Научная статья
УДК 346.26:004.738.5
https://doi.org/10.24143/2073-5537-2025-2-27-33
EDN CQZMCS

Будущее интернета вещей: угрозы, проблемы и перспективы

Елена Михайловна Кобозева*✉, *Дарья Владимировна Берсенева

Краснодарский филиал ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Краснодар, Россия, alena.cobozeva@yandex.ru✉

Аннотация. Рассматривается использование технологии интернета вещей (IoT) в современных условиях. В связи со стремительным развитием этой технологии, ее интеграцией в повседневную жизнь возникают не только новые фундаментальные возможности, но и серьезные вызовы и проблемы. Выявлены основные угрозы для IoT, проблемы и перспективы дальнейшего его использования, отмечена важность понимания современных вызовов и возможностей для специалистов в области технологий, бизнеса, медицины и других сфер. В результате проведенного анализа технологии IoT определены потенциальные угрозы, с которыми связано использование интернета вещей, даны их характеристики. Выделены проблемы в обеспечении безопасности IoT. Анализ объемов и тенденций развития рынка IoT позволил установить, что с 2020 по 2024 г. наблюдался последовательный рост количества подключений и выручки. Зафиксирован наибольший рост применения IoT в энергетике/ЖКХ – 32 %, недвижимости – 24 %, промышленности – 13 %, транспорте – 12 %. Отмечено, что применение IoT в настоящее время не только трансформирует различные отрасли, но и выступает мощным двигателем экономического и инновационного роста, создавая совершенно новые рынки, бизнес-модели и возможности для предпринимательства. Рассмотрены перспективы распространения IoT, раскрывающие будущее IoT, являющегося активно модернизирующейся технологией цифровой экономики России. Выделены тенденции развития и совершенствования IoT, обеспечивающие преодоление выявленных проблем и угроз, позволяющие IoT укрепить свои позиции как драйверу устойчивого экономического роста страны.

Ключевые слова: интернет вещей (IoT), цифровая трансформация, кибератака, устройства, экономика, проблемы IoT, искусственный интеллект, «умный» город, мониторинг, технологии, межмашинное взаимодействие, угрозы IoT, кибербезопасность

Для цитирования: *Кобозева Е. М., Берсенева Д. В.* Будущее интернета вещей: угрозы, проблемы и перспективы // Вестник Астраханского государственного технического университета. Серия: Экономика. 2025. № 2. С. 27–33. https://doi.org/10.24143/2073-5537-2025-2-27-33. EDN CQZMCS.

Original article

The future of the internet of things: threats, problems and prospects

Elena M. Kobozeva*✉, *Daria V. Berseneva

Krasnodar branch FSFEI HE "Financial University under the Government of the Russian Federation", Krasnodar, Russia, alena.cobozeva@yandex.ru✉

Abstract. The use of internet of things (IoT) technology in modern conditions is considered. Due to the rapid development of this technology and its integration into everyday life, not only new fundamental opportunities arise, but also serious challenges and problems. The main threats to the IoT, problems and prospects for its further use are identified, and the importance of understanding modern challenges and opportunities for specialists in technology, business, medicine and other fields is noted. As a result of the analysis of the IoT technology, potential threats associated with the use of the IoT have been identified and their characteristics have been given. The problems in ensuring IoT security are highlighted. An analysis of the volume and trends of the IoT market has revealed that from 2020 to 2024, there was a consistent increase in the number of connections and revenue. The largest growth in the use of the IoTwas recorded in the energy/housing sector – 32%, real estate – 24%, industry – 13%, transport – 12%. It is noted that the use of IoT is currently not only transforming various industries, but also acting as a powerful engine of economic and innovative growth, creating completely new markets, business models and opportunities for entrepreneurship. The prospects for the development of IoT are considered, revealing the future of the IoT, which is an actively developing technology of the digital economy of Russia. The trends in the development and improvement of the IoT are highlighted, en-

suring overcoming the identified problems and threats, allowing IoT to strengthen its position as a driver of the country's economic development.

