DOI: 10.25586/RNU.V9276.19.02.P.029 УДК 004.056; 004.738.5

Г.М. Микрюкова, С.Е. Вечерская

# ВОЗМОЖНОСТИ И ПРОБЛЕМЫ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИНТЕРНЕТА ВЕЩЕЙ

Посвящено возможностям и проблемам внедрения технологий Интернета вещей. Рассмотрены основные принципы Интернета вещей, его структура и тенденции развития. Проанализированы возможные угрозы и проблемы безопасности, связанные с Интернетом вещей, отмечена необходимость в разработке предложений по решению этих проблем и определен круг соответствующих задач.

*Ключевые слова:* Интернет вещей, IoT, тенденции, информационная безопасность, качество информации.

G.M. Mikryukova, S.E. Vecherskaya

# OPPORTUNITIES AND PROBLEMS OF THE IMPLEMENTATION OF THE TECHNOLOGY OF THE INTERNET OF THING

Dedicated to the opportunities and challenges of implementing IoT technologies. The basic principles of the Internet of Things, its structure and development trends are considered. The possible threats and security problems associated with the Internet of Things were analyzed, the need for developing proposals to solve these problems was noted, and a number of relevant tasks were identified.

*Keywords:* Internet of Things, IoT, trends, information security, quality of information.

Понятие «Интернет вещей» (Internet of Things, IoT) впервые появилось в Массачусетском технологическом институте: в 1999 г. там был создан Центр автоматической идентификации (Auto-ID Center), занимавшийся радиочастотной идентификацией (RFID) и новыми сенсорными технологиями. Центр координировал работу семи университетов, расположенных на четырех континентах.

Существуют множество определений IoT. Так, например, ведущие консалтинговые компании дают следующие определения:

- IDC – Internet of Things – это сеть сетей с уникально идентифицируемыми конечными точками, которые общаются между собой в двух направлениях по протоколам IP и обычно без человеческого вмешательства;
- Gartner – Internet of Things – это сеть физических объектов, которые имеют встроенные технологии, позволяющие осуществлять взаимодействие с внешней средой, передавать сведения о своем состоянии и принимать данные извне;
- McKinsey – Internet of Things – это датчики и приводы (исполнительные устройства), встроенные в физические объекты и связанные через проводные или беспроводные сети с использованием протокола Internet Protocol (IP), который связывает Интернет.

Существует также понятие «промышленный Интернет вещей» (Industrial Internet of Things) – многоуровневая система,

включающая в себя датчики и контроллеры, установленные на узлах и агрегатах промышленного объекта, средства передачи собираемых данных и их визуализации, мощные аналитические инструменты интерпретации получаемой информации и многие другие компоненты [2].

Считается, что первая «интернет-вещь» появилась в 1990 г. Это тостер, разработанный американцем Джоном Ромки – одним из создателей протокола TCP/IP. Подсоединив кухонного помощника к Всемирной паутине, инженер сумел включить и выключить его удаленно. Просто так, забавы ради, не подозревая, что его эксперимент станет спусковым механизмом, который вызовет «эффект лавины» и начнет формировать новую реальность.

Архитектура IoT, по данным на 2016 г., только формируется, однако к системообразующим относят четыре уровня: устройства, связь, обработка и управление данными. Свои эталонные модели предлагают США, Германия (рис. 1–2), ЕС и Китай.

