УДК 004.7
doi:10.15217/issn1684-8853.2018.2.84

СИСТЕМА ДЕТЕКТИРОВАНИЯ ОПАСНЫХ ВЕЩЕСТВ ПО ЗАПАХУ, ПОСТРОЕННАЯ НА ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ

Т. М. Татарникова[a], *доктор техн. наук, профессор, tm-tatarn@yandex.ru*
И. Н. Дзюбенко[a], *магистрант, azruhal@gmail.com*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Постановка проблемы: *при обеспечении защиты от внешних угроз террористического характера отсутствует комплексное решение, позволяющее детектировать угрозы по запаху, т. е. по нахождению определенных частиц вещества в воздухе.* ***Цель:*** *разработка концепта системы детектирования опасных веществ по запаху, построенной с применением технологии Интернета вещей.* ***Результаты:*** *создан концепт системы детектирования, позволяющей обеспечивать безопасность на территории путем обнаружения угроз по запаху. Система детектирования представляет собой разновидность беспроводной сенсорной сети с топологией типа «звезда», которая состоит из трех типов узлов: сенсорного узла, шлюза, центрального узла. Концепт доведен до макета, позволяющего обнаруживать такие угрозы, как утечка бензола, бутана, метана, пропана и возгорание на ранней стадии. Комплексность предлагаемого решения обеспечивается выбором платформы Интернета вещей.* ***Практическая значимость:*** *разработанный концепт системы детектирования на базе платформы Интернета вещей является инновационным решением, направленным на создание новой продукции, востребованной рынком систем безопасности.*

Ключевые слова *— безопасность человека, детектирование угроз по запаху, система детектирования, Интернет вещей, макет системы.*

Цитирование: Татарникова Т. М., Дзюбенко И. Н. Система детектирования опасных веществ по запаху, построенная на технологии Интернета вещей // Информационно-управляющие системы. 2018. № 2. С. 84–90. doi:10.15217/issn1684-8853.2018.2.84
Citation: Tatarnikova T. M., Dzubenko I. N. IoT System for Detecting Dangerous Substances by Smell. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 2, pp. 84–90 (In Russian). doi:10.15217/issn1684-8853.2018.2.84

Введение

Безопасность — это одна из основных проблем современности и актуальных направлений деятельности государства и общества. Безопасность и противодействие терроризму входят в перечень приоритетных направлений развития науки, технологий и техники Российской Федерации [1].

Представленные на рынке технические решения обнаружения угроз человеку, обусловленных терроризмом, в основном ограничиваются незначительным выбором систем физической охраны. Однако эти системы сложно назвать идеальными, и в свете последних событий, связанных с террористическими актами, произошедшими в России и странах Европы, идеи для улучшения подобных систем и появления новых остаются актуальными [2].

Одним из признаков, указывающим на возникновение такого типа угроз, является запах. Хотя есть отдельные методы, позволяющие обнаруживать угрозы террористического характера по запаху, например с помощью детектора пороха в аэропорту, комплексных решений этой проблемы пока не существует.

В статье предлагается технология построения системы детектирования веществ по запаху, основанная на концепции Интернета вещей.

Интернет вещей (Internet of Things — IoT) — это новая инфокоммуникация, технически реализованная как вычислительная сеть, состоящая из множества физических предметов («вещей»), оснащенных встроенными технологиями для обмена данными между собой и внешней средой. Изначально придуманный для описания умных бытовых вещей, в настоящее время Интернет вещей стремительно развивается благодаря распространению беспроводных сетей, появлению облачных вычислений, развитию межмашинных вычислений и уменьшению стоимости производства микросхем [3].

Сегодня в среде Интернета вещей существует огромное количество разнообразных программных и аппаратных решений: «умных устройств», платформ разработки, датчиков, программного обеспечения, — что позволяет использовать технологию IoT для создания самых различных систем, в том числе и в области обеспечения безопасности [4].

Разработка системы детектирования опасных веществ по запаху включает в себя следующие этапы: создание концепта системы, выбор ее платформы реализации и аппаратных элементов, соответствующих требованиям поставленной задачи, написание программного обеспечения каждого элемента системы и их интеграция в рамках раз-

рабатываемого концепт-продукта. В работе создан упрощенный макет системы детектирования.