Keywords: internet of things (IoT), digital transformation, cyberattack, devices, economy, IoT problems, artificial intelligence, smart city, monitoring, technologies, machine-to-machine interaction, IoT threats, cybersecurity

For citation: Kobozeva E. M., Berseneva D. V. The future of the internet of things: threats, problems and prospects. *Vestnik of Astrakhan State Technical University. Series: Economics*. 2025;2:27-33. (In Russ.). https://doi.org/10.24143/2073-5537-2025-2-27-33. EDN CQZMCS.

Введение

Многие годы мир стремительно меняется, в том числе и за счет интернета вещей (IoT), использование технологии которого становится все более актуальным. Сегодня интернет вещей представляет собой одну из самых значительных технологических революций нашего времени. Подключенные устройства и уникальные технологии, которые их поддерживают, создают новые возможности, трансформируют существующие процессы во множестве отраслей и преобразуют для нас способ взаимодействия с окружающим миром. С каждым годом количество подключенных устройств растет, охватывая все новые сферы жизни – от «умных» домов и транспортных систем до медицинских приборов и промышленных решений. Эти устройства, оснащенные датчиками и интеллектуальными алгоритмами, собирают и анализируют данные, позволяя принимать более обоснованные решения и оптимизировать процессы.

Однако наряду с перспективой все более широкого применения IoT возникают не только новые фундаментальные возможности, но и серьезные вызовы и проблемы. Понимание этих вызовов и возможностей критически важно для специалистов в области технологий, бизнеса, медицины и других сфер [1].

Методология исследования

Цель исследования заключается в рассмотрении текущего состояния и будущего интернета вещей с акцентом на выявление ключевых угроз, проблем и перспектив данного направления. В работе используются абстрактно-логический и монографический методы исследования, которые позволили объективно оценить настоящее и спрогнозировать будущее IoT.

В работе применялись данные исследования Ассоциации интернета вещей и агентства Onside. Анализируемый период охватывает промежуток времени с 2020 по 2024 г., для прогнозирования развития IoT использовалась динамика до 2027 г.

Определение потенциальных угроз и мер безопасности

Результаты проведенного исследования определили, что по мере роста цифровизации, внедрения новых технологий повышается и подверженность подключенных устройств кибератакам. При таких темпах к 2025 г. ущерб от кибератак будет составлять около 10,5 трлн долл. в год во всем мире, для сравнения – в 2015 г. эта сумма составляла на 300 % меньше [2].

Рассмотрим основные потенциальные угрозы, с которыми связано использование IoT, и их характеристики в таблице.

Характеристика возможных угроз от применения IoT*

Characteristics of possible threats from the use of IoT

Угроза	Характеристика
Взлом устройств	Из-за легкого доступа к устройствам IoT они подвержены взлому и атакам, что ведет к утрате конфиденциальности
Эксплойт	Угрозу трудно обнаружить. Многие устройства имеют ограниченный механизм защиты и могут подвергаться удаленному управлению третьими лицами. Эти уязвимости могут быть использованы с целью доступа к системе
Вредоносное ПО	Установка вирусов, в том числе и троянской вирусной программы, а также шпионского ПО, может привести к несанкционированному доступу к личной информации, манипуляциям с устройствами, отключению системы безопасности и возможности атак на другие связанные устройства
MitM-атака	Перехват и модификация данных, передаваемых между устройствами. Атака подслушивания, которая позволяет не только наблюдать за конфиденциальной информацией, но и манипулировать коммуникацией, например при отправлении неправильных команд устройствам
Программы-вымогатели	Заражение IoT-устройства, блокировка и потеря доступа к нему и критически важным функциям и данным ввиду требования денежных средств. Целью могут стать камеры видеонаблюдения, умные домашние системы, промышленные контроллеры и др.

Окончание таблицы

Ending of the table

Угроза	Характеристика
DDoS-атака	Атака заключается в использовании большого количества устройств IoT для создания ботнета, который будет запрашивать ресурсы целевого сервера или сети, перегружая их и делая недоступными для пользователя. Приводит к остановке в работе сервисов, финансовым убыткам, ухудшению репутации компании

* Составлено по [3].

Для обеспечения безопасности использования интернета вещей необходимо принимать ряд мер, но не всегда это бывает возможно ввиду определенных проблем [3].