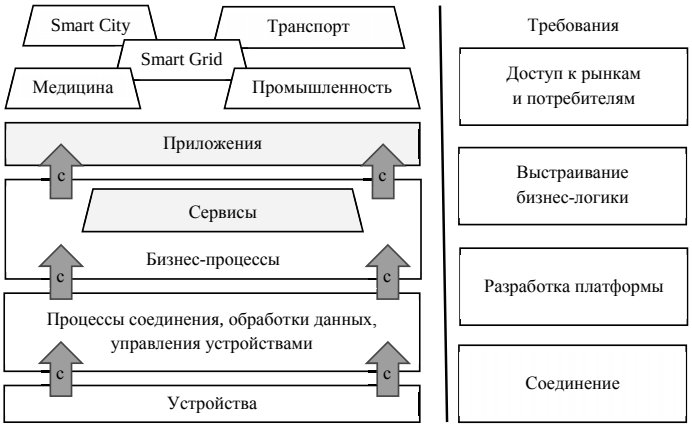


**Рис. 1.** Эталонные модели архитектуры IoT Германии и США

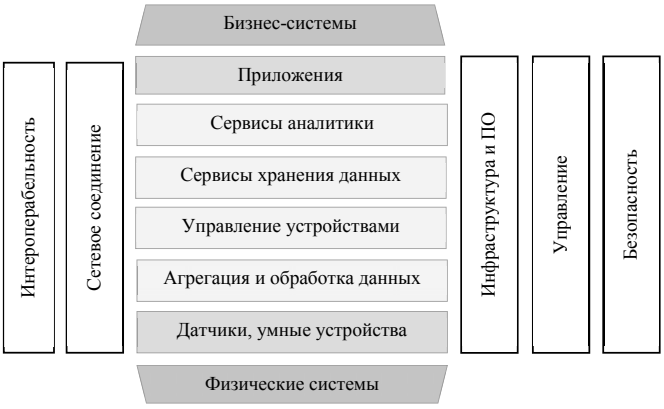


**Рис. 2.** Эталонная архитектура, предложенная Industrial Internet Consortium, включающим Cisco, GE, IBM, Intel и др. (США)

Некоторые эксперты в качестве модели приводят четырехуровневую классификацию структуры:

• Первый уровень. Проводится идентификация каждого объекта по отдельности.

• Второй уровень. Является сервисом, который обслуживает потребности человека (в качестве частного примера можно рассматривать систему «умный дом»).

• Третий уровень. Является сервисом, построенным по концепции «умного города». Предусматривает сбор и обработку всей информации, относящейся к жителям поселения, а также отдельных районов, кварталов и домов.

• Четвертый уровень. Сенсорная планета. Действует по примеру третьего уровня, но уже на территории всей планеты.

Интернет вещей как сеть сетей состоит из слабо связанных между собою разрозненных сетей, каждая из которых была развернута для решения своих специфических задач. К примеру, в современных автомобилях работают сразу несколько сетей: одна управляет работой двигателя, другая – системами безопасности, третья поддерживает связи и т.д.

Таким образом, развитие технологий Интернета вещей включает три этапа:

• межмашинное взаимодействие M2M. Годом начала первого этапа развития Интернета вещей является 1989 г.: IoT представлял собой автоматизированный сбор данных о состоянии системы для последующей обработки человеком;

• объединение устройств в единую экосистему IoT. Начиная с 2008 г. Интернет вещей эволюционирует в интеллектуальное взаимодействие устройств без вмешательства человека через IP-соединение;

• объединение всего в экосистему IoE. Когда наступит этот этап, прогнозировать рано, но можно с уверенностью сказать, что по мере развития Интернета вещей сети будут подключаться друг к другу и приобретать все более широкие возможности в сфере безопасности, аналитики и управления, эксперты прогнозируют переход к Всеобъемлющему Интернету – Internet of Everything, или IoE. Internet of Everything объединит различные процессы, объекты, большие данные и людей для интеллектуального взаимодействия и принятия обоснованных решений по регулировке системы.

Уже сейчас, спустя 15 лет после рождения IoT, Интернет вещей стал одним из главных трендов высоких технологий: едва ли можно найти IT-компанию, у которой не было бы разработок и проектов в этой сфере.

По данным мировых аналитиков [8], на начало 2016 г. в использовании технологий Интернета вещей компании ориентировались (и ориентируются до сих пор) в первую очередь на массовые сегменты IoT, где побуждением конечных пользователей к использованию решений и сервисов IoT являются рыночные стимулы (рис. 3).