Обзор систем, использующих обнаружение угрозы по присутствию веществ в воздухе

Поскольку предлагаемая система детектирования задумана как некоторая комплексная реализация, то представляет интерес обзор технологических решений, использующих методы обнаружения угроз по присутствию веществ в воздухе (таблица).

Следует заметить, что из приведенных в таблице решений электронный нос мог бы претендовать на комплексность, но пока для большинства задач оно является дорогостоящим, к тому же представляет собой локальный способ детектирования [5].

Невозможно не упомянуть и о таком решении, как служебные собаки. В интересах данной работы собаки могут быть своего рода биодетекторами, способными обнаружить опасные вещества по запаху даже при очень небольшой их концентрации, и пока они обладают рядом преимуществ над датчиками запахов. Однако у них есть и множество недостатков по сравнению с технологическим решением. Служебные собаки требуют качественной многолетней дрессировки, нуждаются в дорогостоящем содержании и сопровождении специалиста-кинолога. Кроме этого, служебных собак нельзя использовать для обнаружения химически опасных веществ. Поэтому использование служебных собак для обнаружения опасных запахов на охраняемой территории, как правило, ограничивается поиском наркотических и взрывчатых веществ в зоне входа-выхода.

Концепт системы детектирования

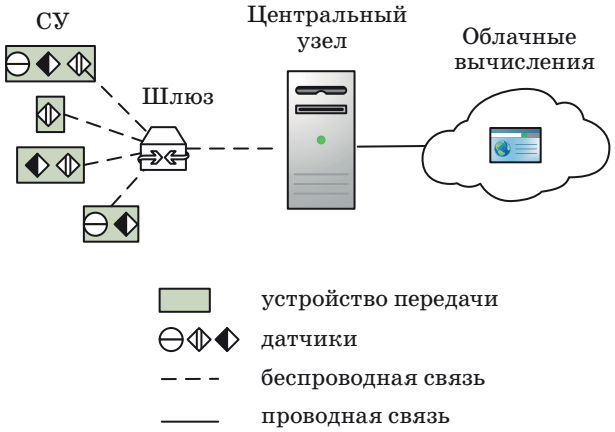
На концептуальном уровне система детектирования представляет собой разновидность беспроводной сенсорной сети с топологией типа «звезда» [6–8]. Система состоит из сенсорного узла *СУ*, шлюза, центрального узла (рис. 1).

Сенсорный узел представляет собой прибор передачи, к которому подключен один или набор датчиков газа, позволяющих обнаруживать различные угрозы.

Шлюз — узел агрегации данных, поступающих от множества СУ с последующей их передачей на центральный узел. Кроме агрегации шлюз обеспечивает связь между узлами системы, выполняя согласование форматов данных, скоростей и протоколов взаимодействия [9]. Взаимодействие между сенсорными узлами и шлюзом осуществляется по технологии Bluetooth, между шлюзом

■ Сравнение существующих решений
■ Comparison of modern solutions

Решение	Назначение	Функциональные возможности	Область применения	Пример практического использования
Датчики газов	Измерение концентрации некого газа в воздухе	Определение концентрации взрывоопасных, токсичных, горючих газов, определение опасно низкого уровня кислорода и возгорания	На объектах, где возможна утечка опасных веществ	Алкотестер Dräger Alcotest 6810
Пожарные извещатели	Обнаружение возгорания	Обнаружение пожара: по повышенной температуре по присутствию дыма в воздухе по газу, выделяемому при тлении или горении материалов	На любых территориях: на предприятиях, в общественных местах, лесных массивах	Отечественный газовый пожарный извещатель ИП 435-7 производства «Юнитест», детектирующий пожар по уровню CO
Детекторы следовых количеств взрывчатых веществ	Охрана от террористических актов	Обнаружение остаточных следов взрывчатых веществ на одежде субъекта или в помещении	В аэропортах и метро	Детектор следов взрывчатых веществ SABRE 5000 Детектор следов ВВ Fido XT
Электронный нос	Определение запахов и вкусов	Комплексная система анализа воздуха в целях определения запаха	Контроль качества продуктов, контроль чистоты	Электронный нос Cyranose 320



■ ***Рис. 1.*** Концепт системы детектирования
■ ***Fig. 1.*** Concept of detection circuit

и центральным узлом — по Wi-Fi, соответственно, шлюз должен поддерживать обе технологии [10].

