СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время существует необходимость в автоматизации рутинных процессов. Более 70 лет мировой истории это представлялось людям, как прислуживающие роботы, но теперь эти процессы стали более известны как IoT. Эта сфера помогает автоматизировать повторяющиеся задачи, проконтролировать протекание длительных процессов, уменьшить потребление ресурсов, таких как электроэнергия, и др.

В ряде западных стран такие системы интегрированы на многие предприятия, заводы, или просто вплетены в городскую среду, например, для контроля освещенности улиц. В Российской Федерации данная сфера находится на этапе активного внедрения у частных компаний, которые используют IoT для современных технологических производств, экономя средства на излишней работе станков. Внедрение IoT в Российской Федерации на данный момент не является достаточным, что делает актуальной тему данного исследования.

Целью НИР является анализ зарубежных и отечественных источников для формирования представления о веб-технологиях, используемых в сфере IoT.

Объектом исследования являются информационные системы, осуществляющие управления элементами IoT.

Предметом исследования являются результаты анализа отечественной и зарубежной литературы по теме исследования.

Задачи исследования:

- Составить обзор российских и зарубежных научных исследований, посвященных IoT.
- Провести анализ отечественных научных исследований о существующих разработках в сфере IoT.
- Провести анализ зарубежных научных исследований в области проектирования IoT сервисов.

Теоретические основы исследования. При анализе источников было выявлено, что тема внедрения элементов IoT освещена подробно, однако массового внедрения этой технологии на территории Российской Федерации не было.

В работе (Г.Ю. Портянкин, О.Ю. Рязанов) описаны принципы работы новой системы, которая позволяет решать ряд расчетных задач сельского хозяйства, получая и обрабатывая данные с умных устройств. По исследованию (Н.В. Рогачева) автор подытоживает текущие проблемы сферы и задачи, которые необходимо решить, чтобы продвинуть эту сферу вперед в Российской Федерации.

В трудах зарубежных авторов (M. Stusek, K. Zeman, P. Masek, J. Hosek, J. Sedova) подробно рассмотрены IOT протоколы передачи данных и перспективы их развития.

В рассмотренных источниках были приведены примеры реализации системы на IoT устройствах, однако сегодня сервисы, по которым были приведены примеры, не существуют по причине закрытия или нерелевантного принципа работы. Приведенные факторы обуславливают **актуальность темы научно-исследовательской работы**.

Информационная база исследования: eLIBRARY, CyberLeninka ResearchGate.

Методы исследования. Для решения задач исследования использовался комплекс теоретических и эмпирических взаимодополняющих методов исследования, среди которых ведущими были следующие методы: анализ, сравнение и обобщение, методы индукции и дедукции.

Результаты исследования. Проведенный анализ:

- ведущих трендов социально-экономического и технологического развития показал, что проблема освещенности сферы интернета вещей в Российской Федерации является актуальной и востребованной, так как ее решение обеспечит создание лучших инструментов по управлению умными устройствами.
- отечественных и зарубежных источников позволил выделить и описать основные направления реализации системы с умными IoT датчиками, а

также были инструменты, которые будут задействованы при ее проектировании.

1 СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОБЛЕМЫ

В настоящее время, особенно в период пандемии COVID-19, возникла необходимость в обустройстве своего жилища, и развития сферы умных га-джетов. В мире растет количество «подключенных» устройств (по оценкам отраслевых аналитиков, их количество достигнет 20–50 млрд единиц к 2020 г.) и вместе с ним – количество примеров применения Интернета вещей (Internet of Things, IoT) в экономике: энергетике, промышленности, жилищно-коммунальном хозяйстве, сельском хозяйстве, транспорте, здравоохранении и др [1].