Кроме того, ожидается, что данные станут «новой валютой» [1].

По данным IBM, каждый день создается 2,5 млрд гигабайт данных. И в исследовании, проведенном журналом Forbes Magazine, «70% ИТ-руководителей считают, что их организация использует ценность из больших данных, что крайне важно для их будущего успеха». Большие данные действительно массивны, потому что в информационную эпоху в них содержится секрет большего количества денег. Например, приложение Uber по прокату велосипедов оценивается в 42 млрд долл. не потому, что это реальная услуга такси, а потому, что оно стало искусно собирать информацию о своих клиентах, которая, скорее всего, станет более ценной, чем сами клиенты.

| | |
|---|---|
| Транспорт | • Грузоперевозки;<br>• спецтехника;<br>• такси;<br>• личный транспорт |
| ЖКХ | • Приборы учета;<br>• состояние инфраструктуры;<br>• погодные условия;<br>• экология |
| Медицина | • Носимые медицинские устройства;<br>• удаленная диагностика |
| Безопасность | • Контроль проникновения;<br>• противоугонные системы;<br>• контроль доступа;<br>• видеонаблюдение |
| Качество жизни | • Носимые устройства;<br>• бытовая техника и электроника;<br>• «умный дом/город» |
| Ритейл | • Вендинговые автоматы;<br>• логистика;<br>• адаптивная реклама;<br>• размер очереди;<br>• заказ товаров |
| Банки | • POS-терминалы;<br>• банкоматы;<br>• терминалы самообслуживания;<br>• верификация клиентов |
| Сельское хозяйство/ животноводство | • Датчики для животных;<br>• контроль полей;<br>• контроль доставки продукции |

**Рис. 3.** Области применения IoT

Доходы крупных компаний по анализу данных растут, и инвесторы вкладывают деньги в эту область.

Чем к большему количеству данных имеет доступ бизнес, тем выше вероятность его успеха. Большие данные являются основой автоматизации в таких отраслях, как наука о здоровье и космические технологии, и помогают управлять Интернетом вещей.

Если совместить данные из различных источников и с различных устройств, можно получить практически бесконечный высокоинформативный поток, который может быть использован в самых разных сферах: от медицины и научных исследований до логистики городского транспорта и добычи полезных ископаемых.

Парадигма «одно приложение – одно устройство» уступит место множественности данных с нескольких устройств и приложений одновременно (или даже с нескольких приложений на одном и том же устройстве). Одним из таких примеров является решение для «умного дома»: в его основе лежит некий смарт-центр или модуль, с помощью которого можно управлять целой группой устройств, электрическими приборами, лампочками, локальными беспроводными сетями или системами сигнализации и кондиционирования (отопления) в домах и квартирах.

С развитием технологий будет происходить постепенное их удешевление и массовый рост. Объединив системы «умных домов» или «умных машин» в одну инфраструктуру, можно получить сверхсистему, данные из которой могут использоваться для удовлетворения как частных, так и коллективных интересов.

Отдельно стоит упомянуть о машинном самообучении – предвестнике полноценно-

го искусственного интеллекта. В качестве примера приведем термостат Nest. Он способен накапливать данные и в дальнейшем подстраивать температурный режим, частоту включения-выключения электричества и работу домашних бытовых приборов под постоянно повторяющиеся циклы или действия. Можно предположить, что через несколько лет «умный термостат» станет вообще центром экосистемы частных домов или даже целых коттеджных поселков (особенно если научить такие устройства обмениваться данными между собой).

Второй интересный пример накопления данных и дальнейшего их использования в разных приложениях и сервисах – фитнес-платформы Apple Health Kit и Google Fit. Они собирают информацию с фитнес-трекеров, смарт-браслетов, «умных часов», обрабатывают и выдают общую картинку состояния здоровья, физических нагрузок и возможных проблем с давлением, сердцебиением, уровнем сахара в крови, перепадами температуры тела. Добавим интеграцию с онлайн-платформами для медиков и больниц и получим облачную сверхплатформу для управления качеством здоровья и жизни для сотен тысяч людей.

