

# ВВЕДЕНИЕ

Сети Интернета вещей (ИВ) становятся неотъемлемой частью современной цифровой инфраструктуры, обеспечивая взаимодействие физических и виртуальных объектов в реальном времени. Широкое внедрение технологий ИВ в различные сферы — от умного дома и промышленной автоматизации до здравоохранения и транспортных систем — обусловлено их способностью повышать эффективность, снижать затраты и создавать новые сервисы. Однако интенсивное развитие экосистемы ИВ сопровождается ростом числа и опасности киберугроз, что делает актуальной проблему обеспечения информационной безопасности таких сетей.

Особенностью Интернета вещей является высокая степень гетерогенности устройств, протоколов связи и архитектурных решений, что значительно усложняет задачу их защиты. Традиционные подходы к обеспечению безопасности, разработанные для классических IT-систем, зачастую оказываются неприменимыми или недостаточно эффективными в условиях ИВ из-за ограниченности ресурсов устройств, динамичности топологии и специфики угроз.

При этом интенсивное развитие технологий ИВ закономерно ведет к увеличению интереса к ним со стороны нарушителей. В связи с этим следует ожидать роста числа компьютерных атак на сети ИВ с использованием различных средств, что делает актуальной проблему обеспечения информационной безопасности (ИВ) данных объектов.

В свою очередь управление рисками ИВ в контексте Интернета вещей требует разработки специализированных методов, позволяющих учитывать как технические, так и контекстные факторы.

К тому же существующие методики анализа рисков зачастую не способны оперативно адаптироваться к изменяющимся

условиям работы сетей ИВ. Кроме того, отсутствие достаточной статистики по инцидентам ИВ и высокая степень их неопределенности затрудняют применение классических вероятностных подходов.

Поэтому при создании и эксплуатации защищенной сети ИВ необходимо систематически осуществлять оценку и регулирование рисков, целью которых является выявление возможных угроз безопасности информации и оценка вероятности их реализации и потенциального ущерба. Особую значимость в этом случае приобретает разработка адаптивных механизмов контроля доступа, способных оперативно реагировать на изменяющуюся среду и потенциальные угрозы.

Причем внедрение технологий ИВ происходит значительно быстрее, чем приобретение необходимых профессиональных знаний и опыта для их адекватной защиты, что обуславливает необходимость использования решений и инструментов, первоначально разработанных для классических информационных систем, но с учетом специфики ИВ.

Комплексный характер проблем обеспечения безопасности в сетях ИВ требует разработки инновационных методологических подходов, основанных на риск-ориентированном управлении. В условиях, когда каждая станция в сети потенциально уязвима, возникает необходимость в строгом соблюдении установленных правил безопасности для предотвращения инцидентов как с точки зрения защиты ИВ, так и с позиций сохранения их эксплуатационных характеристик.

В этом контексте специфика современных сетей ИВ отражается в используемых подходах к анализу рисков. Особенность ИВ сетей ИВ заключается в том, что в результате атак ущерб наносится не только ресурсам самой сети, но и активам организации в целом. При этом многие активы не имеют четкого денежного выражения, что затрудняет количественную оценку возможного ущерба.

Поэтому методологическая база исследования формируется на основе комплексного подхода, включающего анализ архитектур и свойств современных сетей ИВ, систематизацию существующих методов оценки рисков, разработку теоретических моделей риск-анализа и применение современных методов нечеткой логики и нейро-нечетких систем.

Первая глава монографии посвящена фундаментальным основам исследования сетей ИВ как объекта защиты. В ней рас-

смаатриваются архитектура, характеристики и особенности ИВ-систем, проводится анализ актуальных угроз безопасности и существующих методов их нейтрализации. Особое внимание уделяется вопросам аутентификации, авторизации и контроля доступа.

Вторая глава развивает теоретическую базу исследования, представляя комплексную модель риск-анализа и управления рисками для ИВ. Здесь подробно рассматриваются параметры оценки риска, методики работы с экспертными данными и применение аппарата нечеткой логики.

