Обзорная статья
УДК 004.75
DOI: 10.17072/1993-0550-2023-1-70-76

IoT. К вопросу об Интернете вещей

Марина Александровна Зосимова[1], Сергей Александрович Смирнов[2]
[1, 2] Московский технический университет связи и информатики (Волго-Вятский филиал), Нижний Новгород, Россия
[1] ma.zosimova@vvfmtuci.ru
[2] ser-smir@yandex.ru, https://orcid.org/0000-0002-1289-6663

Аннотация. Современная динамичная жизнь вносит изменения как в жизнь отдельных домохозяйств, так и производственных субъектов. Стремящиеся к комфорту и безопасности домохозяйства готовы приобретать и использовать гаджеты, запускающие процессы обеспечения климат-контроля, датчиков движения и передачи данных счетчиков потребления. К использованию интернета вещей стремятся и промышленные предприятия, ищущие драйверы роста за счет оптимизации расходов на наблюдение за процессами производства. Гарантом оперативного реагирования физических лиц и производственных и торговых предприятий на вызовы конкуренции является использование передовых инструментов мониторинга и управления процессами. Это связано с использованием технологий и инструментов интернета вещей.

Ключевые слова: *управление процессами; автоматизация; интернет вещей; домохозяйства; производство; логистика; гаджеты*

Для цитирования: *Зосимова М. А., Смирнов С. А.* IoT. К вопросу об Интернете вещей // Вестник Пермского университета. Математика. Механика. Информатика. 2023. Вып. 1(60). С. 70–76. DOI: 10.17072/1993-0550-2023-1-70-76.

Статья поступила в редакцию 27.10.2022; одобрена после рецензирования 25.11.2022; принята к публикации 16.03.2023.

Review article

IoT. To the Question of the Internet of Things

Marina A. Zosimova[1], Sergey A. Smirnov[2]
[1,2]Moscow Technical University of Communications and Informatics (Volga-Vyatka branch), Nizhny Novgorod, Russia
[1] ma.zosimova@vvfmtuci.ru
[2] ser-smir@yandex.ru, https://orcid.org/0000-0002-1289-6663

Abstract. Modern dynamic life makes changes both in the lives of individual households and industrial entities. Households striving for comfort and safety are ready to purchase and use gadgets that trigger the processes of providing climate control, motion sensors and data transmission of consumption meters. Industrial enterprises are also seeking to use the Internet of Things, looking for growth drivers by optimizing the costs of monitoring production processes. The use of advanced monitoring and process management tools is the guarantor of the rapid response of individuals and industrial and commercial enterprises to the challenges of competition. This is due to the use of technologies and tools of the Internet of Things.

Keywords: *process management; automation; Internet of things; households; manufacturing; logistics; gadgets*

For citation: *Zosimova M. A., Smirnov S. A.* IoT. To the Question of the Internet of Things. Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2023;1(60):70-76. (In Russ.). DOI: 10.17072/1993-0550-2023-1-70-76.

The article was submitted 27.10.2022; approved after reviewing 25.11.2022; accepted for publication 16.03.2023.

Интернет вещей (далее – IoT) — это сложная концепция, представляющая собой экосистему сетевых устройств. Они представляют собой знакомые технологии, которые взаимодействуют друг с другом посредствам сети интернет [1].

Необходимо отметить что, когда люди упоминают IoT, то имеют в виду розетки, кофеварки, замки и другие полезные вещи, но не в очень больших масштабах. Характерно, что чайники, которые автоматически кипятят воду, как только человек просыпается, это часть IoT.

Технология IoT используется в огромном количестве областей. В частности, от нее в значительной степени зависит современная промышленная и сельскохозяйственная инфраструктура. Технология IoT также выглядит перспективным направлением для развития систем "умного города" и других подобных систем.

IoT автоматизирует многие процессы. Например, процесс наблюдения за полевыми работами, за состоянием техники компании или за опустошением садовых мусорных баков. Анализируя получаемую информацию умные устройства выполняют определенные действия. Например, при выходе из строя какого-либо оборудования может автоматически вызываться ремонтная служба [2].

Характерно, что IoT работает в зависимости от приложения и используемого устройства. Говоря упрощенно, мы полагаем, что работу Интернета вещей можно рассмотреть на примере функционирования умного дома – в нем, как правило, всегда используется концентратор (умная колонка, термостат или планшет), подключены совместимые устройства в духе смарт-гаджетов, такие как чайники, кондиционеры, телевизоры, холодильники и т.п. Владельцы умного дома могут отправлять команды в систему или настраивать автоматику для выполнения функций без постороннего вмешательства.