По различным прогнозам, к 2020 г. также ожидается кросс-вертикальная интеграция IoT-систем [6]. Если «замкнуть» весь круговорот информации на одной или нескольких закрытых платформах либо исключительно на одном-двух классах устройств, то множество источников данных не будет иметь никакой ценности, так как вся информация будет находиться в образованных закрытых платформах/классах устройств. К 2020 г. компаниям придется поработать над тем, чтобы их устройства поддерживали интеграцию с разными платформами: научить свои термостаты «общению» с «умной машиной», фитнес-трекеры – интеграции с сервисами покупок, а часы «приобщить» к электронной системе безопасности дома или офиса. Не будет отдельного сценария «для смарт-авто» или «для смарт-дома» – концепция Smart Life (концепция «умной жизни») вступит в свои права, уверены эксперты компании Vision Mobile. Крупные игроки рынка, такие как Google, Apple и Samsung, уже серьезно работают в этом направлении.

В отдаленной перспективе стоит ожидать появления единого целого, состоящего из традиционных технологий для работы с данными и из промышленных систем управления (ICS) и систем диспетчерского управления и сбора данных (SCADA) [9].

Несмотря на широкое применение Интернета вещей и перспективы развития этой технологии, стоит отметить, что существует ряд проблем, связанных с применением IoT.

К слабым местам IoT относятся:

- стандартизация архитектуры и протоколов, сертификация устройств;
- отсутствие единого стандарта в области взаимодействия интернет-вещей между собой;
- информационная безопасность;
- стандартные учетные записи от производителя, слабая аутентификация;
- отсутствие поддержки со стороны производителей для устранения уязвимостей;
- трудность или невозможность обновить ПО и ОС;
- использование текстовых протоколов и ненужных открытых портов;
- легкость попадания во всю сеть через один гаджет;
- использование незащищенных мобильных технологий;
- использование незащищенной облачной инфраструктуры;
- использование небезопасного ПО [4; 5].

Рассмотрим один из наиболее важных аспектов использования Интернета вещей – информационную безопасность. Проблемы безопасности информации можно условно разделить на три уровня:

1. *Уровень восприятия.* IoT не может обеспечить унифицированную систему защиты безопасности и является уязвимым к угрозам злоумышленника: физическому захвату сенсорных узлов, захвату узла шлюза, утечке информации сенсора, угрозе целостности данных, истощению энергообеспечения, угрозе перегрузки, атаке типа DoS (отказу в обслуживании), угрозе маршрутизации установлением в сеть нелегитимных сенсоров и угрозе копирования узла.

2. *Сетевой уровень.* На этом уровне к угрозам безопасности относятся: несанкционированный доступ, перехват данных, угроза конфиденциальности и целостности, атаки типа «человек посередине», DoS-атаки (отказ в обслуживании), вирусы, эксплойты, сетевые черви, руткиты и др. Кроме того, существуют межсетевые проблемы аутентификации, которые могут быть причиной атак DoS. Внимание уделяется и уязвимостям программного обеспечения (Software Vulnerabilities), приводящим к нарушению информационной безопасности после внедрения.

3. *Прикладной уровень.* К нему относятся угрозы повтора, подслушивания, искажения информации, раскрытия информации и другое при использовании облачных вычислений, обработке информации, обеспечении прав на интеллектуальную собственность, защите приватности и др. [7].

В ходе проведенного Hewlett-Packard (далее – HP) исследования обнаружено, что примерно в 70% проанализированных устройств не шифруется беспроводной трафик. Веб-интрефейс 60% устройств эксперты HP посчитали небезопасным из-за уязвимой организации доступа и высоких рисков межсайтового скриптинга. В большинстве устройств предусмотрены пароли недостаточной стойкости. Примерно 90% устройств собирают ту или иную персональную информацию о владельце без его ведома.

