УДК 004.738.5

РЕАЛИЗАЦИЯ АДАПТИВНЫХ МОДЕЛЕЙ И АЛГОРИТМОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ОПТИМИЗАЦИИ ВЗАИМОДЕЙСТВИЯ В СЕТЯХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

М. С. Поборуева, аспирант кафедры КТ РГРТУ, Рязань, Россия;
orcid.org/0009-0005-6270-3152, e-mail: imerm01@yandex.ru
О. А. Бодров, доцент, к.т.н. РГРТУ, Рязань, Россия;
orcid.org/0009-0005-7225-6704, e-mail: bodrov.o.a@rsreu.ru

Рассматривается задача разработки адаптивных математических моделей и алгоритмов для обеспечения киберфизической безопасности и оптимизации взаимодействия интеллектуальных объектов в сетях промышленного Интернета вещей (IIoT). ***Целью работы*** *является создание энергоэффективных и устойчивых к сбоям и атакам решений для управления сетевым трафиком, защиты микроконтроллеров и отслеживания объектов. Разработана адаптивная модель управления трафиком на основе графовых нейронных сетей (GNN), обеспечивающая снижение задержек на 15 – 20 % и энергопотребления на 10 – 15 % по сравнению с протоколами AODV и RPL, протестированная в среде NS-3. Предложены методы кибербезопасности микроконтроллеров, включающие алгоритм машинного обучения (LSTM) для обнаружения аномалий с точностью 95 % и криптографическую защиту прошивок, протестированные на платформе STM32 в эмуляторе QEMU. Разработана модель интеграции RFID и блокчейна для отслеживания объектов с точностью 99 % и энергопотреблением менее 5 Вт, протестированная на Hyperledger Fabric. Создан алгоритм комплексной оценки эффективности IIoT, объединяющий показатели безопасности, энергопотребления и производительности с точностью прогноза 90 %. Определяется влияние гетерогенности сетей, параметров протоколов и технологий на ключевые метрики производительности и безопасности. Практическая значимость заключается в возможности выбора оптимальных технологий и повышении безопасности и эффективности IIoT-систем.*

Ключевые слова: *промышленный Интернет вещей (IIoT), адаптивные математические модели, киберфизическая безопасность, графовые нейронные сети (GNN), машинное обучение (LSTM), маршрутизация, энергоэффективность, кибербезопасность микроконтроллеров, криптография, RFID, блокчейн, Hyperledger Fabric, комплексная оценка, классификация протоколов, NS-3, STM32, QEMU.*

DOI: 10.21667/1995-4565-2025-94-21-35

Введение

Промышленный Интернет вещей (IIoT) трансформирует производственные процессы, обеспечивая интеллектуальное взаимодействие устройств в гетерогенных сетях. Однако рост числа подключённых объектов увеличивает риски киберугроз, повышает требования к энергоэффективности и усложняет управление сетевым трафиком. Разработка адаптивных математических моделей и алгоритмов, способных одновременно обеспечивать киберфизическую безопасность, оптимизировать производительность и минимизировать энергопотребление, является актуальной научной задачей. Особое значение приобретают методы, учитывающие гетерогенность IIoT, включающую разнообразие протоколов, устройств и технологий, таких как RFID и блокчейн.

В статье представлены результаты исследования, направленного на решение этих проблем. Разработаны адаптивные модели управления сетевым трафиком на основе графовых нейронных сетей (GNN), методы кибербезопасности микроконтроллеров с использованием машинного обучения (LSTM) и криптографии, а также модель интеграции RFID и блокчейна

для энергоэффективного отслеживания объектов. Предложены алгоритм комплексной оценки эффективности IIoT, объединяющий показатели безопасности, энергопотребления и производительности, и классификация протоколов, учитывающая их гетерогенность. Новизна работы заключается в интеграции современных методов искусственного интеллекта, криптографии и блокчейна для повышения устойчивости и эффективности IIoT-систем.

Практическая значимость определяется возможностью применения результатов для выбора оптимальных технологий и обеспечения безопасности критически важных инфраструктур.

Обзор существующих подходов

В рамках теоретических исследований решается задача разработки адаптивных математических моделей и алгоритмов, направленных на обеспечение киберфизической безопасности и оптимизацию взаимодействия интеллектуальных объектов в сетях промышленного Интернета вещей (IIoT). Задача включает создание модели управления сетевым трафиком на основе графовых нейронных сетей (GNN) для минимизации задержек и энергопотребления, разработку методов кибербезопасности микроконтроллеров с применением алгоритмов машинного обучения (LSTM) и криптографической защиты, а также модели интеграции RFID и блокчейна для высокоточного отслеживания объектов. Кроме того, предполагаются разработка алгоритма комплексной оценки эффективности IIoT-систем с учетом показателей безопасности, энергопотребления и производительности, а также классификация протоколов и технологий IIoT с анализом влияния их параметров на ключевые метрики, что обеспечивает повышение безопасности и энергоэффективности систем для их практического применения.