Основные проблемы системы IoT:

1. Трудности в поддержке защищенности на этапе обновления устройств. Не всегда устройства имеют вычислительные ресурсы для реализации сложных и надежных механизмов обновления, а при установке обновлений довольно трудно обеспечить безопасность, т. к. особенности интерфейса пользователя не дают возможности производить обновления привычным методом.

2. Отсутствие законодательных актов и стандартов. С ростом числа подключенных устройств и влияния их на повседневную жизнь возрастает и необходимость в регуляции действий.

3. Трудности в интеграции с системами безопасности. Разнообразие устройств и платформ IoT создает сложную экосистему, в которой различные протоколы и стандарты могут конфликтовать друг с другом. Также иногда отсутствует централизованное управление и мониторинг, усложняя обнаружение и реагирование на угрозы.

4. Необходимость в масштабируемости. В связи с большим числом подключенных устройств возникает и необходимость в масштабируемых решениях для обработки и хранения данных. Компаниям следует более эффективно разрабатывать системы для управления большими объемами информации, что будет способствовать быстрой и надежной обработке данных.

5. Нехватка опытных специалистов. Многие компании испытывают недостаток квалифицированных кадров, обладающих необходимыми навыками в программировании, анализе данных, сетевых технологиях и безопасности. Дефицит и нехватка грамотного подхода приводят к затруднению в управлении новыми проектами и внедрении новых технологий.

6. Трудности с обеспечением защиты ПО. Вследствие роста объемов производимых продуктов и решений в области IoT разработчики зачастую не уделяют должного внимания системе безопасности и конфиденциальности на этапе проектирования ввиду различных причин (например, предпочитая безопасности функциональную составляющую устройств, минимизацию себестоимости или сокращение времени разработки).

7. Энергетическая эффективность. Часть IoT-устройств работает на батареях и, соответственно, зависит от источников питания. Разработка энергоэффективных решений и технологий, таких как энергосберегающие протоколы связи и альтернативные источники энергии, является ключевым направлением для повышения жизнеспособности IoT. Аспект энергетической эффективности в данном случае является перспективой развития IoT и шагом на пути к росту всего направления.

Анализ объемов и тенденций развития рынка

В исследовании Ассоциации интернета вещей и агентства Onside говорится о том, что за 2024 г. объем рынка интернета вещей в России составил 181 млрд руб. В соотношении с предыдущим годом, когда объем составлял 158 млрд руб., прирост был отмечен на 15 %.

К концу 2024 г. в России было использовано примерно 102,3 млн различных (неносимых) устройств IoT. Показатель увеличился на 19 % в соотношении с прошлым годом [4].

Рассматривая динамику межмашинного взаимодействия (M2M) и его надмножества – интернета вещей в период 2020–2024 гг., необходимо отметить, что к 2024 г. явно прослеживается тенденция к росту как выручки (181 млрд руб.), так и количества подключений. Прогнозные значения на будущие годы (2025–2027 гг.) также ожидаемо увеличиваются и являются высокими. Так, к 2027 г. предполагается рост количества подключений до 140 млн, а рост выручки – до 230 млрд руб. (рис. 1).

Анализируя тенденции рынка IoT в России, можно сделать вывод о том, что такой рост обусловлен увеличением количества подключения различных устройств, совершенствованием технологий и применением IoT-решений в различных отраслях деятельности, включая промышленность, здравоохранение, транспорт, умные города.

Рассмотрим на примере 2023 г. структуру рынка IoT и межмашинного взаимодействия по отраслям и процентные доли, приходящиеся на основные отрасли (рис. 2).

