Методы определения надёжности и подлинности для устройств интернета вещей

Пан Бо, Е.С. Абрамов

Южный федеральный университет, Ростов-на-Дону

Аннотация: В статье представлен систематический обзор методов обеспечения надёжности и подлинности устройств в экосистеме Интернета вещей (IoT). Анализируются ключевые уязвимости, архитектурные особенности и ресурсные ограничения IoT-систем, определяющие выбор механизмов защиты. Рассмотрены криптографические решения, модели динамического доверия, подходы к контролю доступа, а также протоколы аутентификации для промышленных и распределённых сред. На основе сравнительного анализа методов выявлены актуальные исследовательские пробелы и определены перспективные направления разработки комплексных, адаптивных систем безопасности для гетерогенных IoT-инфраструктур.
Ключевые слова: система Интернет вещей, безопасность, надёжность, подлинность, устройства, методы.

Введение

Концепция Интернета вещей (Internet of Things, IoT), впервые представленная Кевином Эштоном в 1999 году [1], за два десятилетия эволюционировала от идеи до одной из ключевых технологических парадигм, трансформирующих современное общество. Интеграция физических объектов, оснащённых сенсорами, средствами связи и вычислительными возможностями, в единую информационную сеть позволила создать основу для «умных» решений в здравоохранении, транспортных системах, управлении городской инфраструктурой, сельском хозяйстве и промышленности [2, 3]. Ядро данной парадигмы составляет сложное взаимодействие распределённых вычислительных систем, включающих сенсорные устройства, шлюзы и облачные платформы, что обеспечивает непрерывный сбор, передачу и анализ данных для автономного принятия решений [4].

Однако стремительная экспансия IoT сопряжена с критически важными вызовами в области кибербезопасности. Масштабное внедрение разнородных, зачастую ресурсоограниченных устройств в критически важные инфраструктуры значительно расширяет поверхность для

потенциальных атак [5]. К характерным угрозам относятся подмена устройств (spoofing), несанкционированный доступ, перехват и модификация данных, а также внедрение вредоносного ПО. Ресурсные ограничения многих IoT-устройств (низкая вычислительная мощность, ограниченная энергоёмкость) затрудняют применение традиционных, ресурсоёмких криптографических методов защиты [6]. Кроме того, децентрализованная и гетерогенная природа IoT-сетей осложняет обеспечение совместимости и единого уровня безопасности, предоставляемого различными производителями [7].

В этом контексте традиционные механизмы безопасности, сфокусированные преимущественно на криптографии и контроле доступа, оказываются недостаточными для противодействия ряду угроз, особенно исходящих от скомпрометированных легитимных узлов сети [8]. Вследствие этого актуальной исследовательской задачей становится разработка и интеграция дополнительных механизмов, основанных на оценке надёжности (trust) и подлинности (authenticity) участников сети. Эти механизмы позволяют динамически оценивать поведение узлов, изолировать потенциально вредоносные элементы и формировать доверительные отношения между устройствами в условиях неполной информации и отсутствия централизованного управления [9, 10]. Методы оценки доверия часто используют историю взаимодействий и рекомендательные системы, адаптированные для IoT-среды, которые анализируют как прямые наблюдения, так и косвенные отзывы от других узлов [11].

Таким образом, проблема обеспечения безопасности IoT носит комплексный характер, требуя сочетания криптографических методов, протоколов аутентификации и динамических моделей доверия. Несмотря на обширный объём публикаций, посвящённых отдельным аспектам безопасности IoT, ощущается потребность в систематизированном анализе, который бы позволил сопоставить различные подходы к обеспечению

надёжности и подлинности, выявить их синергию, ограничения и перспективные направления интеграции.

