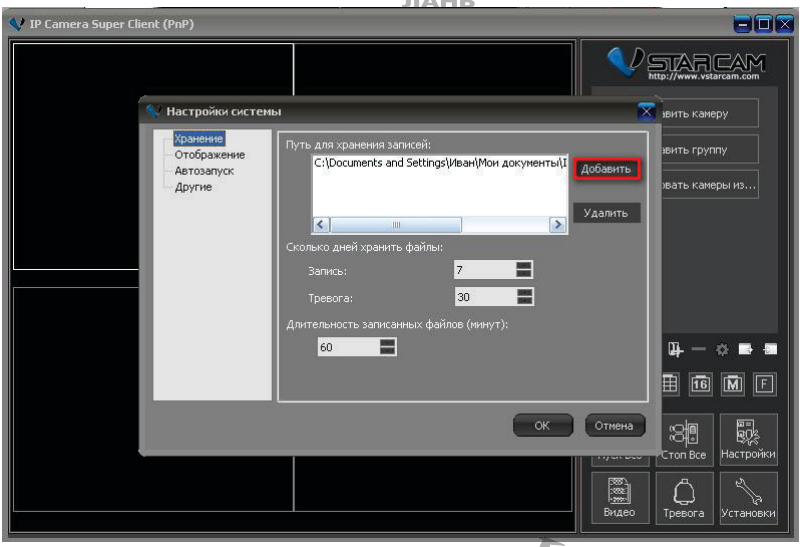

Рис. 2.21. Выбор опции **Путь для хранения записей**

Настройка автозапуска IP Camera Super Client иллюстрируется на рис. 2.22.

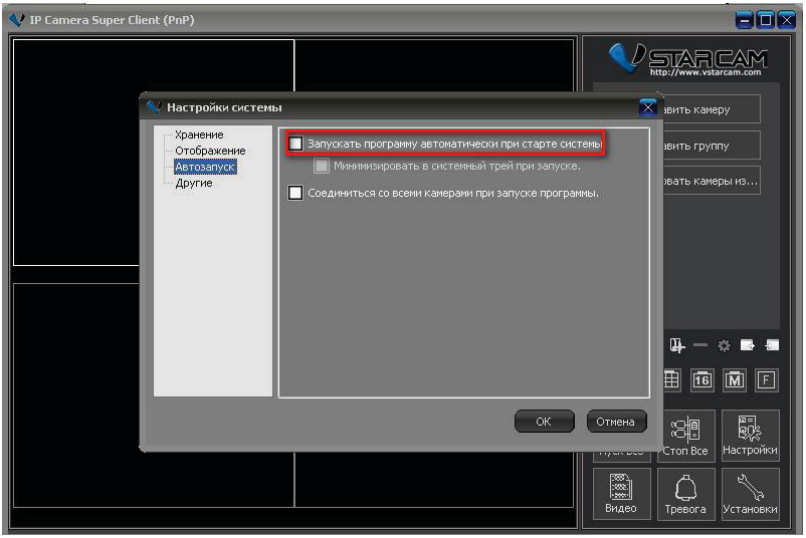

Рис. 2.22. Настройка автозапуска IP Camera Super Client

2.2.4. Основные программные функции

Далее поговорим об основном интерфейсе программы. Основное меню камеры и программного обеспечения представлено на рис. 2.23.

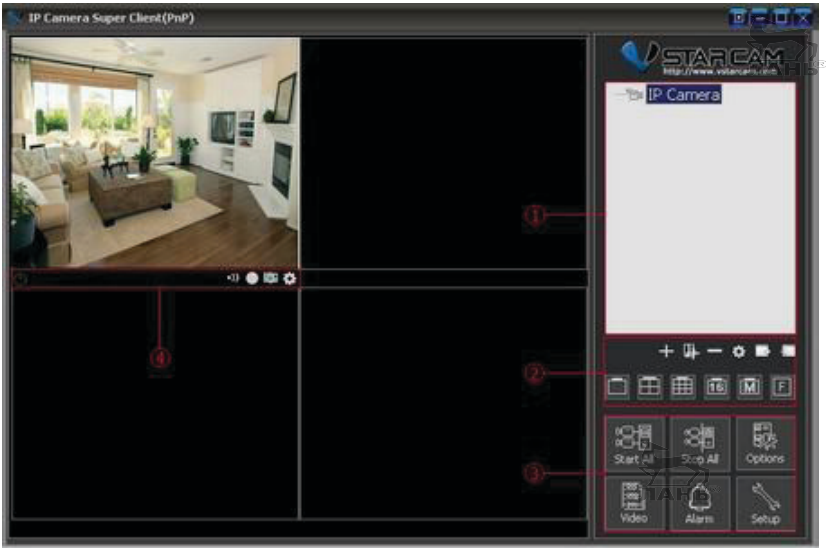

Рис. 2.23. Основное меню камеры и программного обеспечения

Список камер и управление экранным режимом

Список IP-камер. Поддерживается одновременный просмотр множества камер (до 81). Нажмите правой кнопкой мыши на список камер, в выпадающем меню выберите IP-камеры или группы IP-камер для их включения или отключения. Кликните правой кнопкой мыши по конкретной IP-камере, и вы попадете в ее настройки. Двойной клик на IP-камеру автоматически подключает эту камеру.

Управление экранным режимом. Пользователь может выбрать 1 видео на экране или одновременно 4, 9, 16, 25, 64, 81 камеру в первом экране. Также существует поддержка полноэкранного режима. Если количество камер более 81, то вы можете использовать кнопки **Page Up** и **Page Down** для переключения между страницами.

Общие настройки и контроль

Подключайте, отключайте IP-камеру или группы IP-камер, управляйте видеозаписями и видеотоками с камер, включайте настройки тревоги, настраивайте каждую камеру в отдельности или задавайте параметры для группы камер. Этот шаг иллюстрирует рис. 2.24.

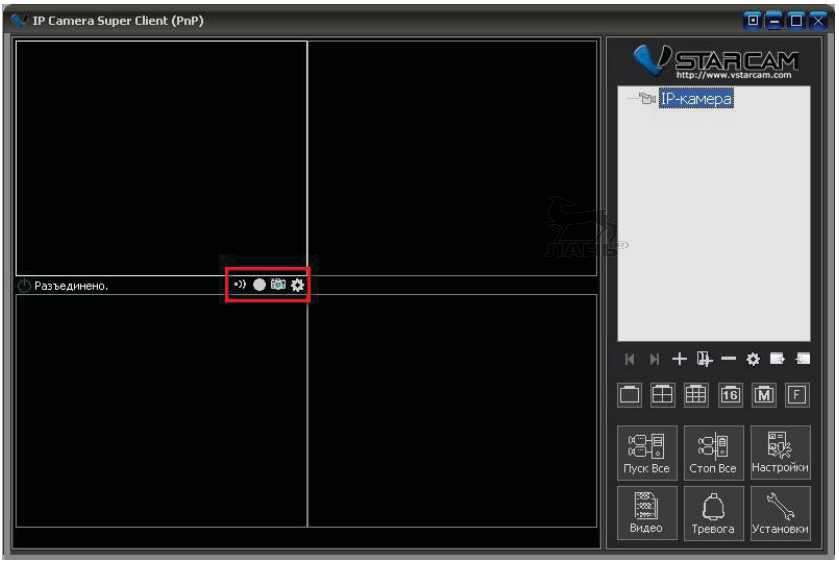

Рис. 2.24. Иллюстрация окна **Общие настройки и контроль**

Статус и меню управления

- Режимы **Тревога** и **Настройка тревоги**.
- Информация о записи видео и настройка видео.
- Снимок вручную.
- Дополнительные настройки камеры.

Как в систему интернета вещей добавить новую камеру

Нажмите **Добавить камеру** в правой части интерфейса программы. После этого нажмите кнопку **Найти**, если камера находится в вашей локальной сети. Этот шаг иллюстрирует рис. 2.25.

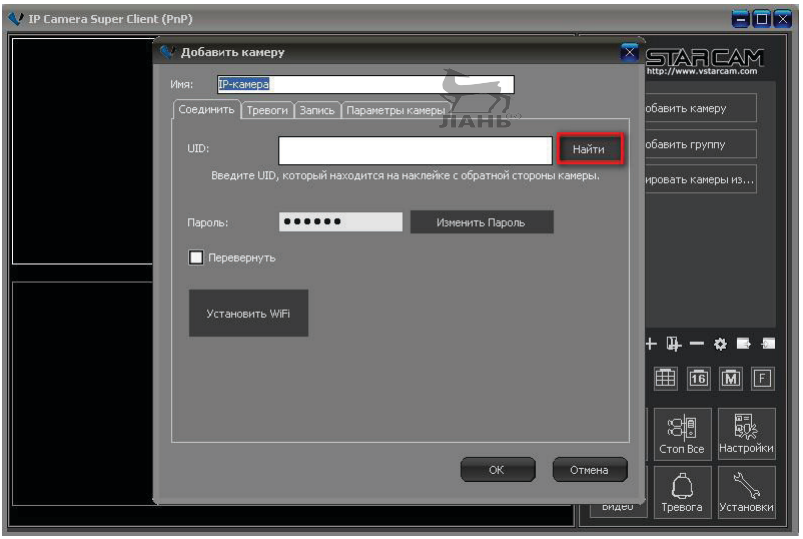

Рис. 2.25. Иллюстрация окна для добавления в систему новой камеры

Для удаленного подключения камеры через интернет введите UID камеры (UID камеры указан на наклейке внизу камеры или на коробке с камерой) – см. рис. 2.26–2.27.