Третья глава содержит описание инструментальной составляющей работы, включая реализацию методики оценки рисков на основе системы нечеткого вывода и адаптивных нейро-нечетких систем. Предложены алгоритмы обработки неточной и неполной информации.

Заключительная глава посвящена разработке риск-ориентированной адаптивной процедуры контроля доступа с использованием смарт-контрактов. В ней рассматриваются проблемы классических механизмов контроля доступа и предлагаются инновационные решения. Помимо этого, она также содержит результаты практического моделирования предложенных решений, анализ их эффективности и сравнение с существующими аналогами.

Работа выполнена при частичной поддержке РФФИ (проект 18-29-22042), а также в рамках проекта «Безопасный Интернет» (рег. № АААА-А18-118050700061-7).

Монография предназначена для специалистов в области информационной безопасности, научных работников, аспирантов и студентов, занимающихся проблемами защиты сложных киберфизических систем.

Авторы выражают благодарность сотрудникам кафедры «Системы информационной безопасности» Воронежского государственного технического университета за поддержку инициативы настоящего издания и помощь в подготовке рукописи.

Авторы будут благодарны за отзывы и пожелания, а также конструктивные предложения о сотрудничестве в области безопасности информационных технологий, которые следует отправлять по адресу:

394049, Воронеж, Ватутина 1, Региональный учебно-научный центр по проблемам информационной безопасности.

Тел./факс: (473) 252-34-20, 278-59-90.

E-mail: alexostap123@gmail.com

# 1 СЕТИ ИНТЕРНЕТА ВЕЩЕЙ КАК ОБЪЕКТ ИССЛЕДОВАНИЯ И ЗАЩИТЫ

---

## 1.1. Сущность и свойства сетей Интернета вещей

### 1.1.1. Определение понятия Интернет вещей

Интернет Вещей (Internet of Things): глобальная система связи, создающая единую среду для обмена информацией между различными устройствами. Технология позволяет объединить реальные и виртуальные объекты в единую сеть, обеспечивая их взаимодействие через современные средства связи. По сути это концепция повсеместного подключения всех возможных устройств к Интернету [1].

Вещь (Thing): в контексте Интернета вещей означает физический или цифровой объект, который обладает уникальным идентификатором, способен подключаться к сети и обмениваться данными с другими элементами системы [2].

Беспроводная или всепроникающая сенсорная сеть (Wireless/Ubiquitous Sensor Network): автономная сеть, состоящая из множества маломощных датчиков, которые автоматически формируют структуру связи и передают информацию о состоянии окружающей среды и подключенных объектов на центральный узел [3].

Пакет (Packet): базовый элемент информации, который передается между устройствами в процессе сетевого взаимодействия [4].

Межмашинная коммуникация (Machine-to-Machine Communication): технология автоматического обмена информацией между устройствами в реальном времени, которая требует минимального участия человека в процессе взаимодействия [5].

Связность: выступает ключевым показателем эффективности самоорганизующихся сетей в экосистеме Интернета вещей,

который определяет продолжительность функционирования отдельных подсетей Интернета вещей. Обязательным условием обеспечения связности является наличие уникальной идентификации для всех устройств и объектов, интегрированных в сеть [6].

Гетерогенность: одно из важнейших свойств сетей Интернета вещей, позволяющее объединять в единую систему устройства с различными программными и аппаратными платформами от разных производителей, которые могут эффективно взаимодействовать как в рамках одной экосистемы, так и в масштабных сетевых структурах [7].