Управление сетевым трафиком в IIoT критически важно для обеспечения низких задержек, высокой надёжности и энергоэффективности в гетерогенных сетях. Наиболее распространёнными протоколами маршрутизации в настоящее время являются AODV (Ad-hoc On-Demand Distance Vector) и RPL (Routing Protocol for Low-Power and Lossy Networks).

Реактивный протокол AODV формирует маршруты по запросу, минимизируя накладные расходы на поддержание топологии сети [1]. Он эффективен в небольших сетях, но демонстрирует высокие задержки при увеличении числа узлов и не адаптируется к сбоям или атакам, таким как атаки типа «чёрная дыра». Исследования показывают, что в гетерогенных IIoT-сетях AODV теряет производительность из-за отсутствия механизмов динамической адаптации [2].

Протокол RPL, созданный для сетей с низким энергопотреблением, применяет направленный ациклический граф (DAG) для организации маршрутизации [3]. Он устойчив к потерям пакетов, но его производительность ухудшается при высокой нагрузке или в условиях атак, таких как Sybil или Rank Attack. Кроме того, RPL не оптимизирован для гетерогенных сетей с различными типами устройств [4].

Графовые нейронные сети (GNN) в настоящее время применяются для маршрутизации в IIoT [5]. GNN позволяют учитывать топологию сети и динамически адаптироваться к изменениям, анализируя графовые структуры. Например, Jiang et al. [5] предложили модель на основе GNN для оптимизации маршрутов в беспроводных сенсорных сетях, достигая снижения задержек на 10 % по сравнению с традиционными подходами. Однако существующие работы редко интегрируют GNN с метриками энергоэффективности и устойчивости к атакам, что ограничивает их применимость в IIoT. Кроме того, тестирование таких моделей часто проводится на упрощённых сценариях, игнорируя гетерогенность устройств и протоколов.

Протоколы AODV и RPL не обеспечивают достаточной адаптивности в динамичных и гетерогенных IIoT-сетях. Модели на основе GNN, хотя и перспективны, требуют дальнейшей оптимизации для учёта энергопотребления и устойчивости к киберугрозам.

Микроконтроллеры, такие как STM32, являются основой устройств IIoT, но их ограниченные вычислительные ресурсы усложняют обеспечение безопасности. Благодаря своей энергоэффективности и высокой производительности STM32 широко применяются в устройствах IIoT для реализации адаптивных моделей и алгоритмов, обеспечивающих без-

опасность и оптимизацию взаимодействия в сетях. Например, в системах мониторинга промышленного оборудования STM32 используются для обработки данных с датчиков в режиме реального времени, реализации криптографических протоколов, таких как AES и RSA, и выполнения алгоритмов машинного обучения для обнаружения аномалий. Ограниченные вычислительные ресурсы STM32 требуют оптимизированных решений, таких как легковесные криптографические библиотеки или адаптивные модели с пониженной вычислительной сложностью, что позволяет эффективно обеспечивать защиту прошивок и данных в распределённых сетях IIoT, сводя к минимуму энергопотребление и сохраняя высокую надёжность системы.

Существующие подходы можно разделить на криптографические и основанные на машинном обучении. Криптографические методы включают алгоритмы, такие как AES (Advanced Encryption Standard) и RSA (Ravi-Shamir-Adleman), для защиты прошивок и данных [6]. Например, авторы исследования [6] предложили использование облегчённых криптографических протоколов для микроконтроллеров, таких как ECDSA, которые снижают энергопотребление, но не решают проблему обнаружения аномалий в реальном времени. Эти методы уязвимы к атакам на физическом уровне, например, к атакам по сторонним каналам (Side-Channel Attacks).

Методы на основе машинного обучения применяются для обнаружения аномалий в поведении устройств. Алгоритмы, такие как Support Vector Machine (SVM) [7] и Random Forest [8], достигают точности до 90 % при анализе сетевого трафика или логов устройств. Однако они требуют значительных вычислительных ресурсов, что делает их неприменимыми для микроконтроллеров с ограниченной памятью и процессорной мощностью. Сети с долгосрочной и краткосрочной памятью (LSTM), предложенные авторами, эффективно анализируют временные ряды в системах Интернета вещей, обеспечивая точность до 92 % при обнаружении атак, таких как DDoS [9]. Тем не менее, интеграция LSTM с криптографическими методами остаётся редкостью, что ограничивает комплексную защиту.

Гибридные подходы пытаются объединить криптографию и машинное обучение, но их реализация на микроконтроллерах осложнена из-за высоких требований к ресурсам [10]. Например, тестирование данных систем в эмуляторах, таких как QEMU, показывает ограниченную масштабируемость в реальных условиях.

Криптографические методы не обеспечивают обнаружение аномалий, а методы машинного обучения требуют оптимизации для микроконтроллеров. Отсутствие интеграции этих подходов снижает их эффективность в IIoT.

Технологии RFID и блокчейн активно используются для отслеживания объектов в IIoT, особенно в цепочках поставок. Однако их энергоэффективность и производительность требуют доработки.