Рис. 2.26. UID камеры на наклейке внизу камеры

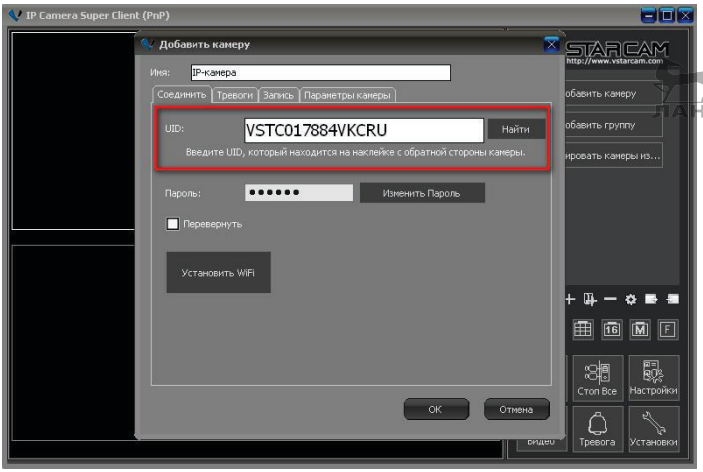

Рис. 2.27. Действия в окне программы – ввод UID

Внимание, важно!

Внимательно проверьте введенные данные UID (в нашем случае VSTC0 (ноль, не буква «О»), введите пароль от камеры. Пароль по умолчанию 888888. Затем дважды кликните по IP-камере для просмотра онлайн.

Для контроля просмотра видео см. рис. 2.28.

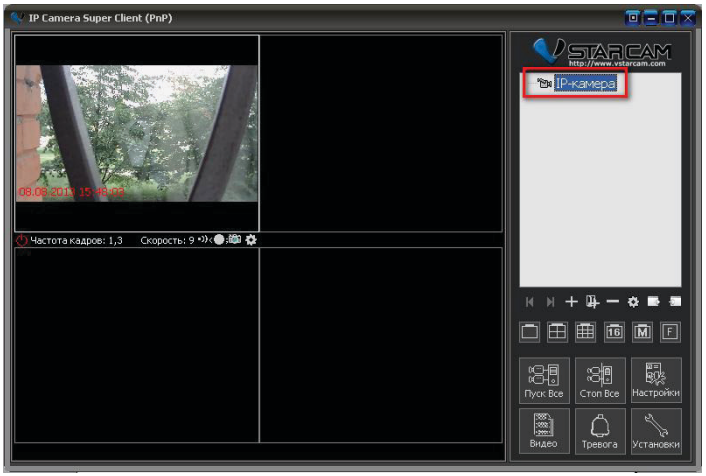

Рис. 2.28. Окно контроля просмотра видео

Запись видео

Для контроля и осуществления записи видео действуйте в соответствии со следующими рекомендациями. Кликните правой кнопкой мыши по видео с камеры, зайдите в **Настройки камеры**; этот шаг иллюстрирует рис. 2.29.

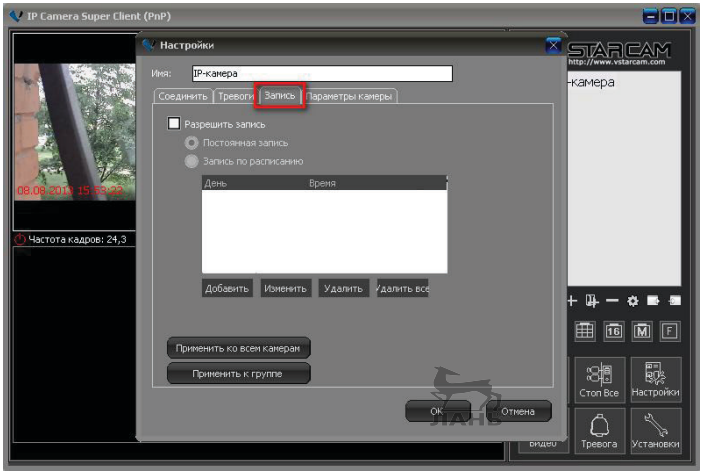

Рис. 2.29. Окно контроля записи видео

Нажмите кнопку **Запись**, **Разрешить запись** – установите расписание записи в зависимости от необходимости (см. рис. 2.30).

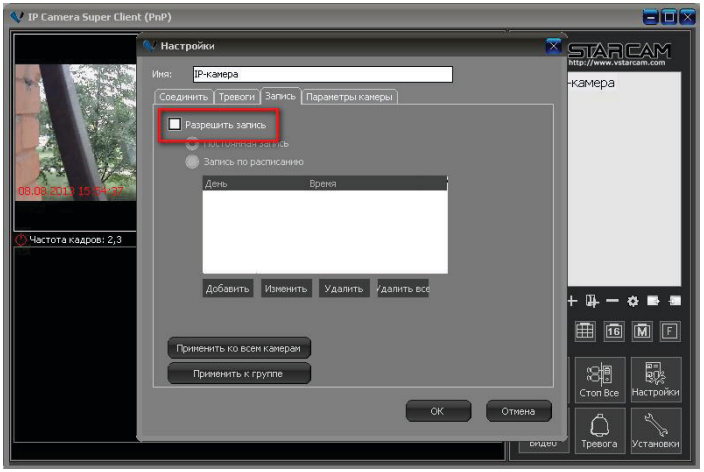

Рис. 2.30. Иллюстрация окна для последующих операций в режиме записи

Для настройки опции **Расписания** см. рис. 2.31.

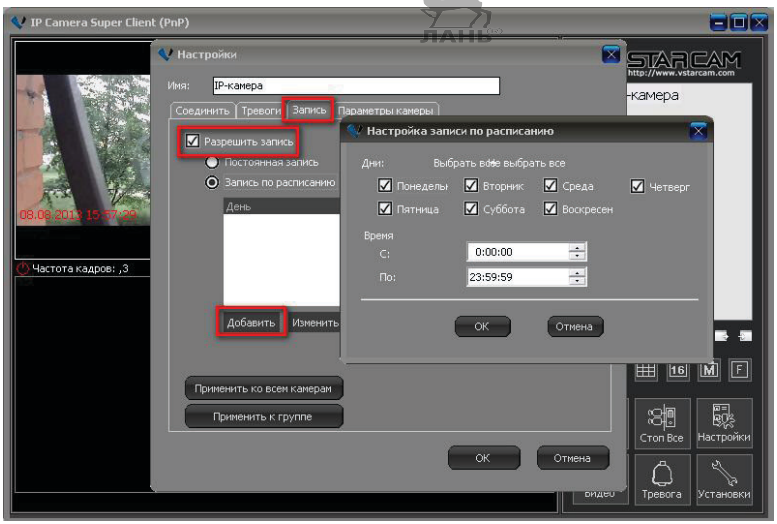

Рис. 2.31. Окно настройки расписания

Для быстрого доступа к настройке записи из главного меню программы существует специальная кнопка (выделена кружком на рис. 2.32).

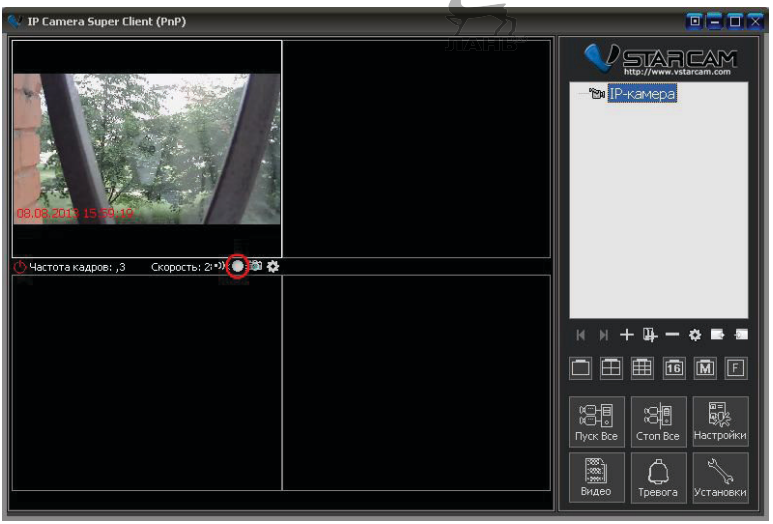

Рис. 2.32. «Быстрая» кнопка доступа к настройке записи

Проверка видеозаписи

Нажмите кнопку **Видео** в главном интерфейсе программы (см. рис. 2.33).