Центральный узел — сервер, обрабатывающий данные со всех узлов системы, представляет собой программное обеспечение на компьютере, обеспечивающее оператору системы детектирования доступ к веб-интерфейсу [11].

Описание реализованного макета системы детектирования

Концепт-продукт предлагаемой системы детектирования реализован в виде макета, представляющего собой цепь из сенсорного, агрегирующего и центрального устройств (рис. 2).

Макет реализован на платформе Genuino 101 по причине наличия встроенного беспроводного интерфейса и большого числа адаптированных под платформу программных и аппаратных решений. СУ представляет собой эту платформу с подключенными к ней датчиками газа, способными обнаруживать ряд угроз [12].

Набор датчиков представляет собой широко распространенные полупроводниковые датчики серии MQ производства Winsen Electronics Technology Co Ltd. Выбраны датчики MQ-3, MQ-5 и MQ-7 [13–15]. Датчик MQ-3 реагирует на пары спирта, что позволяет детектировать такие угрозы, как, например, утечка бензола на предприятии (бензол — крайне опасное летучее вещество, сильный канцероген и при больших концентрациях в воздухе взрывоопасен; широко используется в промышленности). Датчик MQ-5 реагирует на природный газ (бутан, метан, пропан). Датчик MQ-7 реагирует на монооксид углерода (угарный газ) и водород, что позволяет обнаруживать возгорания на ранней стадии. Так как эти датчики являются полупроводниковыми, присутствует

■ ***Рис. 2.*** Схема макета системы детектирования
■ ***Fig. 2.*** Schematic of detection system model

проблема перекрытия их показаний. В предоставленных производителем данных о датчиках указано, что датчик MQ-3 по значениям практически не пересекается с остальными (рис. 3, *а*), а датчик MQ-5 может также иметь реакцию на водород, пусть и в меньшем объеме, чем MQ-7 (рис. 3, *б* и *в*), что необходимо учитывать при анализе данных с датчиков.

Программное обеспечение для СУ написано средствами Arduino IDE. Данные с датчиков собираются в аналоговом виде и представлены как числа от 0 до 1024. Передача данных происходит через Bluetooth low energy (BLE) с помощью библиотеки Genuino 101 CurieBLE.