Целью данной статьи является проведение систематического литературного обзора (Systematic Literature Review, SLR) современных методов и протоколов, направленных на определение и обеспечение надёжности и подлинности устройств в системах Интернета вещей. В работе последовательно рассматриваются:

1. Ключевые требования и угрозы безопасности в контексте IoT.
2. Архитектурные особенности IoT, влияющие на выбор механизмов защиты.
3. Существующие криптографические и протокольные решения для аутентификации.
4. Модели и методы оценки доверия, адаптированные для распределённых IoT-сетей.
5. Анализ интеграции рассмотренных подходов и выявление актуальных исследовательских пробелов.

Проведённый анализ позволит структурировать существующие знания в данной области и сформулировать чёткие направления для будущих исследований, нацеленных на создание комплексных и эффективных систем безопасности для гетерогенных и масштабируемых IoT-инфраструктур.

Беспроводные сенсорные сети (Wireless Sensor Networks, WSN)

Беспроводные сенсорные сети (WSN), как ключевой элемент IoT, представляют собой сети из энергоограниченных автономных устройств для мониторинга среды и передачи данных на центральный узел [16]. Они делятся на неструктурированные (случайное размещение) и структурированные (плановое размещение). Для принятия решений в IoT критически важна достоверность данных, что обеспечивается отслеживанием их происхождения (provenance) для проверки целостности и подлинности

[17]. Однако сама эта проверка требует безопасного источника. Исследование Zafar et al. [18] анализирует схемы доверия через безопасное происхождение, предлагает их таксономию и выделяет перспективные направления, такие как управление доступом и оптимизация хранения.

Мобильные одноранговые сети (Mobile Ad Hoc Network, MANET)

Исследование Sikari et al. [19] анализирует открытый подход к построению IoT-систем, фокусируясь на интеграции технологий связи в промежуточное ПО (middleware) для решения проблем безопасности и правового статуса мобильных устройств. Авторы рассматривают ключевые параметры безопасности (целостность, конфиденциальность, аутентификацию, контроль доступа) и аспекты доверия, однако их работа содержит неопределённую таксономию IoT и отсутствие чёткой классификации алгоритмов [19].

В свою очередь, Ali et al. [20] предлагают практическое решение – облегчённый модуль безопасности Linux (LSM) для удалённой аттестации статического и динамического поведения IoT-приложений, тестируя его с помощью инструмента WEKA. Для защиты конфиденциальности и снижения сетевой нагрузки используются методы вроде регистров конфигурации платформы (PCR) [20].

В контексте моделирования доверия в сложной IoT-среде G. Køien [21] применяет субъективную логику TNA-SL для анализа динамических взаимодействий между человеком и устройством, исследуя такие аспекты, как транзитивность, риск, репутация и конфиденциальность, и отмечая проблему определения оптимальной частоты доверительных взаимодействий [21].

Облачные технологии

Облачные технологии, определяемые как пулы легко доступных виртуализированных ресурсов [22], предоставляют масштабируемые сервисы

по модели pay-as-you-go с гарантиями SLA [23]. Их ключевые черты – оплата по использованию, неограниченный ресурсный потенциал, самообслуживание и виртуализация [23, 24].

Для интеграции с IoT была предложена концепция «Облака вещей» (CoT), виртуализирующая физические устройства в облаке [25]. Для решения проблемы надёжности в CoT-средах Fortino et al. разработали алгоритм CoTAG, основанный на взаимном доверии (репутация, полезность) и голосовании для выявления ненадёжных узлов [25]. Для повышения эффективности принятия решений алгоритм был дополнен методами анализа больших данных.

Контроль доступа

В IoT контроль доступа обеспечивает санкционированное взаимодействие пользователей и устройств, исключая несанкционированное вмешательство. При его разработке критически важны делегирование, масштабируемость и безопасность, так как управление доступом напрямую влияет на доверие пользователей [26]. Например, Alcaide et al. разделяют участников на владельцев и сборщиков данных, где доступ предоставляется после строгой аутентификации [27].