Всего же специалисты HP насчитали около 25 различных уязвимостей в каждом из исследованных устройств (телевизоров, дверных замков, бытовых весов, домашних охранных систем, электророзеток) и их мобильных и облачных компонентах.

Вывод экспертов HP неутешителен: безопасной экосистемы IoT на сегодняшний день не существует. Особую угрозу вещи Интернета таят в себе в контексте распространения целевых атак. Конечные пользователи становятся уязвимыми для злоумышленников, поскольку Интернет вещей открывает доступ в мир владельцев этих вещей.

По мнению Алексея Коняева (ведущего консультанта по противодействию мошенничеству, SAS России/СНГ), понятия «безопасность Интернета вещей» вообще не существует. С точки зрения безопасности большинство устройств («умные телевизоры», игровые приставки, принтеры, т.е. давно уже привычные нам «сетевые» инструменты) сейчас практически никак не защищено. Хотя они и не предоставляют особого интереса для киберпреступников в сравнении, например, с банковскими мобильными приложениями, с которых можно украсть реальные деньги, однако существует риск использования данных устройств как части большой бот-сети для осуществления в дальнейшем DoS-атак. Отслеживать и анализировать подобные атаки крайне сложно даже для обычных компьютеров, что уж говорить про такие девайсы [3].

Развитие IoT предполагает, что работающие автономно сетевые устройства будут

исчисляться не сотнями тысяч, как сейчас, а десятками миллиардов, поэтому, если к этому времени не будут разработаны стандарты по обеспечению их безопасности, мы столкнемся с глобальной проблемой.

Одной из проблем, которые могут возникнуть при внедрении технологии Интернета вещей, является работа пользователя в самом начале эксплуатации. Пользователю обязательно нужно заменить фабричный пароль, установленный по умолчанию, на свой личный, так как фабричные пароли одинаковы на всех устройствах и не отличаются стойкостью. Делают это далеко не все. Поскольку не все приборы имеют встроенные средства информационной безопасности, владельцам также следует позаботиться об установке внешней защиты, предназначенной для домашнего использования, чтобы интернет-устройства не стали открытыми шлюзами в домашнюю сеть или прямыми инструментами причинения ущерба.

Еще одним примером опасности являются «умные дома будущего».

Panda (испанская компания, специализирующаяся на разработке решений в области IT-безопасности) собрала несколько идей о способах, благодаря которым хакеры могли бы получить беспрецедентный доступ к повседневной жизни человека через комплексные устройства, расположенные у него дома.

Первая идея – «выкуп за вход домой». Хотя «умный дом» и превратит помещение в оптимизированное жизненное пространство, полностью предназначенное для обеспечения комфорта, тем не менее он может также нести серьезные риски стать жертвой кибератаки в собственном доме.

Центральное звено любой системы безопасности «умного дома будущего» – это его замок. Недавнее исследование показало, что «умные замки» легко можно взломать, в результате чего они не гарантируют выполнения своей основной функции, для которой, собственно говоря, они и созданы.

Существующие системы достаточно просты для хакеров и не являются препятствием для того, чтобы проникнуть в дом. Если «умный замок» можно взломать, возможно, хакеры найдут способ, как полностью его закрыть, чтобы хозяин дома не смог войти. В этом случае в будущем можно будет достаточно легко проникать в чужой дом: хакер сможет контролировать все события удаленно. Более того, он сможет запрашивать у своих жертв какой-нибудь разумный выкуп за то, чтобы они могли попасть в свои собственные дома.

Если все устройства безопасности взаимосвязаны, то киберпреступники потенциально могли бы получить доступ к домашней сигнализации и даже ключам от автомобиля.