Стоит отметить, что в более сложных проектах работа организована аналогично, только в большем масштабе. Чтобы система функционировала исправно и надежно, используются более сложные алгоритмы и фирменное программное обеспечение. К сожалению, в настоящее время до полноценных умных городов еще далеко, но эффективность этой технологии в компаниях и бизнесе уже впечатляет.

Исходя из сегмента потребления в основном используется IoT двух типов: первый для физических лиц и второй для бизнеса. Самый простой пример IoT-технологий – умный дом. Мы уже анализировали этот пример и от него трудно отказаться, так как это, вероятно, самый популярный вариант на уровне личного использования. Домашняя экосистема интеллектуальных IoT-устройств включает в себя множество чрезвычайно полезных гаджетов – кофеварки и пылесосы, розетки и лампочки. Так, умный холодильник с чайником являются интересным дополнением к нашей жизнедеятельности.

Однако не меньший интерес вызывает датчик воды с автоматическим клапаном, перекрывающим воду в случае прорыва, пока нас нет дома, дверной замок с видеонаблюдением, который позволяет вам мгновенно видеть, кто находится у двери.

Технологии IoT облегчают жизнь домовладельцам и самим жильцам. Этому способствует интеллектуальный счетчик, который автоматически производит измерения и передает данные коммунальной компании. Домофон нового поколения позволяет видеть, кто звонит в вашу квартиру, не отвечая на телефонные звонки с помощью встроенной камеры и мобильного приложения.

Стоит отметить, что во многих современных районах технология IoT уже внедрена на этапе строительства. Например, умная лампочка, которая выключается и отображает уровень счета за электроэнергию через смартфон.

Говоря о технологиях IoT, применяемых для физических лиц, особое внимание следует уделить сфере здравоохранения. Умные часы, тонометры, медицинские браслеты тоже относятся к этой технологии и способны следить за здоровьем человека и повысить качество жизни.

С помощью данных инструментов осуществляется постоянный контроль за здоровьем человека. Они следят за пульсом, отслеживают качество сна и даже сообщают о десатурации крови. Созданы такие системы, которые могут отслеживать ЭКГ и давление в режиме реального времени и отправлять их через Интернет лечащему врачу. Характерно, что различные страны увеличивают финансирование на такие устройства и внедряют их на уровне больниц. Есть предпосылки к тому, что вскоре это повлияет и на повседневную жизнь людей.

Таким образом, комплекс IoT для физических лиц и домохозяйств представляет собой широкий спектр гаджетов, обеспечивающих комфорт жизни, безопасность жилища, здоровьесбережение семьи.

Однако не только физические лица и домохозяйства активно используют преимущества IoT, но и промышленность задействует IoT-инструменты в производственных целях. IoT используют на заводах и складах, при транспортировке и продажах. Сложная система передовых датчиков позволяет профессионалам тратить меньше времени на наблюдение и сбор информации и больше времени на непосредственную работу и принятие решений в динамично меняющихся условиях.

Отдельно следует подчеркнуть, что промышленный IoT отличается от потребительского по масштабу применения. Если умный дом IoT влияет на жизнь одного человека или его семьи, то в промышленном формате влияние IoT распространяется на сотни, а то и тысячи людей. Масштабы и качество обрабатываемой информации в рамках промышленного IoT также находит свое отражение на соблюдении информационной и промышленной безопасности [3].

Говоря о логистике промышленных и коммерческих предприятий стоит отметить, что качественный анализ информации об объемах и структуре перевозок, маршруте, логистических центрах понижает степень непредсказуемости при заказе и доставке товара конечному потребителю. Технология IoT логистики может автоматически направлять погрузочную машину в нужное место в соответствии с заказом. С их помощью водители-доставщики, а также клиенты могут отслеживать местонахождение посылок, а в некоторых случаях есть возможность установить точное местонахождение транспортного средства. Это важно как для физических лиц, заказывающих товары для личного пользования в интернете, так и для бизнеса – в части закупки запчастей и комплектующих и продажи готовой продукции.