Sfar et al. предложили когнитивный и системный подход к безопасности IoT, позволяющий устройствам автономно воспринимать угрозы [28]. Авторы выделили три ключевых направления: эффективная безопасность для малых устройств, адаптивная контекстно-зависимая защита и усиление значимости безопасности через когнитивные системы [28].

Управление доверием, определяемое как унифицированный подход к авторизации на основе политик и учётных данных [30, 31], является основой для оценки надёжности транзакций, где доверие обеспечивается криптографическими удостоверениями, а не фактической идентичностью [29]. Практическим инструментом является набор SecKit от Kounelis et al. для

управления безопасным взаимодействием, хотя он не оценивает параметры надёжности и аутентичности [32].

Перспективным направлением является применение квантово-криптографических методов для качественного повышения защиты данных в IoT [33].

Методология

В настоящей работе применяется методология систематического литературного обзора (Systematic Literature Review, SLR). Её цель – критическая оценка и обобщение существующих исследований по заданной теме на основе чётких критериев поиска и отбора литературы. Данный подход минимизирует предвзятость, повышает достоверность выводов и позволяет выявить пробелы в знаниях, формируя надёжную основу для дальнейших изысканий [34]. Изначально разработанный для медицины, метод SLR в последние годы активно адаптируется для исследований в области социальных наук и инженерных дисциплин.

Безопасность Интернета вещей

В контексте Интернета вещей **безопасность** определяется как свойство системы, обеспечивающее защиту от несанкционированного доступа, модификации данных и иных вредоносных воздействий [35, 36]. Эффективное функционирование IoT-систем требует реализации фундаментальных принципов безопасности, которые визуализированы на рис. 1 и включают:

– Конфиденциальность: доступ к данным имеют только авторизованные субъекты.

– Целостность: гарантия неизменности и достоверности данных.

– Доступность: обеспечение доступа к данным и сервисам в требуемое время.

– Подлинность: возможность подтверждения идентичности компонентов системы.

– Надёжность: наличие достоверного пути аудита операций.

– Приватность: защита персональных данных пользователя от несанкционированного доступа со стороны сервисов.

Рис. 1. Требования к безопасности Интернета вещей

Основными вызовами безопасности в IoT являются конфиденциальность данных (риски из-за слабой аутентификации, небезопасных интерфейсов), секретность (угрозы, связанные с незаконным профилированием и обработкой) и доверие (проблемы, вызванные вредоносным ПО, атаками на доступность и сложностью верификации).

Для реализации защиты необходимо безопасное сетевое соединение, основанное на взаимной аутентификации устройств и сети, использовании криптографических ключей и идентификаторов. Это позволяет минимизировать риски клонирования устройств, подмены и масштабных атак.

Архитектура IoT, такая как модель ITU-T Y.2060 [37] (Рис. 2), определяет ключевые компоненты и их взаимодействие. Важнейшим элементом является защищённый канал связи с обязательным использованием шифрования и аутентификации.

Для ресурсоограниченных IoT-устройств эффективны современные криптографические методы, например, ECC (Elliptic Curve Cryptography), обеспечивающая высокую производительность на маломощных чипах [38]. Краеугольным камнем безопасности является управление ключами и использование цифровых сертификатов, выпускаемых доверенными центрами сертификации (CA). Это позволяет масштабируемо аутентифицировать миллиарды устройств.