Как пишет Forbes, в 2022 году в IoT можно выделать пять мировых трендов развития [2]:

- IoT в медицине – от фитнес браслетов до датчиков в реанимационных палатах.
- Защита передачи данных по сети.
- Edge computing – выполнение вычислений непосредственно на устройстве, без передачи на сервер, усиление мощностей каждого из устройств.
- Увеличение роли IoT в бизнесе, развитие VR, AR устройств, создание цифровых двойников объектов и даже предприятий целиком.
- Внедрение IoT датчиков в больших компаниях для экономии электроэнергии, интернет-трафика, или других потребляемых ресурсов.

В то же время, эксперты ЦНИИ «Электроника» совместно с АНО «Цифровая экономика» утверждают, что большинство производителей оборудования для IoT сферы в России используют отечественные комплектующие. У четверти из них доля российских деталей в цене продукции превыша-ет половину себестоимости.

Генеральный директор ЦНИИ «Электроника» высказывает обеспокоенность тем, что индустрия в России находится на начальных этапах разви-тия, но вместе с этим примечает, что «Интернет вещей – это безусловный тренд», и с каждым годом растет количество компаний-производителей ум-ных устройств, а также компаний, использующих эти устройства для улуч-шения собственных

экономических показателей. Также она утверждает, что данные исследования подтверждают высокую вакантность потребительской ниши [3].

2 АНАЛИЗ ОТЕЧЕСТВЕННЫХ НАУЧНЫХ ИСТОЧНИКОВ ПО ТЕМЕ ИССЛЕДОВАНИЯ

2.1 Современное состояние IoT сферы

В 1999 году одним из исследователей RFID-технологий Кевином Эштоном, возможно, впервые было употреблено словосочетание «Интернет вещей» (Internet of Things, IoT). Эштон использовал новоизобретенный тер-мин в ходе своей презентации для Procter&Gamble, посвященной влиянию RFID на разные рынки.

В работе «Интернет вещей: обзор основных проблем и задач» (Н.В. Рогачева) поднимаются проблемы текущего состояния сферы [4].

- Безопасность.
- Большое количество разнообразных несовместимых стандартов.
- Энергоэффективность.
- Повышенное потребление интернет-трафика.
- Недостаток специалистов с достаточной квалификацией в распределенных системах.

В России активно пытаются решить проблему несовместимых стандартов и создают новые ГОСТы для стандартов IoT, такие как:

- ТК-194 «Киберфизические системы», благодаря которому мы получи-ли в этом году серию национальных стандартов.
- ТК-26 «Криптографическая защита информации», где идут работы по улучшение безопасности протоколов Интернета вещей.

Также можно видеть улучшение взаимодействия между техническими комитетами, что положительно влияет на качество и сроки появления новых стандартов в России [5]. Стоит упомянуть компанию «Доверенная платформа», которая сделала значительный вклад на этом поприще. Авторы статьи «Модуль IoT сервер ИКС “Агроаналитика IoT”» (Г.Ю. Портянкин, О.Ю. Рязанов) пишут о новой созданной ими системе, которая позволяет получать данные

с устройств, хранить и обрабатывать полученные данные. Программа позволяет решать ряд расчетных задач сельского хозяй-ства, такие как подсчет топлива, стоянок, остановок и простоев, составление логистической цепочки по урожаю, выявление неоднородности динамики биомассы, расчет площади обработки [6]. В работе «Классификация систем и устройств IoT» (А.П. Карловский, В.Л. Можгинский) авторы разделяют IoT устройства на несколько категорий [7]:

- Сенсоры и исполнительные механизмы.
- Управление, локальная обработка данных и хранение информации.
- Канал связи со шлюзом в локальную сеть или Интернет.
- Инфраструктура передачи данных, облачные технологии.
- Программно-аппаратные сервисы интеграции устройств, управле-ния, визуализации и обработки информации.
- Аналитические системы.