Динамичность: свойство Интернета вещей, проявляющееся в способности сети к самоорганизации. Количество узлов в такой сети может произвольно меняться в пределах от нуля до максимально возможного значения, а взаимосвязи устройств формируются спонтанно для выполнения определенных задач. Структура самоорганизующейся сети включает два основных компонента: сеть доступа, где целевые узлы взаимодействуют преимущественно с ближайшими элементами без строгой иерархии, и транзитную (ячеистую) сеть, обеспечивающую более сложные маршруты передачи данных. При этом устройства в сети доступа обладают гибкостью: они могут как выполнять роль подчиненных узлов, так и становиться координаторами для других элементов системы, в то время как ячеистые узлы специализируются на маршрутизации и поддерживают множественные соединения [8].

Масштабность подключений: фундаментальная характеристика Интернета вещей, которая заключается в способности сети интегрировать огромное количество разнообразных технических устройств. В рамках этой концепции происходит массовое объединение всевозможных электронных компонентов, включая средства сбора данных, передачи информации и управления, что создает комплексную экосистему взаимосвязанных объектов [9].

Угроза: вредоносная функция или система, которая может использовать уязвимость легитимной системы. Угроза может быть только целевым активом системы ИВ [8].

Свойство угрозы: представляет собой классификацию угрозы по шагу (фальсификация, отказ, раскрытие информации, повышение привилегий), которое принимает перечисленное значение [8].

Уязвимость: уязвимость программного обеспечения, оборудования или политики использования, которая может быть использована злоумышленником для компрометации системы Ин-

тернета вещей. Уязвимости аппаратного и программного обеспечения можно выявить с помощью таких методов, как тестирование на проникновение [7].

Протокол: протоколом называется набор правил, позволяющий осуществлять соединение и обмен данными между двумя и более включенными в сеть устройствами [10].

Сеть: система, обеспечивающая обмен данными между устройствами Интернета вещей [5].

Шифрование: обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением в это же время авторизованным пользователям доступа к ней [11].

Злоумышленник: человек, намеренно идущий на нарушение из корыстных побуждений и/или выполняющий чьи-либо преступные указания, который еще не совершил действий, приведших к нарушению характеристик информационной безопасности, но имеет намерения и подготавливается к совершению преступления или готовит к совершению иных лиц [12].

Концепция Интернета вещей базируется на формировании единой цифровой экосистемы, в которой интеллектуальные приборы способны к самостоятельному взаимодействию и обмену информацией. Все элементы этой системы — от вычислительных устройств до различных механизмов — объединены общей инфраструктурой связи, функционирующей на базе стандартных интернет-протоколов или специализированных коммуникационных стандартов, обеспечивающих эффективное взаимодействие всех компонентов сети.

Проще всего представить Интернет вещей через следующую формулу [14]:

$$\text{ИВ} = \text{Датчики} + \text{Данные} + \text{Сети} + \text{Услуги}.$$

Каждый компонент играет важную роль в формировании целостной системы: датчики собирают информацию об окружающем мире, данные обрабатываются и анализируются, сети обеспечивают передачу информации, а услуги предоставляют конечные решения пользователям.

Технологии ИВ находят широкое применение в различных сферах. В здравоохранении они позволяют осуществлять дистанционный мониторинг пациентов и контроль за состоянием здоровья. В сфере энергетики и ЖКХ системы помогают оптимизировать потребление ресурсов и управлять энергопотреблением. Умный дом предоставляет возможности для автоматизи-

зации бытовых процессов, управления освещением и климатом, обеспечения безопасности жилища.

В транспортной сфере технологии ИВ способствуют мониторингу транспортных потоков и оптимизации маршрутов. Промышленность получает инструменты для автоматизации производства, мониторинга оборудования и контроля качества. Городская инфраструктура развивается в направлении создания умных городов с оптимизированной средой и эффективными коммунальными услугами.

Развитие Интернета вещей открывает широкие возможности для улучшения качества повседневной жизни, оптимизации рабочих процессов, создания комфортной городской среды и развития инновационных сервисов. Технология способствует автоматизации различных сфер деятельности и повышению эффективности использования ресурсов.