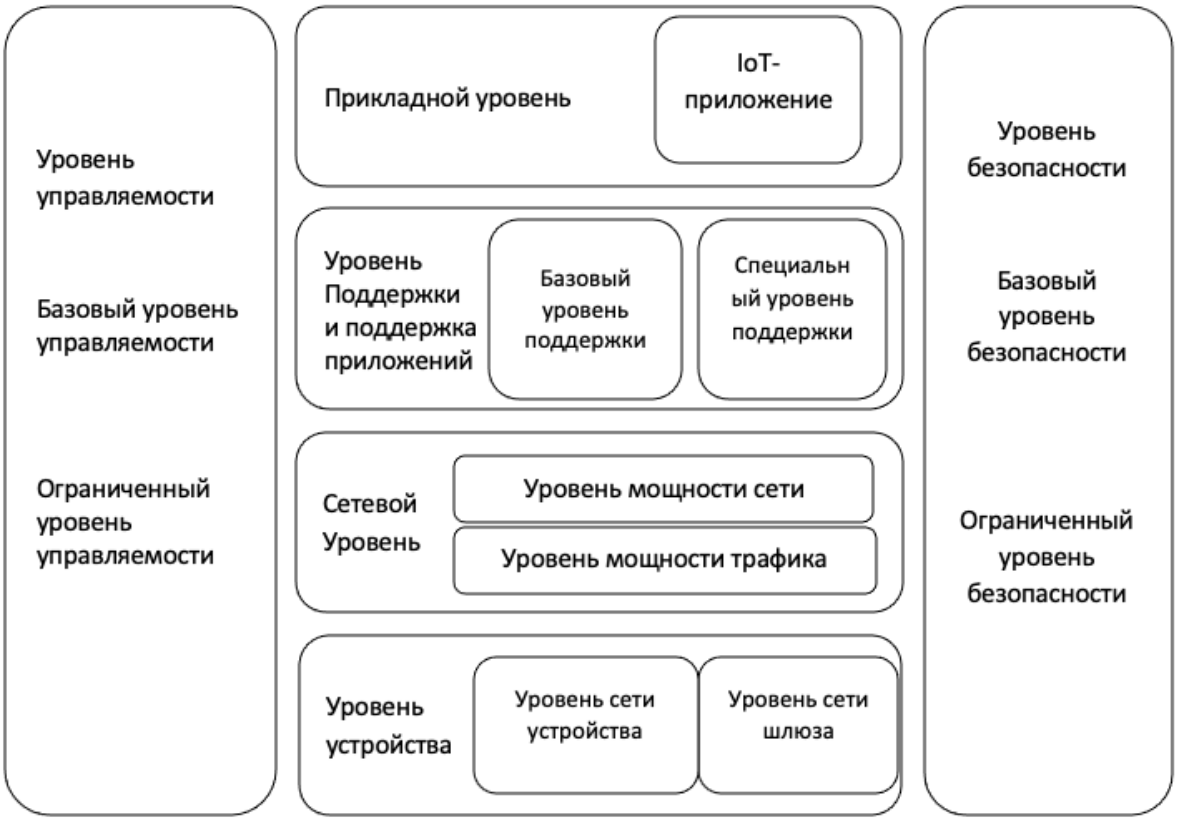

Рис. 2. Архитектура IoT

Взаимная аутентификация между всеми участниками (устройство-устройство, устройство-облако) является критическим требованием. Она часто реализуется через стандартные протоколы (TLS/DTLS), которым предшествует управление жизненным циклом сертификатов с помощью протоколов SCEP, EST или OCSP.

После установления защищённого соединения обеспечивается конфиденциальность данных за счёт их шифрования. В сценариях, где

конфиденциальность не приоритетна (например, в многопрыжковых сетях), для экономии ресурсов может применяться проверка только подлинности данных без их полного шифрования [38].

Протоколы аутентификации в промышленных IoT-системах

Промышленные IoT-системы представляют собой специализированный класс IoT-приложений, предназначенных для автоматизации и удалённого контроля критически важных процессов [40]. Обеспечение их безопасности требует реализации надёжных протоколов аутентификации для защиты от несанкционированного доступа и вредоносных атак, угрожающих не только функциональности, но и ресурсам и репутации предприятия.