Одна функция безопасности, которая уже встроена в некоторые доступные на рынке детекторы дыма, – это возможность, позволяющая «умному дому» получать информацию (и использовать ее в дальнейшей работе) от других смарт-устройств, что позволяет системе реагировать соответствующим образом в случае опасности. Данная функция внедрена для безопасности пользователя, позволяя домашней системе, которая обнаружила пожар, например, разблокировать все двери в доме, чтобы помочь выбраться из него как можно быстрее.

Это отличный пример того, как производители IoT-решений работают над прозрачной интеграцией и взаимодействием смарт-устройств внутри «умного дома». Однако есть одна оговорка: если эта технология будет использоваться киберпреступниками, то существует вероятность создания нежелательной цепной реакции, которая в конечном итоге может, наобо-

рот, снизить уровень безопасности «умного дома».

Еще один способ причинения вреда собственнику – это создание хакером ложной тревоги о пожаре, которая отправляется в пожарные службы в виде картинки с задымленным помещением. В итоге это делает пользователя легкой добычей для других потенциально вредоносных кибератак.

Источником опасности может быть смарт-холодильник. Еще два года назад ЦРУ отметили угрозу со стороны смарт-холодильников в «умных домах». ЦРУ всполошилось оттого, что холодильник использовался как часть бот-сети для выполнения DDoS-атаки. И все это происходило совершенно незаметно для хозяина этого холодильника, который даже и понятия не имел о том, что его смарт-устройство может выполнять какие-то другие действия, кроме охлаждения и сохранения еды.

Злоумышленники, как правило, работают на массы: например, распределенные атаки на отказ в обслуживании (DDoS), когда тысячи электронных писем или запросов отправляются на какой-то сервер, чтобы замедлить его работу или вообще вывести из строя.

В этом случае в будущем мы можем столкнуться с ситуациями, когда хакеры попытаются «завалить» как можно больше машин в надежде на то, что какая-то их часть будет работать неправильно, что приведет к тяжелым последствиям. Возможно, по этой причине правительственные органы говорят о потенциальных опасностях Интернета вещей, связанных с кибератаками.

В IoT в промышленности проблем будет еще больше, потому что объемы данных, генерируемые промышленными машинами, больше, чем у бытовых, а вопросы безопасности – критичнее. Обеспечить адресацию ко всем возможным устройствам по протоколу IPv6 (Internet Protocol version 6) недостаточно для решения проблем IT/OT convergence. Поэтому, если подумать, за разрекламированной ширмой под названием IoT скрывается сервисная платформа PaaS с доступом к облачным ресурсам [8].

Можно сделать вывод, что стремительное развитие концепции Интернета вещей вызвано широким распространением беспроводных технологий и межмашинного обмена, развитием технологии облачных вычислений и началом перехода на IPv6. Однако использование IoT во многих областях ограничено сложными проблемами в части обеспечения информационной безопасности и качества информации.

Существует необходимость в разработке предложений по решению проблем безопасности в IoT, а также решении следующих задач:

1. Оценка уязвимости подключаемых устройств на этапе производственного процесса. К сожалению, в настоящее время, в связи с лавинообразным спросом на подобные устройства, многие производители не уделяют достаточного внимания данной проблеме.

2. Разработка ПО, отвечающего требованиям безопасности, с использованием стандартов разработки безопасных приложений. Кроме этого, необходимо предусмотреть возможность обновления данного ПО.

3. Управление логистикой устройств на всех этапах: от производства до инсталляции на объекте. Данный подход позволит значительно снизить уязвимость в аппаратно-зависимом коде.

## Литература

1. Данные – новая валюта бизнеса: ток-шоу // Про Бизнес. URL: https://probusinesstv.ru/programs/111/12455/ (дата обращения: 11.02.2019).