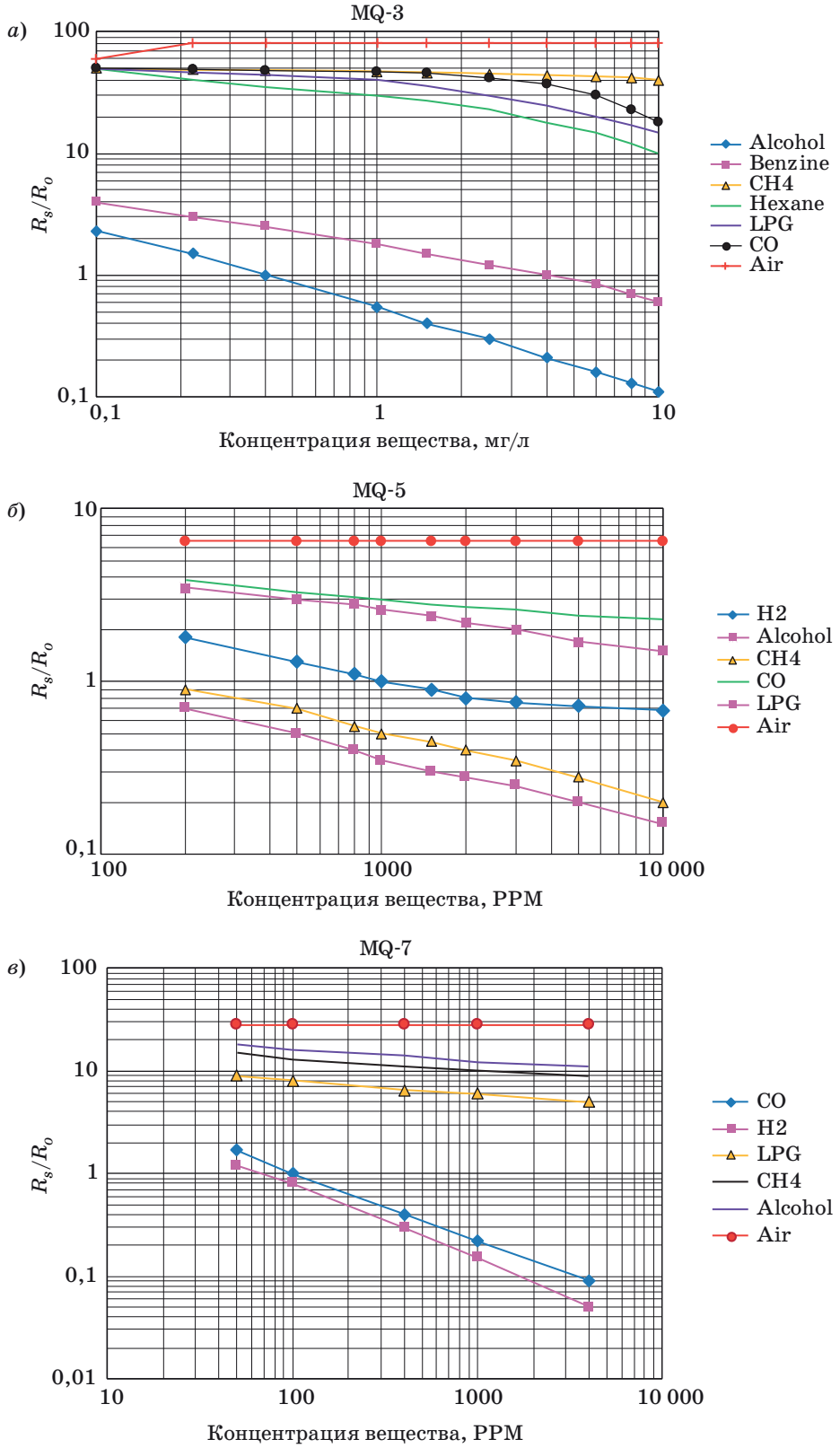
Реализованный макет СУ (рис. 4, *а* и *б*) способен обнаруживать такие угрозы, как утечка бензола, природного газа и возгорания на ранней стадии, и имеет возможность передавать данные об этих событиях по технологии BLE.

Для обеспечения задач шлюза выбрана платформа Intel Edison, поддерживающая технологии BLE и Wi-Fi. Intel Edison — это полноценный компьютер на плате (computer on board) с двухъядерным процессором Atom, 1 ГБ оперативной памяти, 4 ГБ eMMC флеш-памяти, модулями Wi-Fi, Bluetooth 4 и контроллером USB. Для обеспечения питания платформа Intel Edison подключена через коннектор Hirose 70-pin DF40 Series к Arduino-совместимой плате расширения (рис. 5).

Программное обеспечение для шлюза написано средствами программной платформы Node.js, представляющей собой транслятор языка JavaScript в машинный код, что позволяет использовать JavaScript как язык общего назначения.

Центральное устройство реализовано как локальный сервер на компьютере средствами программной платформы Node.js. Кроме обработки поступающих данных сервер обеспечивает работу простого веб-приложения для оператора системы детектирования. Веб-приложение использует фреймворк node express [16].

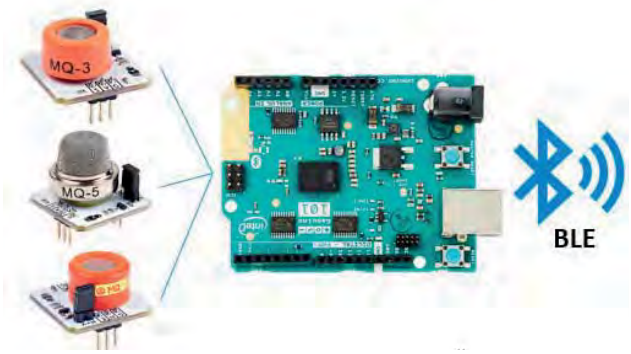
Обработка получаемых сервером данных происходит следующим образом: для каждого датчика запоминаются 10 последних значений; если новое значение m_i датчика больше суммы усредненного по десяти значениям показаний и порога Δ (для MQ-5 и MQ-7 $\Delta = 20$, для MQ-3 $\Delta = 50$), то счи-