В качестве решений предлагаются различные подходы к аутентификации, адаптированные для специфических сред. Например, в автомобильных одноранговых сетях (VANET), являющихся частным случаем IoT, применяются протоколы с сохранением приватности, такие как предложенный W. Li и др. Помимо классических сенсорных сетей, аутентификация может реализовываться с использованием технологий уровня восприятия, включая RFID-метки и смарт-карты. Перспективным направлением также является интеграция блокчейн-технологий, которые могут обеспечить децентрализованные и устойчивые к фальсификации методы проверки подлинности устройств в IoT-системах.

Представленная сравнительная таблица 1 систематизирует основные технологические подходы к обеспечению безопасности в экосистеме Интернета вещей, выделяя их ключевые функциональные характеристики, практические ограничения и типичные области применения. Данный анализ позволяет наглядно оценить компромиссы между криптостойкостью, производительностью, масштабируемостью и стоимостью реализации для каждого метода.

Таблица 1

Технологические подходы к обеспечению безопасности IoT

Категория	**Ключевые преимущества**	**Основные ограничения**	**Типовые сценарии использования**
Криптография (ECC, лёгкие алгоритмы)	Высокая стойкость, обеспечение конфиденциальности и целостности. Оптимизация для маломощных устройств.	Вычислительная нагрузка, сложность управления ключами. Меньшая стойкость лёгких алгоритмов.	Аутентификация устройств, защита каналов связи (TLS/DTLS), сенсорные сети.
Модели доверия (Trust Management)	Выявление внутренних угроз, адаптивность, дополнение криптографии.	Субъективность метрик, накладные расходы, уязвимость к сговору.	Децентрализованные и динамические сети (VANET), системы совместного использования услуг.
Контроль доступа (ABAC/RBAC)	Гибкость и детализация политик, поддержка контекста, масштабируемость.	Сложность администрирования, производительность при проверке прав.	«Умные» здания, промышленный IoT (IIoT), системы здравоохранения.
Блокчейн / DLT	Децентрализация, неизменяемость журналов, прямая аутентификация.	Низкая пропускная способность, задержки, сложность интеграции.	Управление цепочками поставок, микроплатежи, обеспечение подлинности данных.
Аппаратная защита (TPM, TEE)	Высокая изоляция ключей, устойчивость к ПО, надёжная аттестация.	Удорожание устройства, зависимость от вендора, ограниченная мощность.	Критическая инфраструктура, платёжные системы, устройства с защитой прошивки.

Сопоставление демонстрирует, что выбор оптимального решения или их комбинации напрямую зависит от конкретных требований IoT-системы: её архитектуры, критичности обрабатываемых данных, ресурсных ограничений устройств и модели угроз. Таким образом, таблица служит основой для осмысленного проектирования многоуровневой защиты, соответствующей уникальным вызовам различных IoT-сценариев – от массовых сенсорных сетей до промышленных и критически важных инфраструктур.

Заключение

Проведённый систематический обзор выявил, что безопасность Интернета вещей требует комплексного подхода, сочетающего криптографические методы, протоколы аутентификации и динамические модели доверия. Ключевыми вызовами остаются обеспечение подлинности и надёжности в условиях гетерогенности, ресурсных ограничений устройств и децентрализованной архитектуры IoT.

Анализ подтвердил эффективность современных решений – от лёгких криптографических алгоритмов (ECC) и доверенной аутентификации на основе сертификатов до механизмов оценки доверия и интеграции с облачными платформами. Однако для достижения сквозной безопасности необходимы дальнейшие исследования в области:

- энергоэффективных протоколов для маломощных устройств,
- унифицированных моделей доверия,
- практического применения блокчейн- и квантово-криптографических методов.

Перспективным представляется также заимствование и адаптация методов оценки доверия из смежных областей информационной безопасности, таких как скоринг источников разведданных об угрозах [41], для создания комплексных систем оценки надёжности узлов в гетерогенных IoT-сетях. разработка адаптивных протоколов, устойчивых к глушению [42], может быть интегрирована с системами динамического доверия для создания комплексных решений, обеспечивающих безопасность IoT-устройств в условиях активного противодействия

Таким образом, развитие IoT напрямую зависит от создания адаптивных, масштабируемых и контекстно-ориентированных систем безопасности, способных противостоять эволюционирующим угрозам.