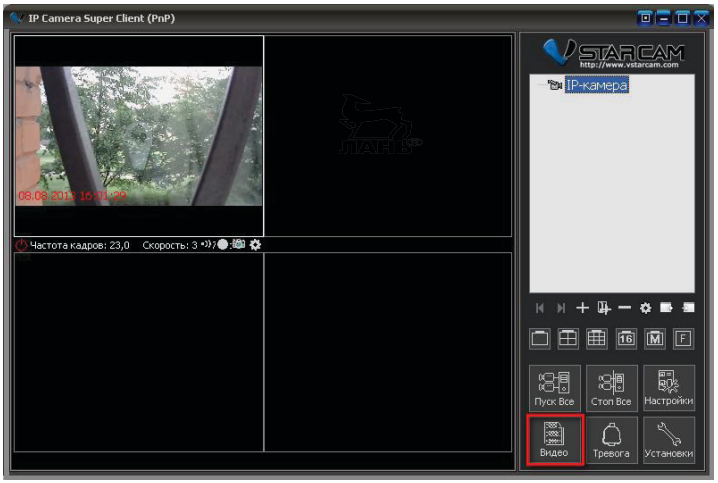

Рис. 2.33. Иллюстрация окна программы проверки видеозаписи

Затем используйте поиск видеозаписи по дате события. Как это сделать, показано на рис. 2.34.

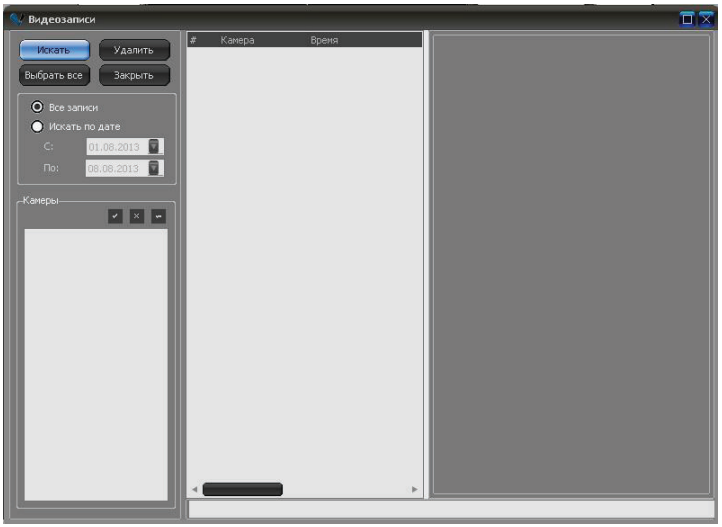

Рис. 2.34. Иллюстрация поиска видеозаписи по дате события

Настройки датчика движения режима «Тревога»

1. Кликните правой кнопкой мыши по видео с камеры и зайдите в раздел настроек камеры, потом выберите пункт **Параметры камеры**, как это показано на рис. 2.35.

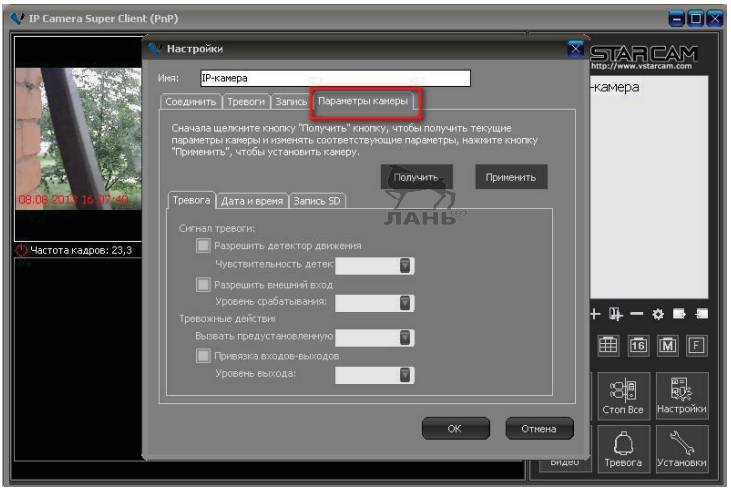

Рис. 2.35. Иллюстрация выбора режима работы датчика движения в окне **Параметры камеры**

2. Нажмите кнопку **Получить** (см. рис. 2.36).

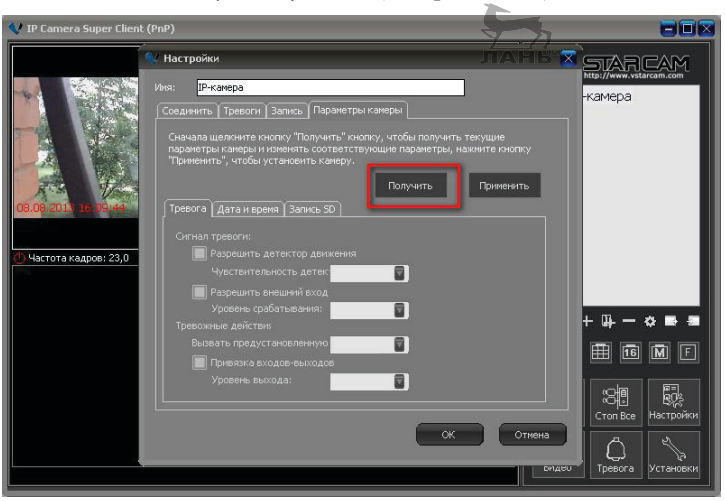

Рис. 2.36. Иллюстрация следующего шага

3. Выберите нужную чувствительность датчика движения в зависимости от необходимости и ситуации (см. рис. 2.37).

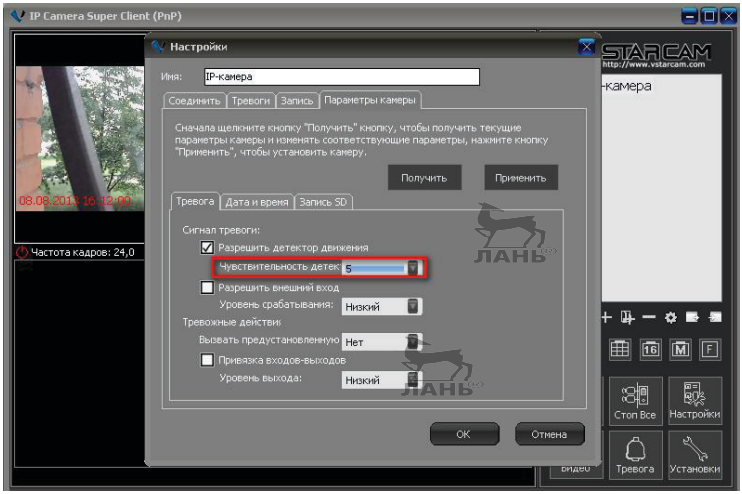

Рис. 2.37. Иллюстрация выбора необходимой чувствительности

4. Затем в разделе **Тревога** нажмите **Добавить** (см. рис. 2.38).

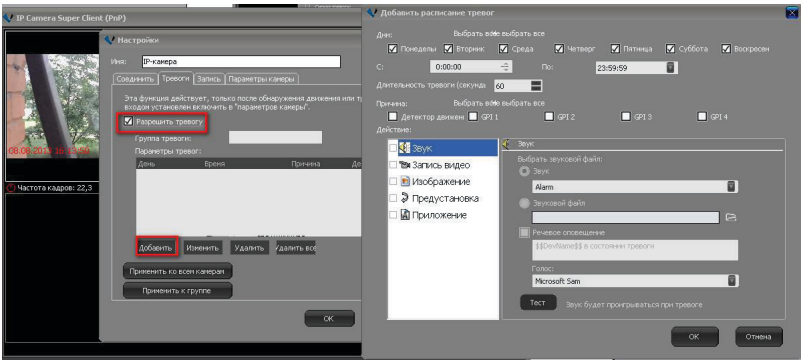

Рис. 2.38. Иллюстрация операций в разделе **Тревога**

5. Следующим действием добавьте расписание для срабатывания тревоги. Для этого выберите время срабатывания и причину, к примеру датчик движения. Если случается указанное событие срабатывания (движение в зоне детекции датчика движения), то происходит некий сценарий, который задается в разделе **Действия**. Этот шаг иллюстрирует рис. 2.39.