Интеграция технологий Интернета вещей порождает целый комплекс проблем в сфере обеспечения информационной безопасности. Ключевая проблема заключается в том, что существующие защитные механизмы не способны полностью обеспечить необходимый уровень безопасности в новой цифровой среде. Огромное количество взаимосвязанных устройств, необходимость постоянного взаимодействия элементов, глобальная доступность и круглосуточная работоспособность сервисов создают потенциальные риски для ИВ и шансы для злоумышленников.

Для успешного развития Интернета вещей требуется комплексный подход, включающий создание надежных стандартов безопасности, разработку новых методов защиты данных, оптимизацию взаимодействия между устройствами и обеспечение масштабируемости систем. Важно также учитывать потребности конечных пользователей и обеспечивать удобство использования технологий.

При успешном решении этих задач Интернет вещей станет ключевым фактором развития цифровой экономики и повышения качества жизни людей, открывая новые горизонты для инноваций и технологического прогресса в различных сферах деятельности.

### 1.1.2. Концепция Интернета вещей

Интернет вещей — это социотехническая система цифровых устройств, людей, животных, различных датчиков и сенсоров, которые имеют уникальные идентификационные номера (адреса)

и связаны между собой с помощью технологий передачи данных по сети Интернет.

Вещью в Интернете вещей могут быть различные объекты: сельскохозяйственное животное с биочипом, человек с имплантированной умной инсулиновой помпой, всевозможные устройства технологии «умный дом», камеры видеонаблюдения, датчики на производстве или любой другой объект, который обладает своим уникальным адресом в пространстве сети Интернет и способен осуществлять обмен данными.

Концепция объединения умных устройств в единую сеть обсуждалась еще в начале 80-х годов прошлого столетия. В это время в университете Карнеги–Меллона был модифицирован для подключения к Интернету торговый автомат [15], который был способен уведомить компанию-владельца о количестве оставшихся товаров в нем [16]. В 1991 году М. Вайзер выпустил статью о повсеместных вычислениях на разнородных устройствах, а на академической площадке UbiComp зародилась современная концепция технологии Интернета вещей [17, 18].

Реза Раджи в начале 1994 года в статье в журнале «IEEE Spectrum» описал идею обмена между различными устройствами как «перемещение маленьких пакетов с данными на большой набор узлов с целью интеграции и автоматизации всего, от бытовой техники до целых заводов». Спустя немного времени компании Microsoft и Novell предложили свои варианты реализации этой идеи at Work и NEST соответственно. На Всемирном Экономическом Форуме в начале 2000-х годов в Давосе профессор В. Джой презентовал концепт технологии обмена между устройствами как часть проекта «Six Web» [19].

Термин «Интернет вещей» придумал и описал К. Эштон из компании Procter & Gamble в 1999 году [20, 21], хотя он предпочитает фразу «Интернет для вещей» [22]. Для того чтобы привлечь внимание руководства P&G к проблеме технологии RFID — идентификации с помощью радиочастот, Кевин назвал свою презентацию «Интернет вещей», чтобы добавить в название модное направление того времени — Интернет [23, 24]. В 1997 году появилась книга профессора Н. Гершенфельда «Когда все начинает задумываться», в которой было описано детальное представление о концепции Интернета вещей и о дальнейшем векторе развития этой технологии [25].

Технология развивалась на основе конвергенции беспроводных соединений, электромеханических систем и Интернета. Она

обеспечила интеграцию операционных и информационных технологий, что позволило анализировать неструктурированные данные, генерируемые машинами, и извлекать из них информацию, необходимую для повышения эффективности и совершенствования процессов.

Определяя Интернет вещей как «момент времени, когда к интернету подключено больше вещей, чем людей», компания Cisco Systems подсчитала, что ИВ «родился» в период между 2008 и 2009 годами, при этом соотношение вещей к людям выросло с 0,08 в 2003 году до 1,84 в 2010 году в количественном эквиваленте [26].

Эволюция Интернета вещей началась с взаимодействия машина — машина. Machine-to-Machine (далее — M2M) взаимодействие — это общепринятое название для технологий, обеспечивающих связь машин друг с другом и позволяющих обмениваться информацией в одностороннем порядке, без вмешательства человека [27-31].