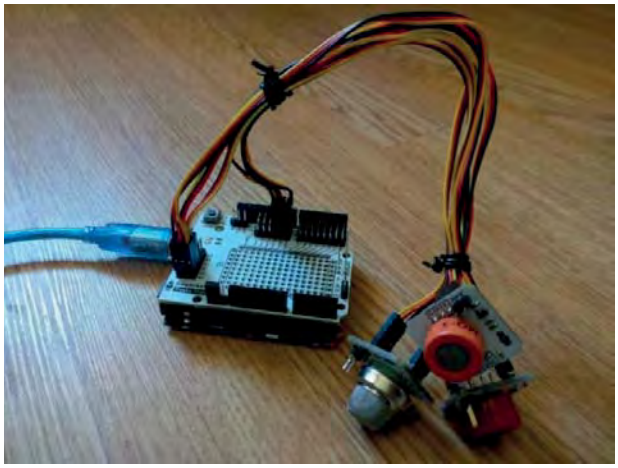
■ ***Рис. 3.*** Отношение концентрации веществ к показаниям R_s/R_o датчика MQ-3 (*а*), MQ-5 (*б*) и MQ-7 (*в*) (R_s — сопротивление датчика при определении им концентрации газа в окружающей среде, R_o — сопротивление датчика, измеренное при определенной концентрации детектируемого газа)

■ ***Fig. 3.*** The ratio of the concentration of substances to the readings of the R_s/R_o of the MQ-3 (*a*), MQ-5 (*б*) and MQ-7 (*в*) sensor (R_s is the resistance of the sensor when determining the gas concentration in the environment, R_o is the resistance of the sensor measured at a certain concentration of the detected gas)

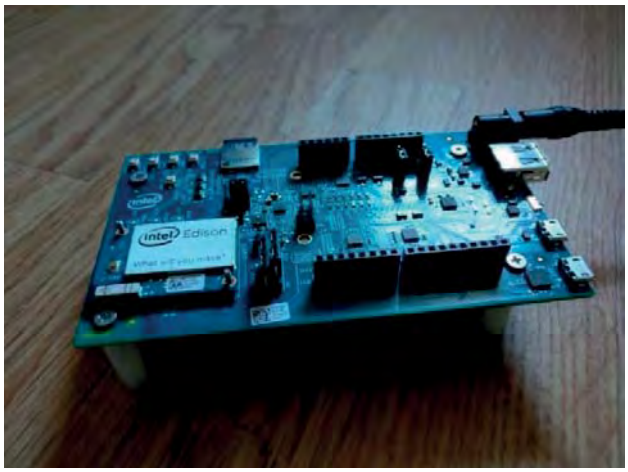
а)



б)



■ ***Рис. 4.*** Общая схема (*а*) и вид (*б*) реализованного сенсорного устройства
■ ***Fig. 4.*** General scheme (*a*) and form (*б*) of the realized sensor device



■ ***Рис. 5.*** Реализованное агрегирующее устройство
■ ***Fig. 5.*** The realized aggregating device

■ ***Рис. 6.*** Страница веб-приложения центрального устройства
■ ***Fig. 6.*** The central device web application page

тается, что датчик сработал на резкое повышение концентрации вещества:

$$m_i > \frac{\sum_{k=1}^{10} m_k}{10} + \Delta.$$

На странице веб-приложения выводятся данные с датчиков, и если значение концентрации вещества превышает допустимое, то напротив значения датчика появится соответствующее сообщение (рис. 6).

Заключение

Предложенный в работе концепт системы детектирования на базе платформы Интернета вещей по сути варианта исполнения является инновационным решением, поскольку оно направлено на создание, главным образом, новой продукции, востребованной рынком систем безопасности.

Имея широкий спектр применения, система детектирования, позволяющая обеспечивать безопасность на территории путем обнаружения угроз по запаху, в ближайшее время может стать ключевым направлением развития индустрии безопасности, открывающим новые возможности для повышения качества подобных систем.

Разработанный концепт-продукт системы детектирования в виде макета демонстрирует возможности по обнаружению таких угроз, как утечка бензола, бутана, метана, пропана и возгорания на ранней стадии.