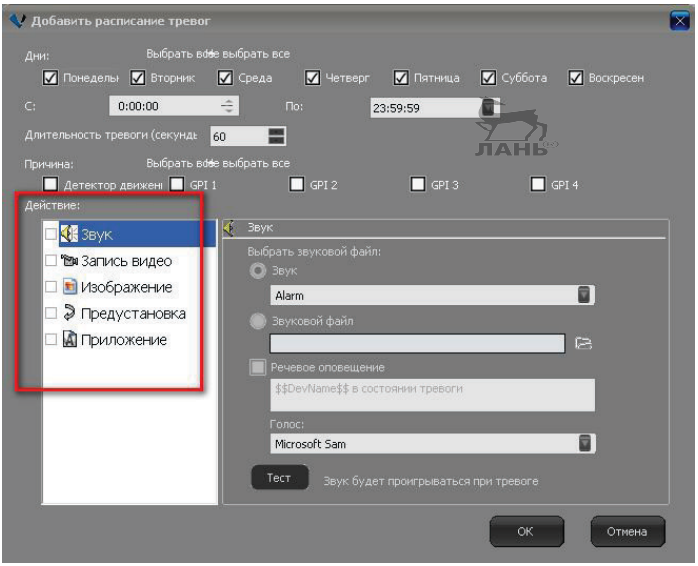

Рис. 2.39. Выбор времени срабатывания сигнализации и причины срабатывания

Проверка записи по расписанию

Нажмите **Тревога** в меню основного интерфейса программы. Иллюстрация этого шага представлена на рис. 2.40.

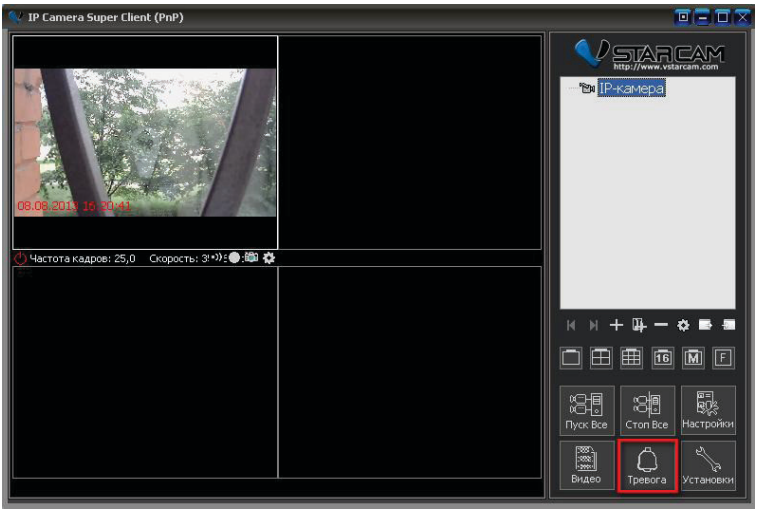

Рис. 2.40. Иллюстрация меню основного интерфейса программы

Затем можно выбрать **Запись из списка** или **Искать по дате** (см. рис. 2.41).

Рис. 2.41. Иллюстрация окна выбора файлов **Запись из списка** или **Искать по дате**

И теперь самое главное...

Настройка Wi-Fi

Нажмите кнопку **Параметры камеры** и зайдите в раздел **Соединение**, выберите **Настройки Wi-Fi** (см. рис. 2.42).

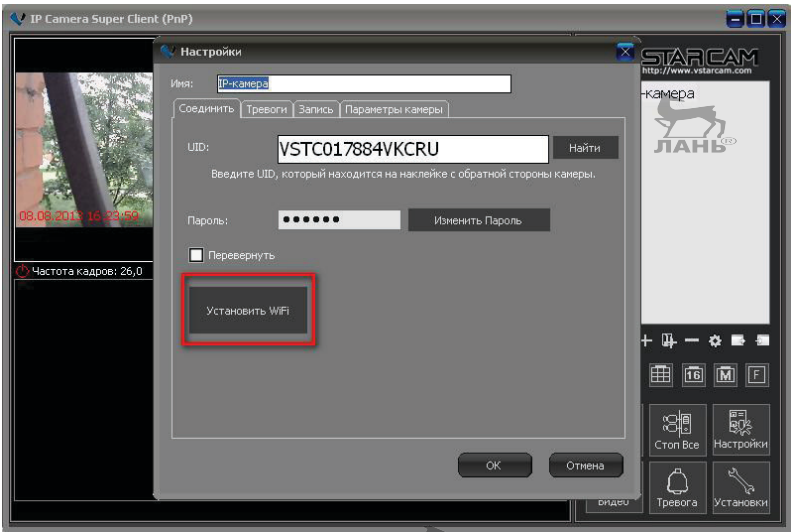

Рис. 2.42. Окно **Настройка Wi-Fi**

В соответствии с описанным алгоритмом в теоретической части книги (глава 1) нажмите **Поиск сигнала**. Этот шаг иллюстрирует рис. 2.43.

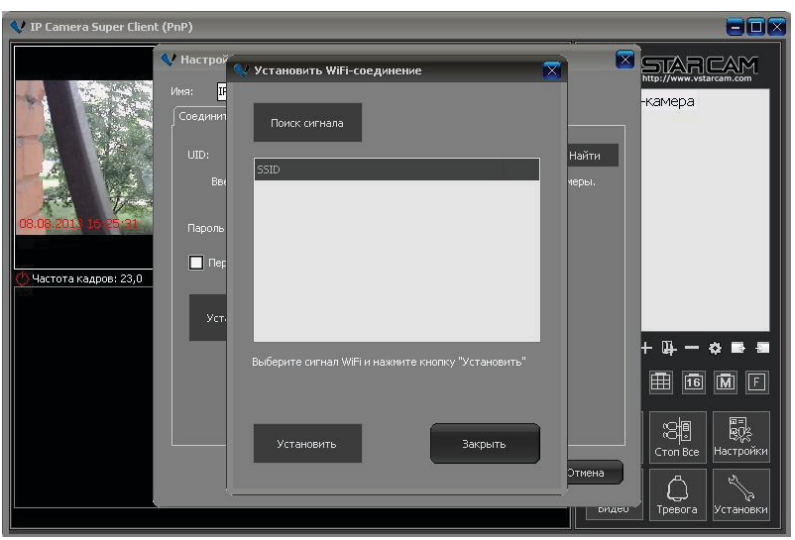

Рис. 2.43. Окно **Поиск сигнала**

Когда поиск сигнала будет завершен, выберите нужную Wi-Fi-сеть и нажмите кнопку **Установить**. В выпадающем меню введите пароль от Wi-Fi-сети и нажмите **Ввод**.

На этом настройка оборудования для успешной работы в системе интернета вещей завершена.

Глава 3

ДРУГИЕ ИСПОЛНИТЕЛЬНЫЕ УСТРОЙСТВА В СИСТЕМЕ ИНТЕРНЕТА ВЕЩЕЙ

В этой главе рассмотрим управляемые исполнительные устройства, которые предназначены для удаленного включения и отключения бытовых электроприборов с напряжением 220 В и мощностью до 2,5 кВт. Пользователь может управлять всеми подключаемыми устройствами через облачный интернет-сервис бесплатно, через личный кабинет из любой точки мира, с любого устройства.

3.1. Особенности и возможности исполнительных устройств бытового назначения

Устройства для дистанционного управления электрической нагрузкой в системе интернета вещей можно условно разделить на бытовые и специальные. Даже хорошо известная сегодня электронная розетка с контроллером внутри может иметь огромные перспективы в плане сбора информации вокруг себя. Освещенность, температура воздуха, наличие движения/присутствия и далее – запись голоса, видео и прочее, прочее, прочее, с возможностью передачи информации куда угодно. Более того, с подобным дистанционным управлением можно сделать и аварию в нужном месте.

3.1.1. Интересные вопросы безопасности

Как мы выяснили в первой главе книги, за аббревиатурой IoT скрываются весьма интересные открытия. Эта очень удобная система, получившая название интернета вещей (IoT), отнюдь небезопасна. Уже существуют различные вирусы, в том числе «трояны», для устройств, управляемых через интернет. К рас-

сматриваемой теме эти сведения имеют прямое отношение, поскольку мы собираемся управлять нагрузкой в электрической цепи именно с помощью интернета и локальной сети Wi-Fi. Кофеварки, чайники и другое бытовое оборудование, системы, управляемые по Wi-Fi, «родились» не вчера, но и они небезупречны, несмотря на то что с их появлением для пользователей всего мира открылись новые перспективные возможности. Но одновременно с ними появились и причины всерьез опасаться нового витка прогресса. Надо полагать, производители устройств, подпадающих под определение системы управления IoT, не задумывались о безопасности пользователей или же, осознавая возможности несанкционированного управлениями своими «детищами», предлагают их именно как бытовое развлечение, не более того... Действительно, большинство производителей и поставщиков такой техники, как Wi-Fi-устройства управления и, в частности, интернет-розетки, рассмотренные во второй главе книги, озабочено лишь удобством для пользователей, созданием «электронного комфорта», дружелюбным интерфейсом и скоростью вывода продукта на широкий рынок, то есть собственными доходами небезупречного предприятия.