Анализируя возможности IoT-технологий в сфере логистики, следует обратить внимание – инструмент применим как в сфере промышленных и коммерческих перевозок, общественного транспорта, так и личного транспорта. Существует автобус с датчиком GPS, что позволило нам создать сервис в духе Яндекс Транспорта. Это комфортно, и такие технологии упрощают жизнь. Многие владельцы транспортных средств имеют подключении к сети Интернет и используют смартфоны для диагностики, подключения к службам мультимедиа и сообщениях о сбоях. Отметим, что на данный момент времени пока еще не все автомобили достаточно умны, чтобы мы отказались от водителей, но использование умных технологий помогает обеспечить безопасность дорожного движения, предупредить возникновение нештатных ситуаций и повысить точность логистических операций.

Также IoT непосредственно участвует даже в сельскохозяйственной деятельности. Так, с помощью датчиков, контролирующих состояние почвы, предпринимаются меры по достижению оптимального состояния грунта, сокращению издержек и повышению урожайности. Они представляют собой способ без вмешательства человека определить, достаточно ли влажна земля и содержит ли она достаточное количество веществ, необходимых растениям для нормального роста. IoT и связанные с искусственным интеллектом технологии (далее – ИИ) позволяют нам оценивать состояние фермы без сложного анализа. ИИ может взять на себя функцию по сбору и анализу данных и предоставит всю необходимую информацию для принятия решения. Это позволяет даже небольшим странам организовать работу в сельском хозяйстве и обеспечить население сельскохозяйственной продукцией.

Добавление технологии IoT в городскую среду значительно упрощает жизнь в городских условиях, особенно в мегаполисах. Многие устройства уже используются и обеспечивают комфорт и безопасность городских жителей. К таким инструментам относятся:

– транспорт с датчиками GPS, чтобы помочь горожанам планировать маршрут и время нахождения в пути;

– "безопасный город" – система видеонаблюдения, в частности, используемая в своей деятельности правоохранительными органами;

– специальный датчик определяет, когда мусорный контейнер заполнен, и автоматически вызывает службу уборки.

Мы полагаем, что развитие системы умных городов невозможно переоценить. Такие системы делают жизнь безопаснее и удобнее.

IoT, как мы уже отмечали, включает в себя камеры видеонаблюдения со встроенным распознаванием лиц. Это всего лишь одна часть умного города, которая способна помочь правоохранительным органам быстро найти преступников и пропавших без вести. Мы полагаем, что IoT будет и дальше развиваться; так, по прогнозам экспертов, к 2025 г. количество устройств и других гаджетов, подключенных к сети Интернет, вырастет до двадцати пяти миллиардов штук. В частности, это произойдет вследствие развития сетей 5G. Это связано с тем, что данные передаются быстрее и надежнее по сети 5-го поколения, что позволяет активно использовать IoT без сбоев или снижения.

Необходимо отметить, что, конечно, будущее развитие умных городов пока туманно, так как это направление не считается приоритетным. Ключевые области роста IoT включают медицинскую, энергетическую и автомобильную промышленность. Правительства тратят огромные денежные средства на разработку экосистемы устройств для наблюдения за пациентами, создание умных автомобилей и использование ИИ и IoT для оптимизации производства энергии.

Также нельзя не сказать, что у IoT есть свои плюсы и минусы.

Преимущества заключается в:

– постоянном мониторинге различных показателей. Сейчас нет необходимости тратить свой опыт или время. ИИ сам определяет необходимые данные и уведомляет о каких-либо критических изменениях;

– предоставлении новых возможностей для людей и сообщества в целом. IoT значительно улучшает жизнедеятельность человека, путем добавления вещей, раньше считавшимися непрактичными. Еще совсем недавно автоматический заказ еды и домофоны с камерами казались достаточно дорогостоящими и сложно выполнимыми технологическими решениями;

– автономности системы. В большом количестве областей деятельности не требуется каких-то действий со стороны человека так как они происходят автономно, что положительно влияет на быстроту, эффективность и надежность их исполнения. Таким образом, на наш взгляд, каждый сектор может выиграть от автоматизации процессов.

Минусы IoT заключаются в:

– отсутствии общепринятых стандартов. Чтобы создать экосистему умных домашних устройств, – по нашему мнению, необходимо отдавать приоритет устройствам определенных брендов. Это связано с проблемами совместимости различных производителей умных устройств;

– необходимости промышленным компаниям создавать собственные аналоги датчиков, чтобы заставить их работать корректно в соответствии с их бизнес-требованиями;

– уязвимости (как и другие устройства, компоненты IoT подвержены взлому и другим типам уязвимостей). К примеру, взлом смарт-замка приведет к несанкционируемому доступу в жилище.

К сожалению, угрозы безопасности от технологии IoT неизбежны. Сами разработчики таких систем создали условия, препятствующие нормальному развитию безопасного IoT.