Литература

1. Постановление Правительства РФ от 25.03.2015 № 272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)». http://pravo.gov.ru/proxy/ips (дата обращения: 19.08.2017).
2. Р 78.36.026-2012 Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны огражденных территорий и открытых площадок. — М.: НИЦ «Охрана», 2012. — 182 с.
3. **Hersent O., Boswarthick D., Elloumi O.** The Internet of Things: Key Applications and Protocols. — Willey, 2012. — 370 p.
4. **Гольдштейн Б. С., Кучерявый А. Е.** Сети связи пост-NGN. — СПб.: БХВ-Петербург, 2014. — 160 с.
5. **Долгополов Н. В. Яблоков М. Ю.** «Электронный нос» — новое направление индустрии безопасности // Мир и безопасность. 2007. № 3. С. 54–59.
6. Recommendation Y.2060: Overview of Internet of Things. — Geneva: ITU-T, February 2012. http://www.itu.int/rec/T-REC-Y.2060-201206-I (дата обращения: 26.01.2017).
7. **Росляков А. В., Ваняшин С. В., Гребешков А. Ю., Самсонов М. Ю.** Интернет вещей. — Самара: ПГУТИ, 2014. — 200 с.
8. **Татарникова Т. М., Елизаров М. А.** Модель оценки временных характеристик при взаимодействии в сети Интернета вещей//Информационно-управляющие системы. 2017. № 2. С. 44–50. doi:10.15217/issn1684-8853.2017.2.44
9. **Kellmereit D.** The Silent Intelligence: The Internet of Things. — DND Ventures LLC, 2013. — 454 p.
10. **Татарникова Т. М.** Структурный синтез центра сопряжения корпоративных сетей // Информационно-управляющие системы. 2015. № 3. С. 92–98. doi:10.15217/issn1684-8853.2015.3.92
11. **Bonomi F.** Fog Computing and its Role in the Internet of Things // Proc. of the First Edition of the MCC Workshop on Mobile Cloud Computing. 2012. P. 13–16.
12. IEEE Std 802.11-2007 IEEE Standard for Information Technology — Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks — Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. — IEEE Computer Society, June 2007. https://www.twirpx.com/file/1167805/ (дата обращения: 01.02.2018).
13. Technical Data MQ-3 Gas Sensor. https://arduino-market.ru/sensory-:-datchiki/modul-mq-3 (дата обращения: 01.02.2018).
14. Technical Data MQ-5 Gas Sensor. https://arduino-market.ru/uploads/ DatasheetMQ_5.pdf (дата обращения: 01.02.2018).
15. Сайт gas-sensor.ru (дата обращения: 01.02.2018).
16. Recommendation Y.2069: Framework of the WEB of Things. — Geneva: ITU-T, July 2012. http://www.itu.int/rec/T-REC-Y.2069-201207-I (дата обращения: 01.02.2018).

UDC 004.7
doi:10.15217/issn1684-8853.2018.2.84

IoT System for Detecting Dangerous Substances by Smell

Tatarnikova T. M.[a], Dr. Sc., Tech., Associate Professor, tm-tatarn@yandex.ru
Dzubenko I. N.[a], Graduate Student, azruhal@gmail.com
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: When providing protection against external terrorist threats, there is no comprehensive solution which would allow you to detect threats by smell, i.e. by finding certain matter particles in the air. **Purpose:** Concept of dangerous substance smell detection system built with the use of Internet of Things (IoT) technology. **Results:** We have created a concept of a detection system which would provide security within a certain area by detecting smell threats. The detection system is a variation of wireless sensor network with a "star" topology, consisting of three types of nodes: a sensor node, a gateway, and a center node. The concept has reached a prototype which detects such threats as leaks of benzene, butane, methane or propane and early-stage conflagration. The comprehensiveness of the proposed solution is. provided by choosing IoT as a platform. **Practical relevance:** The developed concept is an innovative solution which can be used to create new products demanded at the market of security systems.

Keywords — Human Security, Detection of Threats by Smell, Detection System, Internet of Things, System Prototype.