Давайте задумаемся на минуту как пользователи и потребители этих гаджетов, и мы поймем, что производители торопятся заставить нас как можно скорее купить эти вещи. Но в результате, в соответствии с кратким анализом, предложенным в данной книге, оказывается, что наш дом легко может превратиться в... минное поле. Каждое подобное устройство будет иметь все более сложное программное обеспечение (прошивку, неподконтрольную пользователю) и сетевые права доступа. Уже сегодня нежелательно безусловно доверять «радионяням», снабженным двусторонним аудиосопровождением, а также двусторонним видеоканалам, ибо велика вероятность подмены. Можно «взломать» экологически чистые «умные решения» – термостаты для отопления, «умные» светодиодные лампы, что приводит к возможности внешнего (несанкционированного) управления системой освещения. «Умные дверные звонки» и системы видеозаписи в XXI веке также оказались уязвимыми, что составляет счастье и интерес для потенциальных воров с соответствующим образованием.

Самое неприятное и страшное в том, что интернет вещей не ограничен уязвимостями описанного характера: он реально может быть использован против нас – граждан и пользователей,

причем оплативших его из своих средств. Некоторые модели телевизоров Samsung могут записывать информацию и передавать третьим лицам обо всем, что слышат их микрофоны и, возможно, видят их камеры. К сожалению, то, о чем я сейчас пишу, не химера и не результат паранойи. Не важно, какая именно электронная вещь взламывается. Ею может в конкретном случае стать бытовой холодильник, дверь, автомобиль или медицинское оборудование в клинике. Все эти и многие другие устройства, которыми можно управлять дистанционно, могут быть использованы для упрощения доступа и к другим интернет-вещам. Еще интереснее соединять полученные обрывки информации для получения целостной картины в формате даже простого анализа того, что творится вокруг. То же касается и рассмотренных в книге устройств.

Такие электронные устройства, использующие систему интернета вещей, должны защищаться так же, как персональные компьютеры, телефоны, КПК и планшеты, если не строже. Они не должны хранить пароли в виде простого текста, им нельзя позволять собирать данные о пользователе – в любых целях. Поэтому читатели моей книги и потребители таких устройств – в общем смысле – должны понимать потенциальные опасности Wi-Fi-управления наряду с рекламой производителя их инновационных функциональных признаков.

3.1.2. Варианты совершенствования безопасности системы интернета вещей

Для реализации такой практической идеи используют сеть Pi, на которой будет крутиться веб-сервер, аккумулирующий собранные данные. Управлять несколькими розетками, каждая со своим IP, через веб-сервер не очень удобно. Конечно же, все современные устройства управляются сейчас с мобильных приложений, и никаких проблем с реализацией любого произвольного поведения не существует. Но одно дело – это управляться с мобильного приложения, а другое – реализовывать автономную логику, к примеру включение вытяжки в ванной при повышении влажности, для этого нужен стационарный девайс, который будет за всем этим следить. Этим устройством вполне может служить модуль, реализованный на MCU AR9331.

3.2. Практические модели управляемых электронных устройств в системе интернета вещей

В качестве бытовых устройств рассмотрим «электронные розетки», внешний вид которых представлен на рис. 3.1.

Рис. 3.1. Внешний вид электронных розеток в системе интернета вещей

Возможности исполнительных устройств таковы:

- удаленное включение и отключение электрических приборов через сеть интернет;
- удаленное управление Wi-Fi-розеткой с ПК, ноутбука, планшета или смартфона;
- бесплатное приложение для удаленного управления Wi-Fi-розеткой, в том числе для Android и iPhone;
- сервис управления доступен 24 ч в сутки;
- возможность управления несколькими розетками с одной учетной записи;
- таймер для автоматического включения и отключения управляемой Wi-Fi-розетки;
- максимально допустимая сила тока 10 А;
- максимально допустимая мощность подключенного электрического устройства не более 2,5 кВт;
- Wi-Fi 2.4 ГГц стандарт IEEE801.11b/g.

Необходимым условием для удаленного управления электронной розеткой является наличие интернета.

3.2.1. Совместимость устройств

Как правило, модели управляемых в системе интернета вещей электронных розеток совместимы с Android-устройствами с поддержкой Wi-Fi и версией ОС 4.0 и выше, а также iOS-устройствами с поддержкой Wi-Fi и версией ОС Android 5.0 и выше.

3.2.2. Принцип работы устройств

Электрические осветительные лампы, вентиляторы, обогреватели, бойлеры, насосы, все иные устройства активной нагрузки можно включать из любой точки земли, где есть возможность подключения к сети интернет в системе интернета вещей. При этом управление устройствами нагрузки осуществляется с сотового телефона, планшета, КПК или ноутбука.

Управляемая розетка позволяет не только включать/выключать электронные устройства дистанционно, но и создавать однократное событие или расписание по дням недели. Пользоваться этим функционалом весьма просто: установите время, когда хотите включить/выключить устройство, и ждите реакции.

Управляемая розетка использует Wi-Fi-сеть и интернет, благодаря этому пользователь может управлять розеткой HL0107 с мобильного устройства, даже находясь в пути (в движении). Устройство HL0107 (представленное на рис. 3.1 и аналогичные) задумано как часть системы интернета вещей. Однако сей полезный электронный прибор может использоваться и отдельно. Для этого варианта необходимо включить обогреватель на даче, чтобы к приезду хозяев в доме было тепло. Она поможет в ряде других случаев. Забыли отключить насос в доме или свет в гараже? Не беда. С помощью такого устройства можно поправить забывчивость дистанционно.

3.2.3. Как пользоваться?

Краткая инструкция на примере работы с планшетом Apple iPad такова.

1. Скачиваем программу – сканер QR-кода, к примеру под названием Scanvi, устанавливаем ее на планшет.

2. Сканируем код с Wi-Fi-розетки, находим по нему программу I-smart, устанавливаем ее.
3. Включаем розетку в сеть, ждем 2 мин.

Внимание, важно!

Обеспечиваем нажатие на кнопку (на корпусе розетки – в нее же встроен индикатор) около 4 с, при этом необходимо поймать момент моргания синего светодиода – это «режим ожидания».

Следующим шагом запускаем программу I-smart. Нажимаем снова на моргающую синим кнопку индикации, кнопка должна быстро моргать сине-зеленым светом, ловим этот момент (если этого не произошло, то повторяем – это «режим определения устройств планшетом»).

Затем заходим в программу I-smart в меню **Add new Device**, вводим пароль для доступа розетки к интернету (по Wi-Fi) – к роутеру для удаленного подключения. На этом этапе, если все сделано правильно, на корпусе устройства сине-зеленый свет моргает очень быстро, что означает – программа найдена. Если этого не произошло, то необходимо повторить поиск в «режиме ожидания».

Если поиск устройств прошел успешно, заходим в пункт **Smart Socket** и видим на дисплее телефона (ноутбука, КПК, планшета) устройство, нажимаем (кликаем) на него – и только после этого можем управлять розеткой, режим включения которой подтверждается постоянной работой (свечением) синего светодиода (в кнопке включения).

3.2.4. Распространенные ошибки подключения

Без учета наиболее распространенных ошибок подключения рассматриваемых устройств не обойтись:

- неправильно введен пароль доступа к Wi-Fi на роутере (невозможно подключиться к интернету);
- неправильно выставлено время в роутере (некорректно работает управление по таймеру).

Обе ошибки устраняются внимательным отношением при включении и режиме инициализации устройства в сети Wi-Fi.

В некоторых моделях управляемых электронных розеток предусмотрено наличие USB-порта. В каждой есть защита от короткого замыкания и специальный стикер с информацией о QR-коде на корпусе розетки – для установки программного обеспечения. Кроме рассмотренных выше, существуют и другие модели с тем же функционалом, но с разным внешним видом, реализованные различными производителями.

3.3. Совместимые электронные устройства

3.3.1. Беспроводная Wi-Fi-управляемая розетка Orvibo WiWo-S20

На рис. 3.2 представлена беспроводная Wi-Fi-управляемая электрическая розетка модели Orvibo WiWo-S20.

Рис. 3.2. Внешний вид электронной розетки Orvibo WiWo-S20

Модель Orvibo WiWo-S20 предназначена для удаленного включения и отключения бытовых электроприборов с напряжением 220 В и мощностью до 2 кВт. Устройство работает с приложениями FE Wi-Fi Socket и WiWo, которые можно в свободном режиме (бесплатно) скачать на ресурсах интернета, таких как Google Play или Apple Store. Практика действия такова, что достаточно

установить любое приложение, затем настроить розетку и пользоваться. В обоих вариантах приложений предусмотрена возможность подключения до 50 розеток WiWo-S20 с пользовательской индивидуальной настройкой (к примеру, режим тайминга). Необходимым условием для удаленного управления розеткой Smart Socket WiWo-S20 является наличие Wi-Fi-соединения розетки с интернетом.