Технологии M2M легли в основу подключений для Интернета вещей. Это позволило создавать сети из миллионов взаимосвязанных устройств, которые способны соединить в одну экосистему различные гаджеты, приложения для работы с ними, сервера данных, а также обеспечить обмен всей информацией между устройствами [32].

Второй ветвью базовых технологий для Интернета вещей послужили системы SCADA — диспетчерский контроль и сбор данных, которые были распространены на предприятиях. SCADA разрабатывались для управления тех-процессами оборудования, сбора данных в реальном времени, а также для анализа текущей обстановки на производстве. Системы диспетчерского контроля состояли из двух зависимых частей — аппаратуры и программного комплекса для обработки данных. Аппаратная часть отвечает за сбор информации с оборудования и последующую ее передачу на персональный компьютер, где происходит обработка и представление данных для анализа оператором в реальном времени [33]. Из SCADA развились первые системы промышленного Интернета вещей.

В конечном счете Интернет вещей перерос в сеть интеллектуальных устройств, использующих аппаратное обеспечение для сбора, хранения, обработки, шифровании, отправки и обмена данными, которые поступают из среды. К устройствам Интернета вещей относят: коммуникационное оборудование, различные датчики, конечные устройства пользователей, серверы обработ-

ки данных и др. [34]. Все устройства из экосистемы Интернета вещей совместно используют данные, собранные различной аппаратурой, с помощью подключения к облачному шлюзу или к другому пограничному устройству, где анализируются полученные данные [35]. Пример такой системы представлен на рис. 1.1.

Устройства выполняют большую часть работы без вмешательства человека, т. е. автономно, хотя взаимодействие людей с гаджетами не исключается. Например, человек может настраивать «вещи» или назначать им инструкции для выполнения, или же получать доступ к данным с помощью своего смартфона [36].

Устройства Интернета вещей также могут использовать искусственный интеллект (AI) и машинное обучение для упрощения процессов сбора и обработки данных [37].

Существует множество областей жизни, где применяется Интернет вещей. Устройства ИВ охватывают многочисленные промышленные отрасли: автомобильную, телекоммуникационную и энергетическую, производственную и даже сельскохозяйственную [38].

В потребительском сегменте ИВ используется, например, в технологии «умный дом». Интернет вещей позволяет объединить в единую систему камеры видеонаблюдения, «умные» музыкальные колонки, «умные» устройства освещения, бытовые приборы с дистанционным управлением, которые способны обмениваться между собой информацией и поддерживают управление с помощью компьютеров или смартфонов.

Интернет вещей также предоставляет износостойкие устройства для обеспечения общественной безопасности. Для того чтобы улучшить время отклика экстренных служб в случае аварии или чрезвычайной ситуации, а также проранжировать важность вызовов, устройства Интернета вещей, отслеживают жизненные показатели жертв чрезвычайных ситуаций, которые приходят с «умных» наручных часов. В настоящее время на всех опасных объектах рабочие носят умные устройства отслеживания жизненных показателей для служб экстренного реагирования [39].

Используя Интернет вещей в области здравоохранения, можно получить множество преимуществ, в том числе возможность более тщательного наблюдения за состоянием пациентов с помощью анализа данных, собираемых устройствами ИВ. Вольницы часто используют системы ИВ для управления запасами фармацевтических препаратов и медицинских инструментов. Различные стимуляторы, инсулиновые помпы, анализаторы крови,