Литература

1. Ashton K. et al. That 'internet of things' thing. RFID journal, 2009, № 22-7, pp.97-114.

2. Maslova M. A. Analysis and identification of information security risks. Information Technology, 2019, №4-1. pp.31-37.

3. Kobayashi G. et al. Ubiquity of virtual disguisers and potential impact on ethical behavior. Fourth International Conference on Ubi-Media Computing. IEEE, 2011. pp. 186-190.

4. Kobayashi G. et al. The Ethical Impact of the Internet of Things in Social Relationships: Technological mediation and mutual trust. IEEE Consumer Electronics Magazine, 2016. 5-3. pp. 85-89.

5. Zheng S., Jiang T., Baras JS Exploiting trust relations for our equilibrium efficiency in ad hoc networks. IEEE International Conference on Communications (ICC). – IEEE, 2011, pp. 1-5.

6. Titov D.N. Intrusion detection in the Internet of Things. Interexpo Geo-Siberia, 2022, №8-2, pp.118-125.

7. Ricci F., Rokach L., Shapira B. Recommender systems: introduction and challenges. Recommender systems handbook, 2015, pp.1-34.

8. Kalaï A. et al. Social collaborative service recommendation approach based on user's trust and domain-specific expertise. Future Generation Computer Systems, 2018, № 80.pp. 355-367.

9. Celdran AH et al. Design of a recommender system based on users' behavior and collaborative location and tracking. Journal of Computational Science, 2016. №12, pp. 83-94.

10. Baev D.A., Volkov R.O., Zonov A.D. Security monitoring in IoT networks, StudNet, 2021. pp. 4-6.

11. Staab S. et al. The pudding of trust. IEEE Intelligent Systems, 2004. № 19-5, pp. 74-88.

12. Orekhova O.S., Patrakeev K.A. Technologies that improve information security, Research Center. Technical Innovations, 2021, №1, pp. 18-21.

13. Ashton K. et al. That 'internet of things' thing. RFID journal, 2009, № 22-7, pp.97-114.

14. Arasteh H. et al. IoT-based smart cities: A survey, 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), pp. 1-6.

15. Nesterenko A.Yu., Semenov A.M. Methodology for assessing the security of cryptographic protocols. Applied Discrete Mathematics, 2022, №56, pp. 33-82.

16. Yick J., Mukherjee B., Ghosal D. Wireless sensor network survey. Computer Networks, 2008. №52-12, pp. 2292-2330.

17. Ermakov S.A., Bolgov A.A. Overview of methods for building a risk-based access control model in Internet of Things systems. Information and Security, 2022, №25-2, pp. 263-272.

18. Zafar F. et al. Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes. Journal of Network and Computer Applications, 2017, № 94. pp. 50-68.

19. Sicari S. et al. Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, 2015, pp.146-164.

20. Ali T., Nauman M., Jan S. Trust in IoT: dynamic remote attestation through efficient behavior capture. Cluster Computing, 2018. №21, pp. 409-421.

21. Køien GM Reflections on trust in devices: an informal survey of human trust in an internet-of-things context. Wireless Personal Communications, 2011, №61, pp. 495-510.

22. Vaquero LM et al. A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review, 2008, №39-1, pp. 50-55.

23. Voorsluys W., Broberg J., Buyya R. Introduction to cloud computing. Cloud Computing: Principles and Paradigms, 2011, № 1-41.

24. Mell P. et al. The NIST definition of cloud computing, 2011.

25. Fortino G. et al. Using trust and local reputation for group formation in the cloud of things. Future Generation Computer Systems, 2018, №89, pp. 804-815.