Технические возможности Orvibo WiWo-S20

- Удаленное включение и отключение электрических приборов через сеть интернет;
- возможность установки расписания для автоматизации работы домашних устройств;
- удаленное управление Wi-Fi-розеткой с вашего смартфона или планшета;
- бесплатное приложение FE Wi-Fi Socket или WiWo на Google Play или Apple Store для удаленного управления Wi-Fi-розеткой для операционных систем Android и iOS;
- возможность управления несколькими розетками WiWo-S20;
- таймер для автоматического включения и отключения управляемой Wi-Fi-розетки;
- максимально допустимая сила тока 10 А;
- максимально допустимая мощность подключенного электрического устройства не более 2000 Вт;
- Wi-Fi 2.4 ГГц стандарт 802.11b/g/n;
- стандарт беспроводной связи: Wi-Fi 2,4 ГГц 802.11b/g/n;
- частота беспроводной связи: 2,412–2,484 ГГц;
- энергопотребление: менее 0,3 Вт;
- макс. напряжение питания (переменный род тока) 90–260 В;
- рабочая температура: –20...70 ˚С;
- рабочая влажность: менее 80%.

3.3.2. Беспроводная электронная розетка BePlug-15

Модель BePlug-15 представлена на рис. 3.3.

Технические возможности BePlug-15

Технические возможности BePlug-15 практически сопоставимы с рассмотренными выше аналогичными устройствами (разве что данная модель может управлять более мощной активной электрической нагрузкой):

- удаленное включение и отключение электрических приборов через сеть интернет;
- удаленное управление Wi-Fi-розеткой с ПК, ноутбука, планшета или смартфона;
- бесплатное приложение для удаленного управления Wi-Fi-розеткой, в том числе для Android и iPhone;
- сервис управления доступен 24 ч в сутки;
- возможность управления несколькими розетками BePlug-15 с одной учетной записи;
- таймер для автоматического включения и отключения управляемой Wi-Fi-розетки;
- входное напряжение: 220 В, 50 Гц;
- выходное напряжение: 220 В, 50 Гц;
- максимальный рабочий ток: 15 А;
- собственное потребление: 0,5 Вт/ч;
- рабочая температура: от –10 до + 45 °С;
- максимально допустимая мощность подключенного электрического устройства не более 3,5 кВт;
- Wi-Fi 2.4 ГГц стандарт IEEE801.11b/g.

Рис. 3.3. Внешний вид электронного устройства BePlug-15

Необходимым условием для удаленного управления розеткой BePlug-15 является наличие постоянного Wi-Fi-соединения розетки BePlug-15 с сетью интернет.

Правила применения BePlug-15

Подключите управляемую розетку BePlug-15 к домашнему (бытовому) беспроводному Wi-Fi-роутеру, подключенному к сети интернет, зарегистрируйте Wi-Fi-розетку на интернет-портале http://plug.b-home.me. Следующим шагом установите бесплатное приложение для удаленного управления розеткой BePlug-15 для iOS или Android на смартфон. Теперь розетка подключена, можно удаленно управлять ее включением и отключением.

Беспроводная управляемая электрическая розетка BePlug-15 предназначена для удаленного включения и отключения бытовых электроприборов с напряжением 220 В и мощностью до 3,5 кВт. Пользователь имеет возможность управлять всеми подключенными устройствами через облачный интернет-сервис бесплатно, через личный кабинет из любой точки мира, с любого устройства. Возможность подключения – до 30 аналогичных розеток BePlug-15 на личный кабинет с индивидуальной настройкой. Сделать это можно аналогичным образом.

Быстрая настройка электронного устройства BePlug-15

Для удобства пользователя настройка устройства производится в полуавтоматическом режиме. Для этого необходимо установить бесплатную программу, работающую с разными типами устройств: телефоны, планшеты или персональные компьютеры, ноутбуки, – и затем пошагово сделать определенные действия, описанные ниже.

1. Выберите тип системы вашего устройства: iOS, Android или Windows. Запустите установку программы BePlug. Используйте QR-коды или зайдите по соответствующим устройству ссылкам, указанным ниже.
2. Подключите вашу Wi-Fi-розетку BePlug-15 к сети электропитания 220 В.
3. Нажмите кнопку на BePlug-15 и удерживайте ее нажатой в течение 10 с до тех пор, пока синий светодиод в корпусе BePlug не начнет быстро мигать.
4. Запустите программу BePlug, которую вы установили ранее для настройки розетки (см. шаг 1).
5. После запуска программы нажмите пункт меню **Регистрация**, затем введите адрес пользовательской электронной

почты (e-mail будет использоваться в качестве имени пользователя). На указанный адрес придет письмо с кодом подтверждения, который нужно ввести в соответствующее поле, и в завершение установите ваш индивидуальный пароль.

6. Используя e-mail-адрес и установленный пароль, войдите в приложение. После входа приложение спросит: «Хотите ли вы подключить новое устройство?» На вопрос необходимо ответить «Да».
7. Этот шаг актуален только для пользователей iOS. В пользовательском iPhone или iPad в настройках в меню **Настройки → Wi-Fi** найдите Wi-Fi-сеть с именем «РОЗЕТКА» и подключитесь к ней.
8. Вернитесь в программу BePlug и настройте параметры доступа к сети домашнего роутера (имя сети SSID, пароль) и имя, которое хотите дать вашей Wi-Fi-розетке (к примеру, «включение света на даче»). После этого нажмите кнопку **Сохранить**, и программа настроит розетку (5–10 с).
9. Устройство настроено, и теперь вы можете управлять им со своего мобильного устройства или компьютера. Просто переключайте слайдер. Контролировать состояние связи с Wi-Fi-розеткой можно по индикатору справа от имени, которое вы, как пользователь, дали розетке. Кроме того, можно создавать группы устройств, устанавливать включение или выключение Wi-Fi-розетки по таймеру. После этих несложных шагов можно пользоваться управляемой розеткой BePlug-15.

Практические возможности и особенности устройства BePlug-15

- Удаленное включение и отключение электрических приборов через сеть интернет;
- удаленное управление Wi-Fi-розеткой с ПК, ноутбука, планшета или смартфона;
- бесплатное приложение для удаленного управления Wi-Fi-розеткой, в том числе для Android и iPhone;
- сервис управления доступен 24 ч в сутки;
- возможность управления несколькими розетками BePlug-15 с одной учетной записи;
- таймер для автоматического включения и отключения управляемой Wi-Fi-розетки;

- максимально допустимая сила тока 15 А;
- максимально допустимая мощность подключенного электрического устройства не более 3,5 кВт;
- Wi-Fi 2.4 ГГц стандарт IEEE801.11b/g;
- необходимым условием для удаленного управления розеткой BePlug-15 является наличие постоянного Wi-Fi-соединения розетки BePlug-15 с сетью интернет.

У электронного устройства BePlug-15 русскоязычное приложение, «облако» находится в России. Сервисная поддержка в Москве. Исполнительное реле на 17 А. Если вы приобретаете в дальнейшем контроллер BeHome-120, то розетка опционально будет работать с ним офлайн, так как часть облака мы перенесли в BeHome-120. Отличия этого устройства таковы.

При выключении и включении электричества проблем не наблюдается, связь будет восстановлена автоматически. Для розетки требуется минимальная полоса, замечено, что обычно даже сети 2G достаточно. Однако если существует нестабильность в интернет-соединении, то говорить о 100%-ной доступности сервиса сложно. Важна не полоса пропускания, а стабильность соединения. У заинтересованного пользователя могут возникнуть практические вопросы, требующие разрешения – по существу.

Пользователь программирует расписание включения и выключения устройств. Если вдруг интернет пропадает, понятно, что управлять нельзя. А работа по заранее составленному расписанию проходить будет? Расписание хранится на сервере, поэтому для розетки BePlug-15 необходимо постоянное подключение к интернету. Включение/выключение возможно по таймеру. Соответственно, без доступа к интернету локальное управление невозможно. В версиях без «облачной схемы» управления не предусмотрено. Надежность облаков с каждой модификацией растет. Почтовые серверы – это тоже «облако». Узким местом является сама домашняя сеть Wi-Fi.

3.3.3. Электронное устройство SWS-A1

Практически же на примере, рассмотренном в начале 3-й главы, Wi-Fi-розетки модели HL0107 (рис. 3.1) ее основной дистанционный модуль признан универсальным устройством. На рис. 3.4 представлен его внутренний вид в корпусе розетки SWS-A1 производства Финляндии.