2.2 Варианты реализации системы IoT

Существует обобщённая архитектура IoT систем, как написали авторы работы «Современное состояние дел в области создания систем с интеллекту-альными датчиками» Ю.И. Иванов, и др. [8]. Это embedded часть, которая находится непосредственно на устройстве, серверная часть, где хранятся и агреггируются все данные и front-end часть. Общение может происходить по различным протоколам, таким как Zigbee, Wi-Fi, и др. Для анализа front-end части сервиса была изучена работа «Сравни-тельный анализ JS фреймворков: Vue, React и Angular» (К.Н. Калугина), в которой автор подробно описал 3 популярных сегодня JavaScript фреймвор-ков. Автором были выделены фреймворки Angular и React, которые предла-гают высокую относительно Vue производительность и более широкую под-держку комьюнити. Также было отмечено, что у Vue значительно ниже порог входа, из-за которого он может быть предпочтителен для некоторых проек-тов. [9]. Для проектирования серверной части необходимо определиться с су-ществующими решениями для построения API. Ознакомившись с работами «Создание REST API микросервиса с использованием Flask»

[10], «Разра-ботка серверной части web-приложений на JAVA» [11], «Архитектурные особенности проектирования и разработки веб приложений», [12], а также «Использование Node.JS для серверной архитектуры Web-приложения» [13] был сделан вывод, что разработанный сервис на фреймворке Flask обладает наибольшими конкурентными преимуществами, такими как поддерживаемость, высокая скорость разработки, читаемость кода.

3 АНАЛИЗ ЗАРУБЕЖНЫХ НАУЧНЫХ ИСТОЧНИКОВ ПО ТЕМЕ ИССЛЕДОВАНИЯ

В работе «Water preservation using IoT: A proposed IoT system for de-tecting water pipeline leakage» (A. Abusukhon, F. Altamimi) авторы пишут о использовании IoT датчиков для детектирования протечек в водопроводе и автоматическом уведомлении всех подписанных пользователей для быстрого устранения проблемы сантехником [14].

Как пишут в казахстанской работе «Protecting sanctuaries and national parks in Kazakhstan with IoT technologies» (K. Kim), использование IoT устройств релевантно для интеграции в большие национальные парки, которыми сложно или практически невозможно управлять с помощью неавтоматизированных средств [15].

Также можно найти работы по созданию умных кампусов университетов, например, «IoT smart campus review and implementation of IoT applica-tions into education process of university» (A. Zhamanov, R. Suliyev, Z. Kaldyk-ulova, Z. Sakhiyeva. В этом тексте авторы говорят о интеграции умных устройств в университетах, чтобы улучшить процесс обучения студентов. Они интегрировали различные сенсоры на территории кампусов, а также со-здали облако для получения данных с них [16, 17].

Подтверждение этому можно найти и в текстах западных коллег, таким как - «IoT manager: An Open-Source IoT framework for smart cities» (L. Calde-roni, A. Magnani, D. Maio), в которой говорится о новом фреймворке для упрощения работы с большим (1000+) количеством подключенных устройств [18].

Этим использование устройств не ограничивается, и в работе «Fog computing and IoT for remote blood monitoring» (M. Orda-Zhigulina, D. Orda-Zhigulina) авторы рассказывают о возможностях применения интернета вещей в медицине, например, для создания интеллектуального непрерывного мониторинга глюкозы, который имеет возможность отправлять полученное

информации о состоянии крови, отправлять на сервер, чтобы потом пользователь мог получить полную информацию о состоянии своей крови [19].

Для изучения необходимых фреймворков для разработки были изучены официальные ресурсы по React.JS, Angular. Преимущества React.JS были выделены такие [20]:

– Virtual DOM повышает производительность высоконагруженных приложений, снижая вероятность перерисовки и улучшая пользо-вательский опыт.
– Использование изоморфного подхода позволяет производить рендеринг страниц быстрее.
– Повышенное переиспользование кода, можно использовать об-щий код для мобильного приложения и Web версии.
– Декларативное представление компонентов делает код более чи-таемым и предсказуемым.