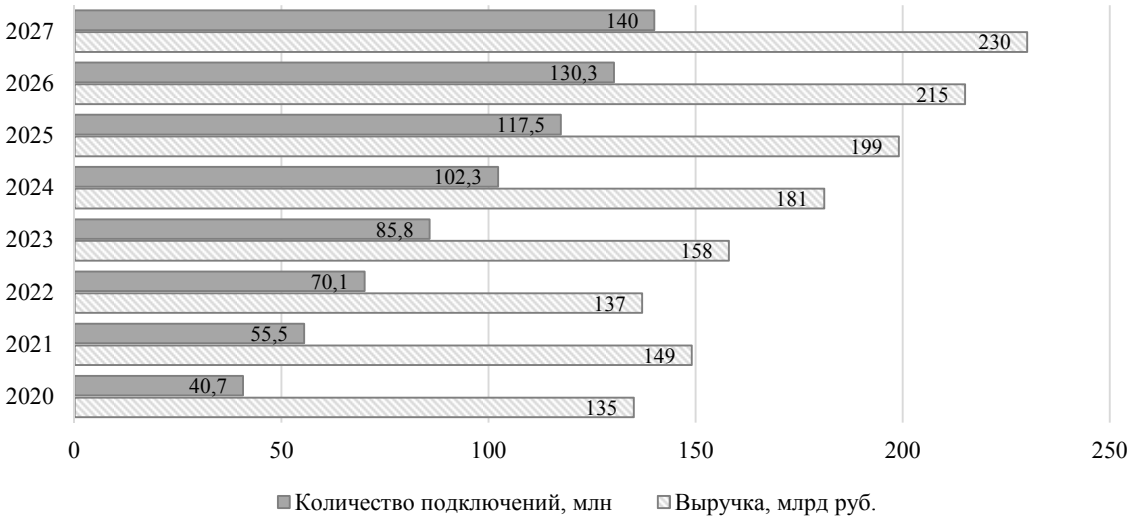

Рис. 1. Динамика рынка IoT/M2M в России в период с 2020 по 2027 г.

Fig. 1. Dynamics of the IoT/M2M market in Russia in the period from 2020 to 2027

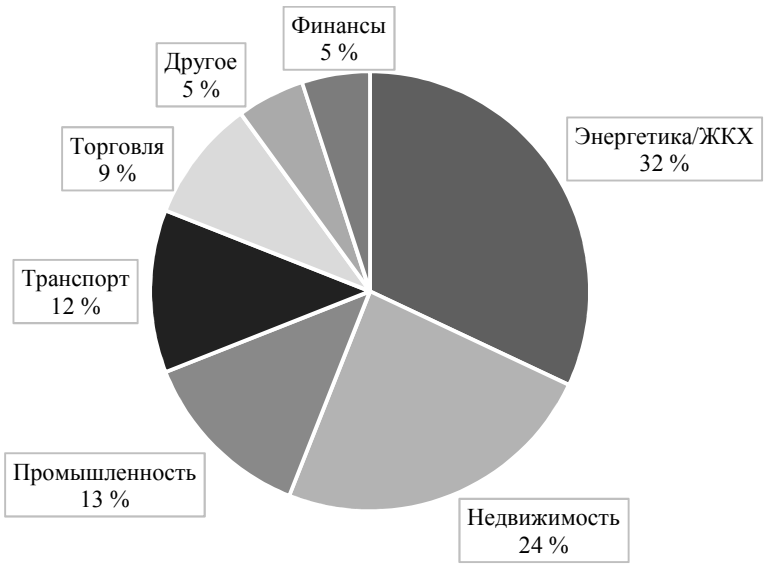

Рис. 2. Структура рынка IoT/M2M в России в 2023 г.

Fig. 2. Structure of the IoT/M2M market in Russia in 2023

Стоит отметить, что больше половины всего рынка приходится на энергетику, т. к. в этой области наблюдается необходимость оптимизировать потребление ресурсов и внедрять интеллектуальные системы управления энергоснабжением и мониторинга, умные счетчики. Эта отрасль в прогнозе покажет рост благодаря цифровой трансформации и оптимизации расходов [5]. Меньшую долю занимает сфера финансов. Традиционно финансовый сектор полагается на проверенные методы, обеспечивающие безопасность и защиту данных, поэтому внедрение IoT-технологий требует соответствия нормам и регламенту, а также значительных инвестиций в кибербезопасность [6].

Одной из ключевых дальнейших перспектив IoT является автоматизация и оптимизация бизнес-процессов. Многие компании уже используют сенсоры для мониторинга состояния оборудования, управления запасами и анализа данных о потреблении ресурсов. В результате это позволяет сократить затраты, повысить эффективность и улучшить качество обслуживания клиентов [7]. Так, например, в промышленности применение IoT-систем позволяет предсказывать поломки оборудования,

что способствует экономии времени и средств на ремонт.