На наш взгляд, это заключается в том, что вместо создания общей системы разработчики начали создавать множество уникальных условий, результатом чего стало бесконечное количество сбоев, ошибок, уязвимостей и т.д., порой достаточно серьезных. Так, эксперт по безопасности сообщил о сотнях уязвимостей в своих обычных устройствах IoT, заявив, что злоумышленники могут использовать их в любое время, чтобы получить контроль над чьим-то домом или всем бизнесом. Таким образом создается угроза не только персональным данным, но и жизням людей.

Согласно исследованию, более 70 % устройств IoT не используют криптографические средства при работе с данными. Это означает, что вся активность происходит в открытых каналах, и в действительности информация может быть перехвачена любым пользователем, который может обнаружить уязвимости в определенных его системах IoT.

Учитывая, что эти устройства собирают данные о пользователе, отсутствие криптографической защиты и стандартов влечет за

собой угрозу не только для личной информации, но и для самого устройства.

Так, после несанкционированной разблокировки умного замка можно легко войти в квартиру. Взлом умного автомобиля может в любой момент отключить автопилот или вообще автомобиль. Существует множество футуристических сценариев, угроз, причем некоторые из которых уже реальны. Причиной этого является слишком громоздкий и запутанный переход на новые технологии.

Так, к примеру: однажды группа хакеров взломала термометр, установленный в аквариуме, и получила доступ к серверу казино. Оказалось, что сотрудник игорного зала с помощью умного термометра следил за состоянием рыбы в воде. Или радионяня Smart Her помогает родителям "наблюдать" за своими детьми, но также дает такую же возможность преступникам, взламывающим устройства IoT. И даже секс-игрушки не являются исключением; неоднократно были объектами взлома камеры умного дома. Известно о случае их взлома и использования для получения личной информации большого количества людей. Примечательно, что, получив к ним доступ, они устраивали целые онлайн-шоу, прямая трансляция которых была доступна по всему Интернету. Причем это затронуло пользователей по всей планете, в том числе и россиян. В 2016 г. в Финляндии хакер запустил DDoS-атаку на термостат, почти заморозив дома, путем отключения системы отопления. И даже управление по санитарному надзору за качеством пищевых продуктов и медикаментов США сообщило о нескольких взломах медицинских устройств.

Одним из самых резонансных случаев стало обнаружение уязвимостей в системах мониторинга пациентов. Таким образом, злоумышленник мог получить к ним доступ и отправить ошибочные данные. Например, отрегулировать пульс у пациента.

И, наконец, еще один интересный факт – в 2015 г. группа исследователей смогла взломать компьютерную систему автомобиля (внедорожник Jeep) и удаленно контролировать его скорость и траекторию.

Необходимо отметить, что по мнению экспертов по безопасности, много IoT-устройств плохо защищены от атак или вообще не защищены. Мы предлагаем регулировать безопасность инфраструктуры, где больше всего угроз представляет Интернет вещей, а не умные устройства. Стандартизация протоколов в области IoT также важна.

Согласно статистике "Лаборатории Касперского", в первой половине 2022 г. количество атак на его IoT-устройства в России увеличилось на 40 %. Так, если в январе было порядка 9 млн атак с 12 тысяч IP-адресов были зафиксированы в компьютерных приманках (ловушках для злоумышленников, имитирующих уязвимые устройства или сервисы), то в июне было зафиксировано около 13 млн атак с 29 тысяч IP-адресов, зарегистрированных в Китае, США, Южной Корее, Индии и Тайване. Злоумышленники создают ботнеты из взломанных устройств и используют их для DDoS-атак.

В то же время вредоносное ПО IoT постоянно обновляется, уделяя особое внимание уязвимостям новых устройств. Екатерина Рудина, руководитель группы аналитиков по информационной безопасности в "Лаборатории Касперского", в комментарии RSpectr сообщила, что в этом году значительно увеличилось количество так называемых хактивистов без серьезного уровня подготовки. Их атаки направлены на наиболее уязвимые и незащищенные конфигурации, имеющие стандартные пароли по умолчанию. Эксперты особенно осознают, что риску подвержены как медицинские, так и промышленные устройства, подключенные к сетям. Часто именно эти IoT-устройства становятся уязвимостью компании. SearchInform не собирает статистику киберинцидентов в своем IoT-пространстве, но сегодняшние эксперты документируют крупнейшие кибератаки в истории. В большинстве случаев у производителей отсутствуют принципы безопасной разработки именно поэтому IoT-устройства становятся жертвами хакеров. В большинстве случаев пользователи IoT-устройств сами не обращают внимания на безопасность.