У Angular они несколько отличаются [21]:

– Angular – это фреймворк, который предлагает свою архитектуру построения системы, в отличии от React, который предоставляет только некоторые табличные методы.
– Наличие CLI системы для генерации стандартных решений.
– Строгая типизация кода по умолчанию.
– Наличие Dependency Injection из коробки.

Минусы Angular:

– Посредственная документация.
– Большой объем результирующего кода.
– Высокий порог входа.

ЗАКЛЮЧЕНИЕ

В рамках выполнения НИР на основе анализа программ были выделены и проанализированы ведущие тренды: 1. Электронные IoT устройства, а также софт к ним, в Российской Федера-ции существуют и разрабатываются, но в значительно меньшем мас-штабе, чем на западе. 2. В странах ЕС и США IoT устройства получили более широкое распро-странение, начиная от медицинских умных датчиков до огромных си-стем, которые автоматизируют множество процессов в национальных парках. 3. Использование современных инструментов front-end и back-end разра-ботки позволят создать масштабируемую систему для контроля и управления разными объектами. Проведен анализ зарубежной (M. Stusek, K. Zeman, P. Masek, J. Hosek, J. Selova, K. Kim) и отечественной (Н.В. Рогачева, А.П. Карловский, В.Л. Можгинский, Ю.И. Иванов, К.В. Колоколова, А.Я. Номерчук, В.В. Соловьев, В.В. Щадрина, Д.Ю. Щербак, О.В. Гурин, В.П. Замышляев, Л.Е. Попок, И.А. Васюткина, Т.Н. Филимоненкова, А.Д. Григорьев) научной литературы и информационных источников (Официальные сайты Angular и React). Анализ ведущих трендов социально-экономического и технологическо-го развития показал, что проблема развития IoT в Российской Федерации яв-ляется актуальной и востребованной, так как ее решение улучшит уровень автоматизации различных процессов. Проведенный анализ зарубежных научных источников по теме иссле-дования «Исследование веб-технологий в стеке IoT» позволил выявить акту-альное состояние умных электронных устройств в Российской Федерации и в мире и варианты их развития. В ходе практики было полностью выполнено Индивидуальное задание.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Прудникова, А.А. Безопасность облачных вычислений / А.А. Прудникова // Мир телекома. – 2013. – №1. – С. 50-55.

2. Методические указания «Процедура системного анализа при проектировании программных систем» для студентов-дипломников дневной и заочной формы обучения специальности 7.091501 / Сост.: Сергеев Г.Г., Скатков А.В., Мащенко Е.Н. – Севастополь: Изд-во СевНТУ, 2005. – 32 с.

3. Методические указания к расчетно-графическому заданию на тему «Метод анализа иерархий» по дисциплине «Теория оптимальных решений» для студентов специальности 7.091501 «Компьютерные системы и сети» дневной и заочной формы обучения / Сост.: Ю.Н. Щепин – Севастополь: Изд-во СевНТУ, 2008. – 28 с.

4. Блюмин С.Л., Шуйкова И.А. Модели и методы принятия решений в условиях неопределенности. – Липецк: ЛЭГИ, 2001. – 138 с.

5. Hogan, M. NIST Cloud Computing Standarts Roadmap / M. Hogan, F. Liu, A. Sokol, J. Tong // NIST Special Publication 500-291, Version 2 Roadmap Working Group, 2013. – 113 с.

6. The 2016 Global Cloud Data Security Study. Ponemon Insitute LLC, 2016. – 40 с.

7. Беккер, М.Я. Информационная безопасность при облачных вычислениях: проблемы и перспективы / М.Я. Беккер, Ю.А. Гатчин, Н.С. Карманов-ский, А.О. Терентьев, Д.Ю. Федоров // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2011. – №1(71). – С. 97-102.

8. Емельянова, Ю.Г. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления / Ю.Г. Емельянова, В.П. Фраленко // Программные системы: теория и приложения. – 2011. – №4(8) – С. 17-31.