Citation: Tatarnikova T. M., Dzubenko I. N. IoT System for Detecting Dangerous Substances by Smell. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 2, pp. 84–90 (In Russian). doi:10.15217/issn1684-8853.2018.2.84

References

1. *Postanovlenie Pravitel'stva RF ot 25.03.2015 N 272 "Ob utverzhdenii trebovanii k antiterroristicheskoi zashchishchennosti mest massovogo prebyvaniia liudei i ob"ektov (territorii), podlezhashchikh obiazatel'noi okhrane politsiei, i form pasportov bezopasnosti takikh mest i ob"ektov (territorii)"* Available at: http://pravo.gov.ru/proxy/ips (accessed 19 August 2017).
2. *R 78.36.026-2012 Rekomendatsii po ispol'zovaniiu tekhnicheskikh sredstv obnaruzheniia, osnovannykh na razlichnykh fizicheskikh printsipakh, dlia okhrany ograzhdennykh territorii i otkrytykh ploshchadok* [R 78.36.026-2012 Recommendations on the Use of Detection Technology based on Various Physical Principles for the Protection of Fenced Areas and Open Areas]. Moscow, Nauchno-issledovatel'skiy tsentr "Okhrana" Publ., 2012. 182 p. (In Russian).
3. Hersent O., Boswarthick D., Elloumi O. *The Internet of Things: Key Applications and Protocols*. Willey, 2012. 370 p.
4. Gol'dshtejn B. S., Kucherjavyj A. E. *Seti svjazi post-NGN* [Post-NGN Communication Networks]. Saint-Petersburg, BKhV-Peterburg Publ., 2014. 160 p. (In Russian).
5. Dolgopolov N. V., Yablokov M. Yu. Electronic Nose — a New Direction of the Security Industry. *Mir i bezopasnost'* [Peace and Security], 2007, no. 3, pp. 54–59 (In Russian).
6. *Recommendation Y.2060: Overview of Internet of Things*. Geneva, ITU-T, February 2012. Available at: http://www.itu. int/rec/T-REC-Y.2060-201206-I (accessed 26 January 2017).
7. Roslyakov F. V., Vanyashin S. V., Grebeshkov A. Y., Samsonov M. Y. *Internet veshchei* [Internet of Things]. Samara, PGUTI Publ., 2014. 200 p. (In Russian).
8. Tatarnikova T. M., Elizarov M. A. Model of Estimating Temporal Characteristics of IoT Network Interaction. *Informatsionno-upravlyayushhie systemy* [Information and Control System], 2017, no. 2, pp. 44–50 (In Russian). doi:10.15217/issn1684-8853.2017.2.44
9. Kellmereit Daniel. *The Silent Intelligence: The Internet of Things*. DND Ventures LLC, 2013. 454 p.
10. Tatarnikova T. M. Structural Synthesis of an Interface Center for Corporate Networks. *Informatsionno-upravlyayushhie systemy* [Information and Control System], 2015, no. 3, pp. 92–98 (In Russian). doi:10.15217/issn1684-8853. 2015.3.92
11. Bonomi F. Fog Computing and its Role in the Internet of Things. *Proc. of the First Edition of the MCC Workshop on Mobile Cloud Computing*, 2012, pp. 13–16.
12. *IEEE Std 802.11-2007 IEEE Standard for Information Technology —Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Network — Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE Computer Society, June 2007. Available at: https://www.twirpx.com/file/1167805/ (accessed 01 February 2018).
13. *Technical Data MQ-3 Gas Sensor*. Available at: https://arduino-market.ru/sensory-:-datchiki/modul-mq-3 (accessed 01 February 2018).
14. *Technical Data MQ-5 Gas Sensor*. Available at: https://arduino-market.ru/uploads/ DatasheetMQ_5.pdf (accessed 01 February 2018).
15. Available at: *gas-sensor.ru* (accessed 01 February 2018).
16. *Recommendation Y.2069: Framework of the WEB of Things*. Geneva, ITU-T, July 2012. Available at: http://www.itu.int/rec/T-REC-Y.2069-201207-I (accessed 01 February 2018).

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста: входите на страницу http://www.researcherid.com, слева под надписью «New to ResearcherID?» нажимаете на синюю кнопку «Join Now It's Free» и заполняете короткую анкету. По указанному электронному адресу получаете сообщение с предложением по ссылке заполнить полную регистрационную форму на ORCID. Получаете ID.