Тем временем в Европе парламентарии планируют ввести умные правила кибербезопасности своих гаджетов. Европейская комиссия представила проект закона о киберустойчивости. В нем, в частности, говорится о том, что производители гаджетов, которые продаются в ЕС, должны проектировать свои устройства в соответствии с требованиями по кибербезопасности и обеспечивать постоянную поддержку и своевременное предоставление обновлений для IoT-устройств. Кроме того, производители должны предоставлять "достаточно информации", для оценки потребителями возможных рисков и правильной

настройки приобретенного устройства. Если компания совершит серьезное правонарушение, она может быть оштрафована на сумму до 15 млн евро или на 2,5 % от выручки.

Согласно исследованию регуляторов ЕС, только половина соответствующих компаний имеют для защиты от кибератак. А также, согласно пресс-релизу Европейской комиссии, две трети атак связаны с ранее обнаруженными уязвимостями, которые производители не могут исправить.

Отметим, что введение ответственности производителя за сохранность его смарт-устройств обсуждается во многих странах мира. Калифорния (США) хотела принять закон, обязывающий производителей устройств IoT поддерживать обновления и устранять уязвимости. Великобритания опубликовала список рекомендаций о том, как производители могут защитить свою продукцию, и это правильно, потому что закон побуждает производителей предлагать устройства, которые не работают в небезопасных режимах, таких как заводские пароли.

В январе 2022 г. Xiaomi (китайская технологическая компания) опубликовала руководство по стандартам кибербезопасности для устройств IoT. Оно предлагает стандарты для интеллектуальных устройств, их операционных систем, связи между устройствами, и набор требований к конфиденциальности и защите [4]. Xiaomi предлагает свой документ как "единый глобальный стандарт в области Интернета вещей", который могут принять другие компании [5]. Внедрение таких стандартов в РФ в настоящее время нереально, так как полностью отечественных IoT-устройств нет, а с уходом иностранных вендоров и внедрением механизмов параллельного импорта ужесточение требований к IoT-устройствам – не лучший вариант действий. Рынок IoT сильно зависит от продуктов микроэлектроники, и локализация производства в России остается очень сложной проблемой: большая часть производственных мощностей в сфере микроэлектроники находится далеко за пределами Российской Федерации.

В остальном проектирование и разработка ПО в России не представляют большой проблемы и является очень конкурентоспособным. По мнению экспертов, основой развития рынка IoT-устройств являются такие стандарты, как NB-Fi и LoRaWAN RU, которые прошли все необходимые этапы и были опубликованы [6].

Неотъемлемой частью стандартизации, будь то собственные решения или локализация международных разработок, являются необходимые исследования в части доверия и в этом смысле использование предварительных национальных стандартов (ПНСТ) и ГОСТ – это постоянная гарантия качества и безопасности, более того, отдельные стандарты посвящены конкретным вопросам информационной безопасности. Требования должны быть сформулированы "как нужно" в части поддерживаемых протоколов обмена и данных форматы, мандаты, надежность и совместимость. Для этого и существуют стандарты. Рынок не будет развиваться лучше или быстрее, если он будет наводнен иностранными устройствами, о которых неизвестно, как долго, насколько хорошо они работают, какие протоколы используют и т. д.

Более актуальная задача для российского бизнеса – это защита от нападений. Для этого в первую очередь, необходим быстрый импорт альтернатив для систем управления IoT-устройствами, и затем переход на отечественную компонентную базу и ПО [7]. В Российской Федерации нужно регулировать не сами смарт-устройства, как предлагает Еврокомиссия, а безопасность инфраструктуры, где угрозы со стороны интернета вещей наиболее опасны. В первую очередь – промышленные предприятия и объекты критической инфраструктуры. Процесс регулирования информационной безопасности на таких объектах в России уже идет и никаких дополнительных мер на данном этапе не требуется. Характерно, что подключенные к сети Интернет контроллеры, различные автоматические клапаны, камеры распознавания лиц и т. д. хорошо защищены строгими требованиями безопасности и нормами отраслевых регуляторов. Люди должны брать на себя полную ответственность за свою безопасность, когда речь идет о домашних умных устройствах, для этого в первую очередь требуется повысить цифровую грамотность.

Все элементы умного дома должны находиться в защищенной сети Wi-Fi и находиться отдельно от домашней или гостевой сети [8].