9. Chisnall, D. The Definitive Guide to the Xen Hypervisor / D. Chisnall. – 1st Edition // Prentice Hall Open Source Software Development, 2007. – 320 с.

10. Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» / Минкомсвязь России // Опубликован 12.02.2016 на официальном интернет-портале Министерства связи и массовых коммуникаций Российской Федерации

11. Облачные сервисы 2016 [Электронный ресурс] // CNews Analytics Режим доступа: https://goo.gl/cmDSMB (Дата обращения: 30.12.2016)

12. Cloud Security Alliance Releases 'The Treacherous Twelve' Cloud Computing Top Threats in 2016 [Электронный ресурс] // Cloud Security Alliance Research Group Режим доступа: https://goo.gl/l2aWLu (Дата обращения: 11.01.2017)

13. ИТ-инфраструктура предприятия 2010: Пути оптимизации [Электронный ресурс] // CNews Analytics Режим доступа: https://goo.gl/jzrrIO (Дата обращения: 05.01.2017)

14. Kaplan, J. Revolutionizing data center energy efficiency / J. Kaplan, W. Forrest, N. Kindler // Technical report, McKinsey & Company, 2008. – 15 с.

15. AWS signature version 1 is insecure [Электронный ресурс] // Daemonic Dispatches Режим доступа: https://goo.gl/70bggH (Дата обращения: 08.02.2017)

16. The CIS Critical Security Controls for Effective Cyber Defense [Электронный ресурс] // SANS website Режим доступа: https://goo.gl/pMjbNE (Дата обращения: 08.02.2017)

17. OWASP Top Ten Project [Электронный ресурс] // OWASP website Режим доступа: https://goo.gl/kSHOjF (Дата обращения: 08.02.2017)

18. CVE security vulnerability database. Security vulnerabilities, exploits, references and more [Электронный ресурс] // CVE Details. The ultimate security

vulnerability datasource Режим доступа: https://goo.gl/I3RtO2 (Дата обращения: 20.02.2017)

19. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel [Электронный ресурс] // CVE-2016-5195 info website Режим доступа: https://goo.gl/ziy3Nd (Дата обращения: 20.02.2017)

20. Bug 1355987 - (CVE-2016-6258, xsa182) CVE-2016-6258 xsa182 xen: x86: Privilege escalation in PV guests (XSA-182) [Электронный ресурс] // Red Hat Bugzilla Режим доступа: https://goo.gl/dlqtnR (Дата обращения: 20.02.2017)

21. CVE-2016-5696 [Электронный ресурс] // Common Vulnerabilities and Exposures. The Standart for Information Security Vulnerability Names Режим доступа: https://goo.gl/xYpFQQ (Дата обращения: 21.02.2017)

22. CVE-2016-5696 [Электронный ресурс] // Debian Security Bug Tracker Режим доступа: https://goo.gl/BXkTiL (Дата обращения: 21.02.2017)

23. CVE-2016-8655 - Red Hat Customer Portal [Электронный ресурс] // Red Hat Customer Portal Режим доступа: https://goo.gl/QhVbmm (Дата обращения: 21.02.2017)

24. CVE-2016-4997 [Электронный ресурс] // Common Vulnerabilities and Exposures. The Standart for Information Security Vulnerability Names Режим доступа: https://goo.gl/dbtXny (Дата обращения: 21.02.2017)

25. CVE-2016-4484: Cryptsetup Initrd root Shell [Электронный ресурс] // Hector Marco Gisbert - Lecturer and Cyber Security Researcher website Режим доступа: https://goo.gl/Jrfg6H (Дата обращения: 22.02.2017)

26. CVE-2016-1583 [Электронный ресурс] // Debian Security Bug Tracker Режим доступа: https://goo.gl/PIdqGR (Дата обращения: 22.02.2017)

27. gbonacini/CVE-2016-5195: A CVE-2016-5195 exploit example. [Электронный ресурс] // GitHub Режим доступа: https://goo.gl/9tFhHh (Дата обращения: 24.02.2017)