Развитие «умных» городов можно назвать одной из самых перспективных областей применения интернета вещей. С помощью подключенных устройств можно улучшить управление транспортом, энергоснабжением, безопасностью и здравоохранением. Например, интеллектуальные системы управления светофорами могут оптимизировать движение и снизить скопление транспортных средств. Умные датчики могут следить за состоянием инфраструктуры, позволяя своевременно проводить ремонтные работы и облагораживать территорию города [8].

Министерство строительства и жилищно-коммунального хозяйства Российской Федерации запустило проект «Умный город» и оценку с помощью индекса «IQ городов», которые показывают, насколько эффективно в городскую среду внедряются цифровые технологии, при этом затрагивая сферы транспорта, туризма, городского управления и др. Среди лидеров «умных» городов можно отметить Тюмень. В городе был запущен проект Smart City, охватывающий более 50 направлений [9]. В решениях проекта отмечены система дистанционного съема показаний приборов учета, система мониторинга климата в офисном помещении, адаптивный светофор, система вывоза мусора по потребности. В городе установлено видеонаблюдение на дорогах и тротуарах, призванное обеспечивать безопасность, контролировать и регулировать трафик. Для удобства пользования общественным транспортом жители могут посмотреть необходимую информацию, маршруты, прогнозное время прибытия транспорта с помощью приложения «Тюмень.Транспорт».

В Екатеринбурге на данный момент действуют системы распознавания автомобильных номеров, сервис автоматизированного мониторинга ЖКХ, программно-аппаратный комплекс эффективного мониторинга и управления муниципальными и коммерческими парковками города. Данный комплекс позволяет повысить безопасность дорожного движения и уровень удобства в доступе к объектам города [10]. Для использования общественного транспорта в городе стали появляться «умные» остановки, электронное табло позволяет узнать действующее расписание, маршруты, посмотреть карту города и ближайшие объекты, а также подключиться к Wi-Fi или зарядить электронные устройства.

Сфера здравоохранения в стране также получит значительную выгоду от внедрения IoT-решений. Использование в здравоохранении «умных» медицинских устройств позволит более эффективно проводить диагностику, мониторинг и профилактику заболеваний, что позволит врачам оперативно реагировать на изменения в состоянии здоровья пациентов [11].

Следует отметить, что применение IoT не только трансформирует различные отрасли, но и выступает мощным двигателем экономического и инновационного роста, создавая совершенно новые рынки, бизнес-модели и возможности для предпринимательства [12].

Выделим основные тенденции развития и совершенствования IoT и проанализируем их.

1. Совместимость устройств. Разнообразие стандартов и протоколов в IoT создает трудности совместимости межу устройствами разных производителей. Но будущие разработки по стандартизации и облегчению интеграции позволят улучшить взаимодействие между устройствами.

2. Повышение уровня безопасности. Будущее IoT будет сосредоточено на разработке более надежных систем безопасности, включая шифрование данных, аутентификацию пользователей и регулярные обновления ПО. Компании, в свою очередь, будут инвестировать в защиту своих устройств и данных, чтобы предотвратить утечки и атаки [13].

3. Интеграция с искусственным интеллектом. Сочетание IoT и искусственного интеллекта откроет новые горизонты для автоматизации и интеллектуального анализа данных. Искусственный интеллект сможет обрабатывать и осуществлять анализ больших объемов данных, предоставляемых IoT-устройствами, что создаст оптимальные условия для принятия более эффективных решений в режиме реального времени [14]. Так, например, в здравоохранении использование искусственным интеллектом данных от носимых устройств позволит предсказать обострения заболеваний и предложить индивидуальные рекомендации.