26. Gusmeroli S., Piccione S., Rotondi D. A capability-based security approach to manage access control in the Internet of Things. Mathematical and Computer Modeling, 2013, № 58-5-6, pp.1189-1205.

27. Alcaide A. et al. Anonymous authentication for privacy-preserving IoT target-driven applications. Computers & Security, 2013, №37. pp. 111-123.

28. Sfar AR et al. A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 2018, № 4-2. pp.118-137.

29. Jøsang A., Keser C., Dimitrakos T. Can we manage trust? Trust Management: Third International Conference, iTrust 2005, pp. 93-107.

30. Blaze M., Feigenbaum J., Lacy J. Decentralized trust management. Proceedings 1996 IEEE Symposium on Security and Privacy, IEEE, 1996, pp.164-173.

31. Blaze M., Ioannidis J., Keromytis A.D. Experience with the keynote trust management system: Applications and future directions. Trust Management: First International Conference, iTrust 2003 Heraklion, 2003, pp. 284-300.

32. Kounelis I. et al. Building trust in the human–internet of things relationship. IEEE Technology and Society Magazine, 2014, №33-4, pp.73-80.

33. Karnuta D.S. Quantum-cryptographic encryption methods as a relevant and effective means of ensuring information security in IoT networks. Questions of Information Security, 2021. №2-133.

34. Valentine S. Human resource management, ethical context, and personnel consequences: A commentary essay. Journal of Business Research, 2010, №63-8, pp. 908-910.

35. Gupta BB, Tewari A. A Beginner's Guide to Internet of Things Security: Attacks, Applications, Authentication, and Fundamentals. CRC Press, 2020.

36. Stergiou C. et al. Secure integration of IoT and cloud computing. Future Generation Computer Systems, 2018, №78, pp. 964-975.

37. IoT. URL: strij.tech/publications/tehnologiya/chto-takoe-internetveschey.html

38. Oreshkina D. Internet of Things (IoT) Security Reference Architecture. Electronic document. URL: anti-malware.ru/practice/solutions/iot-reference-architecture-protection-part-2

39. Naraliev N.A., Samal D.I. Review and analysis of standards and protocols in the field of the Internet of Things. Modern testing methods and problems of information security IoT. International Journal of Open Information Technologies, 2019, №8, pp. 95-104.

40. Li W., Wang P. Two-factor authentication in industrial Internet-of-Things: Attacks, evaluation and new construction. Future Generation Computer Systems, 2019, №101, pp. 694-708.

41. Туманов Д.А., Абрамов Е.С. Поиск и скоринг источников индикаторов компрометации по индустриям // Инженерный вестник Дона. 2024. №8. URL: ivdon.ru/ru/magazine/archive/n8y2024/9451.

42. Григорян К.С., Басан Е.С. Онтология методов и стратегий защиты радиоканалов от преднамеренных помех // Инженерный вестник Дона. 2025. №11. URL: ivdon.ru/ru/magazine/archive/n11y2025/10533.

References

1. Ashton K. et al. RFID journal, 2009, № 22-7, pp.97-114.
2. Maslova M. A. Information Technology, 2019, №4-1. pp.31-37.