2. Интернет вещей // Портал выбора технологий и поставщиков. URL: http://www.tadviser.ru/index.php/Интернет_вещей_Internet_of_Things_(IoT) (дата обращения: 11.02.2019).
3. Информационная безопасность в Интернете вещей // Интернет-журнал. URL: https://iot.ru/bezopasnost/informatsionnaya-bezopasnost-v-internete-veshchey (дата обращения: 11.02.2019).
4. Информационная безопасность Интернета вещей (Internet of Things) // Портал выбора технологий и поставщиков. URL: http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_интернета_вещей_(Internet_of_Things) (дата обращения: 22.02.2019).
5. *Лукацкий А.* Информационная безопасность Интернета вещей // Блог Cisco в России и СНГ. URL: https://gblogs.cisco.com/ru/iotsecurity/ (дата обращения: 11.02.2019).
6. Перспективы развития «интернет-вещей» до 2020 года // Портал о современных технологиях мобильной и беспроводной связи. URL: http://1234g.ru/novosti/internet-veshchej-k-2020-godu (дата обращения: 11.02.2019).
7. *Соколов М.Н., Смолянинова К.А., Якушева Н.А.* Проблемы безопасности интернет-вещей: обзор // Вопросы кибербезопасности. 2015. № 5. С. 32–35.
8. Что такое Интернет вещей? // Портал выбора технологий и поставщиков. URL: http://www.tadviser.ru/index.php/Статья:Что_такое_интернет_вещей_%28Internet_of_Things%2C_IoT%29 (дата обращения: 11.02.2019).
9. *Шиков С.А.* Проблемы информационной безопасности: Интернет вещей // Вестник Мордовского университета. 2017. Т. 27, № 1. С. 27–40. DOI: 10.15507/0236-2910.027.201701.027-040.

## Literatura

1. Dannye – novaya valyuta biznesa: tok-shou // Pro Biznes. URL: https://probusinesstv.ru/programs/111/12455/ (data obrashcheniya: 11.02.2019).
2. Internet veshchej // Portal vybora tekhnologij i postavshchikov. URL: http://www.tadviser.ru/index.php/Internet_veshchej_Internet_of_Things_(IoT) (data obrashcheniya: 11.02.2019).
3. Informatsionnaya bezopasnost' v Internete veshchej // Internet-zhurnal. URL: https://iot.ru/bezopasnost/informatsionnaya-bezopasnost-v-internete-veshchey (data obrashcheniya: 11.02.2019).
4. Informatsionnaya bezopasnost' Interneta veshchej (Internet of Things) // Portal vybora tekhnologij i postavshchikov. URL: http://www.tadviser.ru/index.php/Stat'ya:Informatsionnaya_bezopasnost'_interneta_veshchej_(Internet_of_Things) (data obrashcheniya: 22.02.2019).
5. *Lukatskij A.* Informatsionnaya bezopasnost' Interneta veshchej // Blog Cisco v Rossii i SNG. URL: https://gblogs.cisco.com/ru/iotsecurity/ (data obrashcheniya: 11.02.2019).
6. Perspektivy razvitiya "internet-veshchej" do 2020 goda // Portal o sovremennykh tekhnologiyakh mobil'noj i besprovodnoj svyazi. URL: http://1234g.ru/novosti/internet-veshchej-k-2020-godu (data obrashcheniya: 11.02.2019).
7. *Sokolov M.N., Smolyaninova K.A., Yakusheva N.A.* Problemy bezopasnosti internet-veshchej: obzor // Voprosy kiberbezopasnosti. 2015. № 5. S. 32–35.
8. Chto takoe Internet veshchej? // Portal vybora tekhnologij i postavshchikov. URL: http://www.tadviser.ru/index.php/Stat'ya:CHto_takoe_internet_veshchej_%28Internet_of_Things%2C_IoT%29 (data obrashcheniya: 11.02.2019).
9. *Shikov S.A.* Problemy informatsionnoj bezopasnosti: Internet veshchej // Vestnik Mordovskogo universiteta. 2017. T. 27, № 1. S. 27–40. DOI: 10.15507/0236-2910.027.201701.027-040.