Заключение

Таким образом, IoT выступает важной технологией, которая будет способствовать развитию конкурентоспособности экономики России. Однако будущее интернета вещей характеризуется как перспективами и трудностями, так и угрозами. Преодоление возникающих проблем, таких как безопасность, стандартизация, управление данными, отсутствие законодательных актов и стандартов, а также угроз (взлома устройств, кибератак, вредоносных ПО) откроет новый уровень применения IoT в различных сферах. При правильном подходе технологии IoT могут значительно изменить жизнь к лучшему, предоставляя новые решения и улучшая качество услуг. В перспективе можно отметить автоматизацию и оптимизацию бизнес-процессов в таких отраслях, как здравоохранение, транспорт, производство и «умные» города, возможность интеграции с другими устройствами и влияние на устойчивое развитие инфраструктуры.

В современных условиях цифровизации экономики и новой геополитической реальности особое значение приобретают повышение производитель-

ности труда и более эффективное расходование ресурсов, чему активно способствует применение технологии интернета вещей. Дальнейшее развитие IoT будет зависеть от способности общества адаптироваться к новым технологиям и использовать их во благо.

Список источников

1. Taranova I. V., Podkolzina I. M., Prokhorova V. V., Kolomyts O. N., Kobozeva E. M. Global financial and economic crisis in Russia: trends and prospects // Research Journal of Pharmaceutical, Biological and Chemical Sciences. 2018. Т. 9. № 6. С. 769–775.

2. Morgan S. Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics // Cybercrime. 2022. P. 34.

3. Верещагина Е. А., Капецкий И. О., Ярмонов А. С. Проблемы безопасности Интернета вещей. М.: Мир науки, 2021. С. 26–32.

4. Интернет вещей, IoT, M2M. Рынок России. URL: https://www.tadviser.ru/index.php/Статья:Интернет_вещей,_IoT_(рынок_России) (дата обращения: 15.12.2024).

5. «Интернет вещей» в электроэнергетике. Применение и перспективы. URL: https://www.elec.ru/publications/tsifrovye-tekhnologii-svjaz-izmerenija/6157/ (дата обращения: 15.12.2024).

6. Интернет вещей в банкинге. URL: https://trends.rbc.ru/trends/industry/65279f2b9a7947713307b739 (дата обращения: 15.12.2024).

7. Кобозева Е. М. Информационная среда в АПК региона // Экономика сельского хоз-ва России. 2018. № 6. С. 24–29.

8. Что такое интернет вещей Internet of Things, IoT. Терминология, применение и развитие технологии. URL: https://www.tadviser.ru/index.php/Статья:Что_такое_интернет_вещей_(Internet_of_Things,_IoT) (дата обращения: 15.12.2024).

9. Тюмень. «Умный город». URL: https://smartcity.tyuiu.ru/ (дата обращения: 17.12.2024).

10. Информатизация города Екатеринбурга. URL: https://xn--80aaucbcxhjuyt8a2j.xn--80acgfbsl1azdqr.xn (дата обращения: 17.12.2024).

11. Перспективы развития интернета вещей: безопасность, экология и другие тренды. URL: https://www.arsis.ru/blog/iot (дата обращения: 17.12.2024).

12. Prokhorova V. V., Kobozeva E. M., Kolomyts O. N., Gurnovich T. G., Mokrushin A. A. Entrepreneurial Ecosystem: Strategies and Prospects // The Challenge of Sustainability in Agricultural Systems. Lecture Notes in Networks and Systems. 2021. V. 206. P. 247–258.

13. Molchan A. S., Osadchuk L. M., Anichkina O. A., Ponomarev S. V., Kuzmenko N. I. The “digitalisation trap” of Russian regions // International Journal of Technology, Policy and Management. 2023. V. 23. N. 1. P. 20.

14. Salikov Y. A., Magomaeva L. R., Sozaeva D. A., Molchan A. S., Il′ina T. V. Cognitive Technologies in the Regional Economic Security Management // Business 4.0 as a Subject of the Digital Economy. Cham: Springer, 2022. P. 251–256.

References

1. Taranova I. V., Podkolzina I. M., Prokhorova V. V., Kolomyts O. N., Kobozeva E. M. Global financial and economic crisis in Russia: trends and prospects. *Research Journal of Pharmaceutical, Biological and Chemical Sciences,* 2018, vol. 9, no. 6, pp. 769-775.

2. Morgan S. Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. *Cybercrime,* 2022, p. 34.

3. Vereshchagina E. A., Kapetskii I. O., Iarmonov A. S. *Problemy bezopasnosti Interneta veshchei* [Internet of Things Security Issues]. Moscow, Mir nauki Publ., 2021. Pp. 26-32.