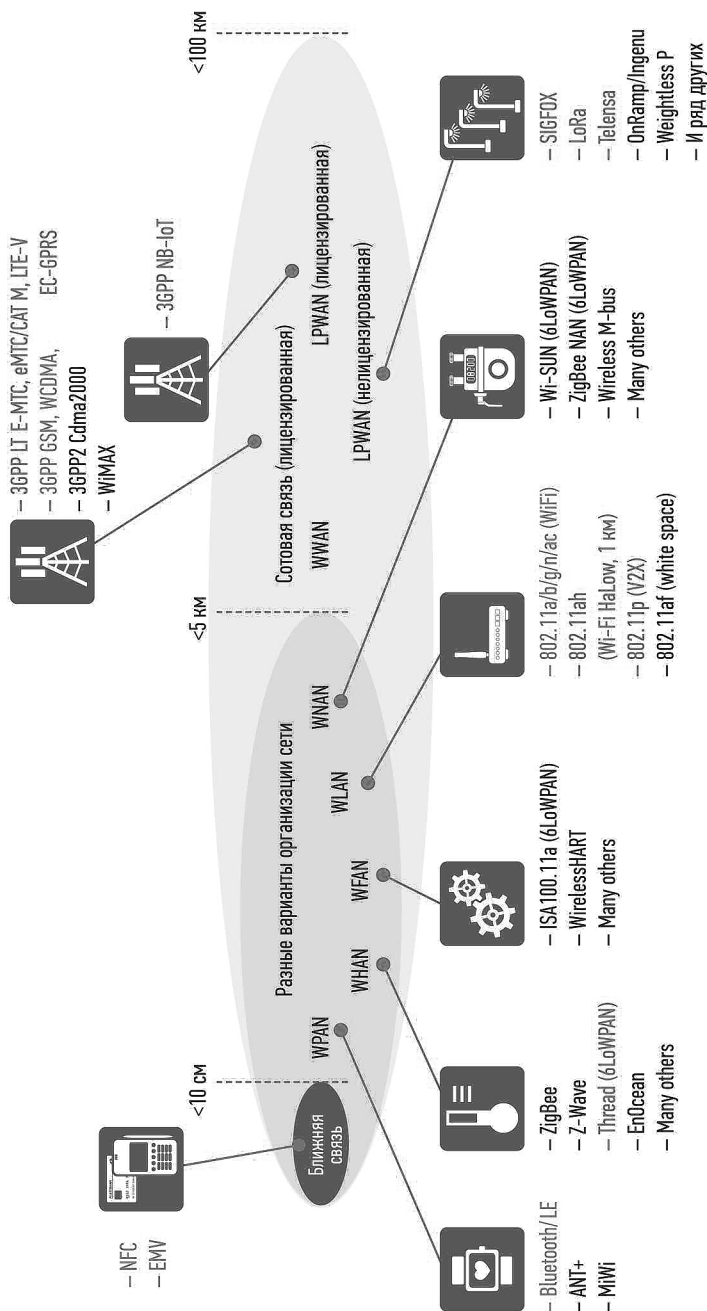


Рис. 1.1. Пример экосистемы Интернета вещей

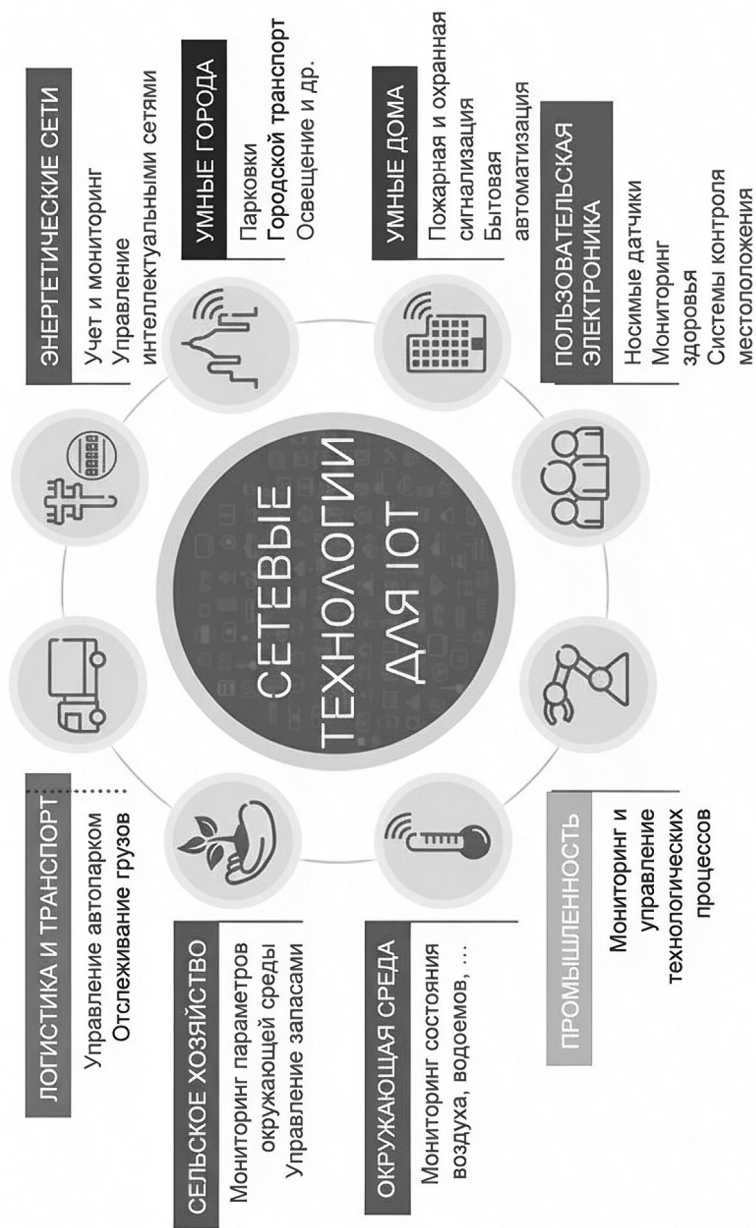


Рис. 1.2. Применение Интернета вещей в различных областях

которые работают в реальном времени, — это не выдумки фантастов — это возможности, которые предоставляют устройства ИВ для здравоохранения [40].

Применяя технологии Интернета вещей при строительстве и эксплуатации рабочих помещений, можно значительно снизить затраты. Использование умных датчиков освещенности помещений позволит сэкономить на электроэнергии, устройства будут включать свет только при присутствии в помещении человека и автоматически его выключать, когда помещение опустеет. Можно настроить процедуру включения кондиционера, если анализаторы наполненности зала обнаружат его заполнение, и обратную ей процедуру выключения, если зал опустел [38–40].

Интеллектуальные системы Интернета вещей широко применяются и в сельском хозяйстве. Различные датчики температуры, освещения, влажности воздуха, анализаторы почвы, а также и другие устройства «умных» систем способствуют лучшей урожайности и росту прибыли за счет автоматизации рутинных процессов и постоянного мониторинга внешней среды [41].

Технологии Интернета вещей применимы и в городской среде. Например, элементы «умного города» можно встретить и в г. Воронеж. В 2018 году на Московском проспекте была установлена система умных светофоров и датчиков, способная анализировать поток машин и изменять интенсивность движения. Система позволила уменьшить дорожный трафик движения, сэкономить электроэнергию. Различные умные датчики углекислого газа, применяющиеся в городах Китая, способны контролировать и решать экологические проблемы, а также улучшить санитарные условия для жителей [42]. На рис. 1.2 схематично представлены области применения Интернета вещей.

### 1.1.3. Архитектура Интернета вещей

В октябре 2014 года Всемирный форум Интернета вещей (IWF) осуществил важный шаг в развитии технологии, представив всеобъемлющую эталонную модель Интернета вещей [43]. Этот фундаментальный документ стал краеугольным камнем для стандартизации и оптимизации процессов внедрения технологий Интернета вещей в разнообразных отраслях экономики и социальной сферы. Разработанная на базе принципов модели взаимодействия открытых систем, представленная эталонная архитектура детально определяет функциональные уровни обра-