3. Kobayashi G. et al. Fourth International Conference on Ubi-Media Computing. IEEE, 2011. pp. 186-190.
4. Kobayashi G. et al. IEEE Consumer Electronics Magazine, 2016. 5-3. pp. 85-89.
5. Zheng S., Jiang T., Baras JS IEEE International Conference on Communications (ICC). IEEE, 2011, pp. 1-5.
6. Titov D.N. Interexpo Geo-Siberia, 2022, №8-2, pp.118-125.
7. Ricci F., Rokach L., Shapira B. Recommender systems handbook, 2015, pp.1-34.
8. Kalaï A. et al. Future Generation Computer Systems, 2018, № 80.pp. 355-367.
9. Celdran AH et al. Journal of Computational Science, 2016. №12, pp. 83-94.
10. Baev D.A., Volkov R.O., Zonov A.D., StudNet, 2021. pp. 4-6.
11. Staab S. et al. IEEE Intelligent Systems, 2004. № 19-5, pp. 74-88.
12. Orekhova O.S., Patrakeev K.A. Technical Innovations, 2021, №1, pp. 18-21.
13. Ashton K. et al. RFID journal, 2009, № 22-7, pp.97-114.
14. Arasteh H. et al. 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), pp. 1-6.
15. Nesterenko A.Yu., Semenov A.M. Applied Discrete Mathematics, 2022, №56, pp. 33-82.
16. Yick J., Mukherjee B., Ghosal D. Computer Networks, 2008. №52-12, pp. 2292-2330.
17. Ermakov S.A., Bolgov A.A. Information and Security, 2022, №25-2, pp. 263-272.
18. Zafar F. et al. Journal of Network and Computer Applications, 2017, № 94. pp. 50-68.
19. Sicari S. et al. Computer Networks, 2015, pp.146-164.
20. Ali T., Nauman M., Jan S. Cluster Computing, 2018. №21, pp. 409-421.
21. Køien GM Wireless Personal Communications, 2011, №61, pp. 495-510

22. Vaquero LM et al. ACM SIGCOMM Computer Communication Review, 2008, №39-1, pp. 50-55.
23. Voorsluys W., Broberg J., Buyya R. Cloud Computing: Principles and Paradigms, 2011, № 1-41.
24. Mell P. et al. The NIST definition of cloud computing, 2011.
25. Fortino G. et al. Future Generation Computer Systems, 2018, №89, pp. 804-815.
26. Gusmeroli S., Piccione S., Rotondi D. Mathematical and Computer Modeling, 2013, № 58-5-6, pp.1189-1205.
27. Alcaide A. et al. Computers & Security, 2013, №37. pp. 111-123.
28. Sfar AR et al. Digital Communications and Networks, 2018, № 4-2. pp.118-137.
29. Jøsang A., Keser C., Dimitrakos T. Trust Management: Third International Conference, iTrust 2005, pp. 93-107.
30. Blaze M., Feigenbaum J., Lacy J. Proceedings 1996 IEEE Symposium on Security and Privacy, IEEE, 1996, pp.164-173.
31. Blaze M., Ioannidis J., Keromytis A.D. Trust Management: First International Conference, iTrust 2003 Heraklion, 2003, pp. 284-300.
32. Kounelis I. et al. IEEE Technology and Society Magazine, 2014, №33-4, pp.73-80.
33. Karnuta D.S. Questions of Information Security, 2021. №2-133.
34. Valentine S. Journal of Business Research, 2010, №63-8, pp. 908-910.
35. Gupta BB, Tewari A. CRC Press, 2020.
36. Stergiou C. et al. Future Generation Computer Systems, 2018, №78, pp. 964-975.
37. IoT. URL: strij.tech/publications/tehnologiya/chto-takoe-internetveschey.html

38. Oreshkina D. Internet of Things (IoT) Security Reference Architecture. Electronic document. URL: anti-malware.ru/practice/solutions/iot-reference-architecture-protection-part-2
39. Naraliev N.A., Samal D.I. International Journal of Open Information Technologies, 2019, №8, pp. 95-104.
40. Li W., Wang P. Future Generation Computer Systems, 2019, №101, pp. 694-708.
41. Tumanov D.A., Abramov E.S. Inzhenernyj vestnik Dona. 2024. №8. URL: ivdon.ru/ru/magazine/archive/n8y2024/9451.
42. Grigoryan K.S., Basan E.S. Inzhenernyj vestnik Dona. 2025. №11. URL: ivdon.ru/ru/magazine/archive/n11y2025/10533.

Дата поступления: 9.11.2025

Дата публикации: 26.12.2025