Список источников

1. *Довгаль В.А., Довгаль Д.В.* Управление ресурсами в Интернете Вещей // Дистанционные образовательные технологии: мате-

риалы II Всерос. науч.-практ. конф., г. Ялта, 2017 г. Симферополь: АРИ-АЛ, 2017. С. 168–173.
2. *Kevin Ashton.* That "Internet of Things" Thing // RFID Journal. 2009. 22 June. URL: http://www.rfidjournal.com/articles/pdi74986 (дата обращения: 16.10.2022).
3. *Интернет* вещей – а что это? URL: https://habr.com/ru/post/149593/ (дата обращения: 20.10.2022).
4. *Рожкова Ж.* Интернет вещей: прогнозы по развитию рынка. URL: https://www.likeni.ru/analytics/internet-veshchey-prognozy-po-razvitiyu-rynka/ (дата обращения: 20.10.2022).
5. *Применение* IOT в реальном бизнесе. URL: https://rb.ru/longread/iot-cards/ (дата обращения: 20.10.2022).
6. *Интернет* вещей в России. URL: https://www.pwc.ru/ru/publications/iot/ IoT-inRussia-research_rus.pdf (дата обращения: 20.10.2022).
7. *Довгаль В.А., Довгаль Д.В.* Проблемы и задачи безопасности интеллектуальных сетей, основанных на Интернете Вещей // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2017. Вып. 4(211). С. 140–147. URL: (дата обращения: 20.10.2022).
8. *IoT* и проблемы безопасности. URL: https://habr.com/ru/company/unet/ blog/410849/ (дата обращения: 20.10.2022).

References

1. *Dovgal' V.A., Dovgal' D.V.* Upravlenie resursami v Internete Veshchej. Distancionnye obrazovatel'nye tekhnologii: materialy II Vseros. nauch.-prakt. konf., g. YAlta, g. Simferopol': ARI-AL. 2017;168-173. (In Russ.).
2. *Kevin Ashton.* That "Internet of Things" Thing. RFID Journal. 2009. URL: http://www.rfidjournal.com/articles/pdi74986 (accessed: 16.10.2022).
3. *Internet* veshchej – a chto eto? URL: https://habr.com/ru/post/149593/ (accessed: 20.10.2022).
4. *Rozhkova ZH.* Internet veshchej: prognozy po razvitiyu rynka. URL: https://www.likeni.ru/analytics/internet-veshchey-prognozy-po-razvitiyu-rynka/ (accessed: 20.10.2022).
5. *Primenenie* IOT v real'nom biznese. URL: https://rb.ru/longread/iot-cards/ (accessed: 20.10.2022).
6. *Internet* veshchej v Rossii. URL: https://www.pwc.ru/ru/publications/iot/ IoT-inRussia-research_rus.pdf (accessed: 20.10.2022).
7. *Dovgal' V.A., Dovgal' D.V.* Problemy i zadachi bezopasnosti intellektual'nyh setej, osnovannyh na Internete Veshchej. Vestnik Adygejskogo gosudarstvennogo universiteta. Ser. Estestvenno-matematicheskie i tekhnicheskie nauki. 2017;4 (211):140-147. (In Russ.).
8. *IoT* i problemy bezopasnosti. URL: https://habr.com/ru/company/unet/ blog/410849/ (accessed: 20.10.2022).

Информация об авторах:

М. А. Зосимова – кандидат экономических наук, и. о. заведующего кафедрой инфокоммуникационных и профессиональных дисциплин, Волго-Вятский филиал Московского технического университета связи и информатики (603011, Россия, г. Нижний Новгород, ул. Менделеева, д. 15), AuthorID 1172206;

С. А. Смирнов – старший преподаватель кафедры инфокоммуникационных и профессиональных дисциплин, Волго-Вятский филиал Московского технического университета связи и информатики (603011, Россия, г. Нижний Новгород, ул. Менделеева, д. 15), AuthorID 805258.

Information about the authors:

M. A. Zosimova – PhD in Economics, Head of Department of Infocommunication and Professional Disciplines, Moscow Technical University of Communications and Informatics (Volga-Vyatka branch) (15 Mendeleeva Street, Nizhny Novgorod, Russia, 603011), AuthorID 1172206;

S. A. Smirnov – Senior Lecturer of Infocommunication and Professional Disciplines Moscow Technical University of Communications and Informatics (Volga-Vyatka branch) (15 Mendeleeva Street, Nizhny Novgorod, Russia, 603011), AuthorID 805258.