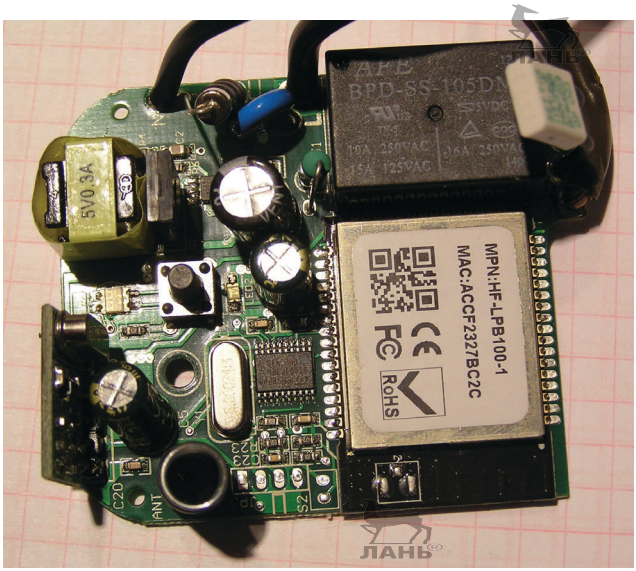

Рис. 3.4. Внутренний вид дистанционного модуля в корпусе розетки SWS-A1 производства Финляндии

На рис. 3.5 дан внешний вид розетки SWS-A1.

Рис. 3.5. Внешний вид розетки SWS-A1

3.3.4. Электронное устройство DSP-W215

Электрическая розетка с интегрированной точкой доступа Wi-Fi для системы интернета вещей модели DSP-W215 также может использоваться для быстрого и удобного подключения датчиков температуры, системы безопасности, датчиков дыма, камер. Настойка и управление осуществляются через веб-интерфейс или специального клиента для ПК.

Внешний вид розетки DSP-W215 производства компании D-Link представлен на рис. 3.6.

Рис. 3.6. Внешний вид устройства DSP-W215

На рис. 3.7 представлена блок-схема подключений для управляемых по системе интернета вещей розеток.

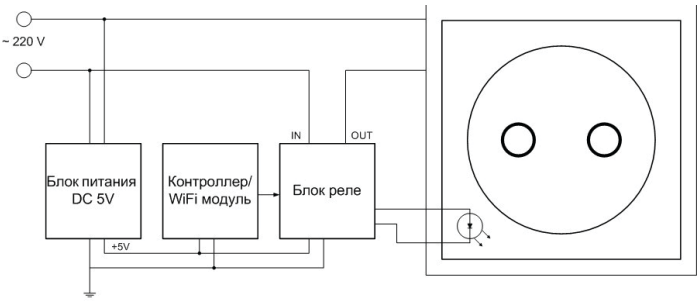

Рис. 3.7. Блок-схема подключений для управляемых электронных розеток

3.4. Как практически можно пользоваться описанными устройствами

В моем хозяйстве необычное применение реализовано для электрического бойлера. Пользуюсь электронной розеткой в загородной резиденции, когда приезжаю/уезжаю на выходные или в отпуске. Бывает, что забываю отключить бойлер, а он продолжает греть воду до 90 ˚С. Сейчас его можно включить/отключить удаленно. Реакция розетки на включение/отключение менее секунды. Подобные устройства дистанционного управления (а главное – практика их применения) достаточно полно и хорошо описаны в книге: *Кашкаров А. П.* Электроника на даче и в загородном доме. М.: ДМК, 2009. 288 с. ISBN 978-5-94074-577-8. Импульс к новым разработкам или инновационному применению промышленных электронных устройств в моем доме был заложен еще 10 лет назад.

Но даже в «новых» промышленных управляемых розетках (любой модификации) есть определенные «минусы». Не в последнюю очередь это цена устройства, которая в розницу сегодня составляет около 1800 руб. В этой связи есть практическое альтернативное решение – сделать такое устройство своими руками: к примеру, может иметь место решение, предложенное в [6]. На шине W1, TWI или RS-485 самодельное устройство обойдется в несколько раз дешевле.

Провести интернет через розетку позволяет специальное устройство стандарта HomePlug (PowerLine-адаптер, к примеру фирмы Tenda). Необходимо несколько однотипных устройств – по одному на каждый компьютер. Выглядит он как небольшая коробочка с вилкой – наподобие зарядки от мобильного, – имеющая сетевой разъем RJ-45 под витую пару.

Несколько PowerLine-адаптеров – столько, сколько нужно прицепить компьютеров. Вставляете в один из них патчкорд, соединяя с роутером, настроенным на интернет-провайдера («PowerLine» означает в переводе «электропроводка»). В соседнем помещении вы вставляете точно такой же PowerLine-адаптер и подключаете его витой парой к другому компу. Всё, интернет через розетку 220 В проведен. Остальные параметры локальной сети (IP, шлюз и др.) настраиваются так же, как если бы пользователь тянул стандартным способом сетевой кабель.

Как это работает? Стандарт HomePlug, лежащий в основе локальной PowerLine-сети, характеризуется преобразованием поступающих через сетевой порт Ethernet данных в высокочастотный сигнал, который транслируется через розетку в электрическую сеть. В другой комнате такой же адаптер получает комбинированный сигнал с передаваемыми пакетами данных. Остается только демодулировать, распознать высокочастотный сигнал, преобразовать его и вывести на сетевой Ethernet-порт, откуда он поступает в другой ПК, или по Wi-Fi. Такой тип подключения намного стабильнее, чем при использовании обычного Wi-Fi-повторителя, поскольку помехи минимальные и качество сигнала почти не падает.

Существуют PowerLine-адаптеры с уже встроенным Wi-Fi-модулем, то есть, подключив его в розетку, можно вывести интернет через электрическую розетку не только по кабелю, но и беспроводным способом, а значит, можно будет к нему подключиться с любого устройства, поддерживающего Wi-Fi, без докупки отдельного оборудования для ретрансляции беспроводного сигнала. Адаптеры с уже встроенным Wi-Fi в современных бытовых обстоятельствах никому не покажутся лишними (избыточными). Внешне их можно распознать по наличию характерной антенны, хотя ее может и не быть – надо смотреть описание на коробке или в инструкции.

У данного метода есть свои недостатки. Во-первых, работающие электроприборы могут создавать значительные помехи, из-за которых будут падать качество связи и скорость. Общая же пропускная способность построенной на PowerLine-адаптерах сети делится между всеми клиентами; чем больше компьютеров, тем ниже скорость и надежность.

Дальность действия сети ограничена 200 м и зависит от качества проводки. Электрическая проводка в старых домах без «свежего» ремонта оставляет желать лучшего. И если электролиния имеет трехфазовую структуру, то для осуществления интернета через розетку необходимо в распределительный электрощит установить устройство фазового сопряжения. Поэтому необходимо подключать данные устройства в сопряженные, параллельно подключенные розетки. Тем не менее, несмотря на описанные недостатки, попробовать стоит, тем более что настройка этих устройств очень проста и позволит организовать локальную сеть на весьма приличное расстояние. Если при построении локаль-

ной сети в частном доме приходится использовать несколько ретрансляторов и антенн для стабилизации Wi-Fi-сигнала, или сверлить перекрытия и тянуть десятки метров кабелей, то здесь для расширения достаточно лишь купить дополнительный адаптер. Перспективы технологии PowerLine-сети очень заманчивы: данным способом можно объединить всю бытовую технику в одну умную систему с единым центром управления на персональном компьютере.

Как настроить HomePlug PowerLine-адаптеры? Первый адаптер подключают в электрическую розетку, а патчкордом подключают к роутеру в его порт LAN. Последующие подключают к другим розеткам и соединяют с персональными компьютерами, которые входят в локальную сеть. После технических этапов соединения кабелей и вставки устройств в розетки находят на их корпусах кнопки **SYNC** или **PAIR**. Нажимаем их по очереди на всех адаптерах, и таким образом они автоматически вступают в режим «коннекта» и начинают обмениваться информацией.

При успешном подключении друг к другу на корпусе, помимо прочих индикаторов, должен загореться светодиод. Также загорятся индикаторы **Power**, **Сеть** и **Wi-Fi** (при наличии беспроводного модуля). Остальные настройки, необходимые для работы пользовательского оборудования в локальной сети, производятся в маршрутизаторах и в самих ПК. Тем не менее необходимо учесть IP-адреса данных адаптеров по умолчанию, чтобы иметь возможность зайти для управления в их панель конфигурации. Эти данные указаны чаще всего на наклейке на корпусе адаптеров. К примеру, PowerLine-адаптеры фирмы D-Link в моем случае имеют IP 192.168.0.222. Соответственно, вся сеть должна иметь такой же вид – у роутера внутренний IP 192.168.0.1, а у остальных компьютеров адреса вида 192.168.0.XXX, где «XXX» – число от 2 до 253.