4. *Internet veshchei, IoT, M2M. Rynok Rossii* [The Russian market]. Available at: https://www.tadviser.ru/index.php/Stat'ia:Internet_veshchei,_IoT_(rynok_Rossii) (accessed: 15.12.2024).

5. *«Internet veshchei» v elektroenergetike. Primenenie i perspektivy* [“The internet of things” in the electric power industry. Application and prospects]. Available at: https://www.elec.ru/publications/tsifrovye-tekhnologii-svjaz-izmerenija/6157/ (accessed: 15.12.2024).

6. *Internet veshchei v bankinge* [The Internet of Things in banking]. Available at: https://trends.rbc.ru/trends/industry/65279f2b9a7947713307b739 (accessed: 15.12.2024).

7. Kobozeva E. M. Informatsionnaia sreda v APK regiona [Information environment in the agro-industrial complex of the region]. *Ekonomika sel'skogo khoziaistva Rossii,* 2018, no. 6, pp. 24-29.

8. *Chto takoe internet veshchei Internet of Things, IoT. Terminologiia, primenenie i razvitie tekhnologii* [What is the Internet of Things (IoT)? Terminology, application and development of technology]. Available at: https://www.tadviser.ru/index.php/Stat'ia:Chto_takoe_internet_veshchei_(Internet_of_Things,_IoT) (accessed: 15.12.2024).

9. *Tiumen'. «Umnyi gorod»* [Tyumen. Smart City]. Available at: https://smartcity.tyuiu.ru/ (accessed: 17.12.2024).

10. *Informatizatsiia goroda Ekaterinburga* [Informatization of the city of Yekaterinburg]. Available at: https://xn--80aaucbcxhjuyt8a2j.xn--80acgfbsl1azdqr.xn (accessed: 17.12.2024).

11. *Perspektivy razvitiia interneta veshchei: bezopasnost', ekologiia i drugie trendy* [Prospects for the development of the Internet of Things: security, ecology and other trends]. Available at: https://www.arsis.ru/blog/iot (accessed: 17.12.2024).

12. Prokhorova V. V., Kobozeva E. M., Kolomyts O. N., Gurnovich T. G., Mokrushin A. A. Entrepreneurial Ecosystem: Strategies and Prospects. The Challenge of Sustainability in Agricultural Systems. *Lecture Notes in Networks and Systems,* 2021, vol. 206, pp. 247-258.

13. Molchan A. S., Osadchuk L. M., Anichkina O. A., Ponomarev S. V., Kuzmenko N. I. The “digitalisation trap” of Russian regions. *International Journal of Technology, Policy and Management,* 2023, vol. 23, no. 1, p. 20.

14. Salikov Y. A., Magomaeva L. R., Sozaeva D. A., Molchan A. S., Il′ina T. V. Cognitive Technologies in the Regional Economic Security Management. *Business 4.0 as a Subject of the Digital Economy*. Cham, Springer, 2022. Pp. 251-256.

Статья поступила в редакцию 21.01.2025; одобрена после рецензирования 19.03.2025; принята к публикации 15.05.2025
The article was submitted 21.01.2025; approved after reviewing 19.03.2025; accepted for publication 15.05.2025

Информация об авторах / Information about the authors

Елена Михайловна Кобозева – кандидат экономических наук, доцент; доцент кафедры математики и информатики; Краснодарский филиал ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»; alena.cobozeva@yandex.ru

Дарья Владимировна Берсенева – магистрант кафедры математики и информатики; Краснодарский филиал ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»; dariavl@internet.ru

Elena M. Kobozeva – Candidate of Economic Sciences, Assistant Professor; Assistant Professor of the Department of Mathematics and Computer Science; Krasnodar branch FSFEI HE “Financial University under the Government of the Russian Federation”; alena.cobozeva@yandex.ru

Daria V. Berseneva – Master’s Course Student of the Department of Mathematics and Computer Science; Krasnodar branch FSFEI HE “Financial University under the Government of the Russian Federation”; dariavl@internet.ru