Если же в конкретном случае работает на маршрутизаторе DHCP-клиент, раздающий IP автоматически, поменяйте адрес роутера (на указанный выше – см. пример). Также актуален вопрос безопасности – ведь, приобретя адаптер этой же фирмы, любой сосед, который каким-то образом связан с вашей пользовательской разводкой электросети, сможет бесплатно пользоваться вашей сетью. Но это не проблема – для обеспечения максимальной защиты можно контролировать подключения сторонних пользователей, для чего существует специальная утилита

(ПО, к примеру, от компании TP-Link), с помощью которой можно с одного ПК контролировать все подключенные к «розеткам» устройства.

Работает она так. После установки в главном окне пользователь видит MAC-адрес того адаптера, к которому ПК подключен. Кликаем по его иконке с помощью кнопки **Connect**. При успешном подключении появится надпись **Connected on High Speed** и начнется сканирование всей сети, а обнаруженные адаптеры отобразятся в списке ниже.

Обратите внимание на пустое поле пароля (**Password**). Кликните по строке, нажмите на кнопку **Enter Password** и задайте вручную уникальный ключ, указанный на наклейке, помещенной на дне корпуса адаптера. Проделываем то же самое со всеми устройствами из списка, после чего переходим на вкладку **Privacy** – именно тут настраивается безопасность. По умолчанию вся сеть является открытой (потенциальный сосед может ее легко использовать в своих целях). Но пользователь может и для безопасности должен сделать свою сеть приватной. Для этого надо задать свое уникальное название в поле **Private Network Name**, чтобы активировать протокол шифрования DES. Далее нажимают кнопку **Set All Devices**, чтобы добавить в нее все имеющиеся в локальной сети компьютеры.

Во второй главе книги [6] довольно подробно описаны многофункциональные розетки с дистанционным управлением как промышленного изготовления, так и сделанные своими руками. Особое внимание уделено тому, что обычно в многоквартирных домах реализуется одна и та же схема электропроводки: в домах в одной из комнат розетки объединены в блоки по два двухрозеточных модуля вплотную друг к другу, в двух стандартных пластиковых «подрозетниках» соответственно. Что надо пользователю? Во-первых, получать команды через Wi-Fi и выдавать соответствующие управляющие сигналы на замыкание контактов. То есть нужен модуль контроллера с Wi-Fi. Поскольку существует стандартная плата на AR9331 и ее модификации, то реализация собственноручного изготовления Wi-Fi-управления не представляет проблемы.

Исполнительный блок – токовый ключ с реле, коммутирующие контакты которого рассчитаны на ток 16 А и напряжение в сети 220–250 В. В этом случае подходит практически любая схема и (или) модуль, готовый к выполнению описанной задачи, то есть

управляемый импульсом амплитудой 5...9 В. Питать два модуля (Wi-Fi и исполнительного устройства) надо напряжением 5–8 В, для чего вполне подойдет любой маломощный адаптер сетевого питания с соответствующим выходным напряжением. Дополнительно потребуется плата с обвязкой и разъемом RJ-45.

ЛИТЕРАТУРА

1. Изделия электронной техники – импортные компоненты. Каталог 2018 г. / Симметрон.
2. *Кашкаров А., Козлов А.* Techwell: комплексный подход к обработке видеосигналов // CHIPNEWS Украина. 2007. № 1. С. 17.
3. *Кашкаров А.* Система видеонаблюдения для охранного телевидения на основе видеоконтроллера TW2700 фирмы Techwell Inc. // Компоненты и технологии. 2008. № 9. С. 22.
4. *Кашкаров А. П.* Электроника на даче и в загородном доме. М.: ДМК, 2009. 288 с. ISBN 978-5-94074-577-8.
5. *Кашкаров А. П.* Электронные устройства для глушения беспроводных сигналов (GSM, Wi-Fi, GPS и некоторых радиотелефонов). М.: ДМК Пресс, 2016. 96 с. ISBN 978-5-97060-210-2.
6. *Кашкаров А. П.* Управление и настройка Wi-Fi в своем доме. М.: ДМК Пресс, 2016. 64 с. ISBN 978-5-97060-351-2.
7. *Кашкаров А. П.* Радиолюбителям: схемы для быта и отдыха. М.: ИП РадиоСофт, 2003. 96 с.: ил. (Книжная полка радиолюбителя. Вып. 3.)
8. *Кашкаров А. П.* 500 схем. Радиолюбителям: электронные датчики. СПб.: НиТ, 2007. 208 с.: ил.
9. *Кашкаров А. П.* Чудо XX века: реальность и перспективы // Радиомир – Ваш компьютер. 2005. № 10. С. 25.
10. *Скуснов А.* Тестирование точек доступа: беспроводной интернет в каждую квартиру // Upgrade: компьютерный еженедельник. 2004. № 44 (186).

Справочный материал интернета

1. http://www.motoizh.ru.
2. http://www.tadviser.ru/index.php: Что_такое_интернет_вещей_(Internet_of_Things,_IoT).
3. http://www.topobzor.com/obzor-10-oblachnyx-xranilishh-dannyx/.html: Что такое 1G, 2G, 3G, 4G и всё, что между ними.

4. https://habrahabr.ru/post/112: «Умный дом» технологии.
5. http://sensehome.ru/technology.htm: Google про интернет вещей (Internet of things, IoT).
6. https://www.youtube.com/watch?v=xnPsW4_FeRA: Открытая лекция Роба ван Краненбурга об интернете вещей.
7. https://www.youtube.com/watch?v=zacDuBofPHE: Материалы «The 4th Annual Internetof Things Europe: Shaping Eu-rope's Future Internet Policy – Theroadto Horizon 2020».
8. http://www.eu-ems.com/summary.asp?event_id=124&page_id=991&/: «Internet_of_things».
9. https://en.wikipedia.org/wiki/Internet_of_things.
10. http://entertainment.ivlim.ru/showsite.asp?id=75871.
11. http://www.ntpo.com/electronics.
12. http://www.povt.ru/povt2/?mode=downloads&area=9.
13. http://qrx.narod.ru/spravka/pr_om.htm.
14. http://www.platan.ru/td_pltn/15.htm.
15. http://www.jammer.su/.
16. http://www.wiki-telesys.1gb.ru/edic-mini_tiny_b21.
17. http://www.sdelaysam-svoimirukami.ru/622-glushitel-chastoty-tele-i-radio-signalov.html.
18. http://kupsilla.narod.ru/lake.htm.
19. http://fsell.biz/showthread.php?t=7309.
20. http://www.smersh.ru/prod/st110.shtml.
21. http://pulti-came.ru/index.php.
22. http://vrtp.ru/index.php?act=categories&CO...le&article=1260.
23. http://Wi-Fika.ru/internet-cherez-rozetku-homeplug-adapter-powerline.html.
24. https://ru.wikipedia.org/wiki/Wi-Fi.
25. http://Wi-Ficenter.ru/xarakteristiki-koaksialnyx-kabelej/.
26. Get IEEE 802. http://standards.ieee.org/getieee802/download/802.11-2007.pdf.
27. standards.ieee.org – ссылка на страницу скачивания полного официального текста стандартов.

28. Тестирование альтернативных прошивок современных роутеров: http://www.overclockers.ru/lab/40205/Testirovanie_alternativnyh_proshivok_sovremennyh_routerov.html.
29. Virtual Wi-Fi в Windows 10: https://ru.intel.com/business/community/index.php?automodule=blog&blogid=1960&showentry=1126.
30. Интернет-газета Comnews публикует материал на тему регистрации радиоэлектронных средств с Wi-Fi: http://rkn.gov.ru/main/about/858/887.shtml?id_news=62.
31. Use of laptop computers connected to internet through Wi-Fi decreases human sperm motility and increases sperm DNA fragmentation (англ.): http://www.fertstert.org/article/S0015-0282%2811%2902678-1/fulltext.
32. www.fertstert.org.
33. Wi-Fi не вреден для здоровья: «Вокруг света» // http://www.vokrugsveta.ru/news/996/.

Книги издательства «ДМК Пресс» можно заказать в торгово-издательском холдинге «Планета Альянс» наложенным платежом, выслав открытку или письмо по почтовому адресу: **115487, г. Москва, 2-й Нагатинский пр-д, д. 6А**.

При оформлении заказа следует указать адрес (полностью), по которому должны быть высланы книги; фамилию, имя и отчество получателя. Желательно также указать свой телефон и электронный адрес.

Эти книги вы можете заказать и в интернет-магазине: **www.a-planeta.ru**.

Оптовые закупки: тел. **+7(499) 782-38-89**.

Электронный адрес: **books@alians-kniga.ru**.

Антти Суомалайнен

Интернет вещей: видео, аудио, коммутация

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com
Корректор *Синяева Г. И.*
Верстка *Паранская Н. В.*
Дизайн обложки *Мовчан А. Г.*

Формат 60×90 $^{1}/_{16}$.
Печать цифровая. Усл. печ. л. 7,35.
Тираж 200 экз.

Веб-сайт издательства: www.dmkpress.com