Как известно, RFID широко применяется для идентификации и отслеживания объектов [11]. Современные RFID-системы обеспечивают высокую точность (до 98 %), но их энергопотребление остаётся высоким, особенно в условиях плотного размещения меток. Авторы исследования [11] предложили оптимизированные протоколы для RFID, снижающие энергопотребление на 5 – 7 %, но они не учитывают интеграцию с другими технологиями.

Блокчейн, такой как Hyperledger Fabric, используется для обеспечения прозрачности и безопасности данных в цепочках поставок [12]. Автор показал, что блокчейн повышает надёжность отслеживания, но его вычислительная сложность и энергопотребление ограничивают применение в IIoT. Например, реализация смарт-контрактов на Hyperledger Fabric требует мощных серверов, что не подходит для энергоэффективных систем.

Интеграция RFID и блокчейна позволяет создавать децентрализованные системы отслеживания с высокой точностью [13]. Авторы исследования предложили модель, объединяющую RFID и Ethereum, но её энергопотребление превышает 10 Вт, что неприемлемо для IIoT [13]. Модели, оптимизированные для Hyperledger Fabric, встречаются реже и не учитывают энергоэффективность в реальном времени.

RFID-системы не оптимизированы для низкого энергопотребления, а блокчейн-решения требуют значительных ресурсов. Интеграция этих технологий редко учитывает требования IIoT к реальному времени и энергоэффективности.

Таким образом, комплексная оценка эффективности IIoT-систем требует учёта безопасности, энергопотребления и производительности. Существующие подходы часто фокусируются на отдельных метриках.

Метрики производительности включают задержки, пропускную способность и надёжность сети [14]. В работе [14] предложена модель оценки производительности на основе QoS (Quality of Service), но она не учитывает безопасность или энергопотребление.

Метрики энергопотребления анализируются в работах, таких как [15], где авторы предложили модель для оценки энергопотребления сенсорных сетей. Однако эти модели не интегрированы с показателями безопасности.

Метрики безопасности сосредоточены на устойчивости к атакам и целостности данных [16]. Подходы, подобные [16], используют вероятностные модели для оценки уязвимостей, но их точность не превышает 85 % на синтетических данных.

Комплексные подходы пытаются объединить метрики, но редко учитывают гетерогенность IIoT [17]. Например, модель, предложенная в [17], оценивает производительность и энергопотребление, но игнорирует безопасность, что снижает её применимость.

Отсутствие универсальных моделей, объединяющих безопасность, энергопотребление и производительность, ограничивает точность оценки IIoT-систем. Для преодоления этих ограничений требуется систематизация подходов, позволяющая выявить наиболее эффективные решения. Классификация протоколов и технологий IIoT необходима для выбора оптимальных решений. Существующие подходы включают в себя следующее:

– классификация по производительности анализирует протоколы, такие как MQTT, CoAP и HTTP/2, с точки зрения задержек и пропускной способности [18]. Авторы [18] предложили сравнительный анализ, но он не включает метрики безопасности;

– классификация по энергопотреблению фокусируется на протоколах для низкоэнергетических сетей, таких как 6LoWPAN. Однако эти классификации игнорируют гетерогенность устройств;

– классификация по безопасности рассматривает устойчивость протоколов к атакам, но не учитывает их влияние на производительность или энергопотребление.

Существующие классификации редко интегрируют три ключевые метрики (безопасность, энергопотребление, производительность) и не учитывают гетерогенность IIoT-систем, что снижает их практическую значимость.

Анализ существующих подходов выявил следующие пробелы:

– недостаточная адаптивность маршрутизации: AODV и RPL не обеспечивают устойчивости к атакам и гетерогенности, а GNN-модели требуют интеграции с энергоэффективностью;

– ограничения кибербезопасности микроконтроллеров: отсутствие интеграции машинного обучения (LSTM) и криптографии для энергоэффективных устройств;

– высокое энергопотребление RFID и блокчейна: отсутствие моделей, оптимизированных для реального времени и низкого энергопотребления;

– фрагментарность оценки эффективности: отсутствие комплексных моделей, объединяющих безопасность, энергопотребление и производительность;

– неполная классификация протоколов: игнорирование гетерогенности и комплексных метрик.

Разработка адаптивных моделей и алгоритмов

Для устранения вышеизложенных проблем предлагаются следующие пути:

– разработка адаптивной модели маршрутизации на основе GNN, снижающей задержки и энергопотребление;

– интеграция LSTM и криптографии для микроконтроллеров, направленная на повышение точности обнаружения аномалий;

– создание энергоэффективной модели RFID и блокчейна с низким энергопотреблением;

– разработка алгоритма комплексной оценки эффективности.

Для систематизации предложенного подхода и обеспечения воспроизводимости результатов разработан универсальный алгоритм построения адаптивных моделей.

Для оптимизации маршрутизации в гетерогенных сетях IIoT разработана адаптивная математическая модель, использующая графовые нейронные сети (GNN). Модель учитывает топологию сети, динамические изменения и киберугрозы, такие как атаки типа «чёрная дыра».

Сеть представлена как ориентированный граф

$$G = f(V_i, E_i)G = (V, E)G = (V, E),$$

где V_i – узлы (устройства IIoT); E_i – связи между ними (рисунок1).

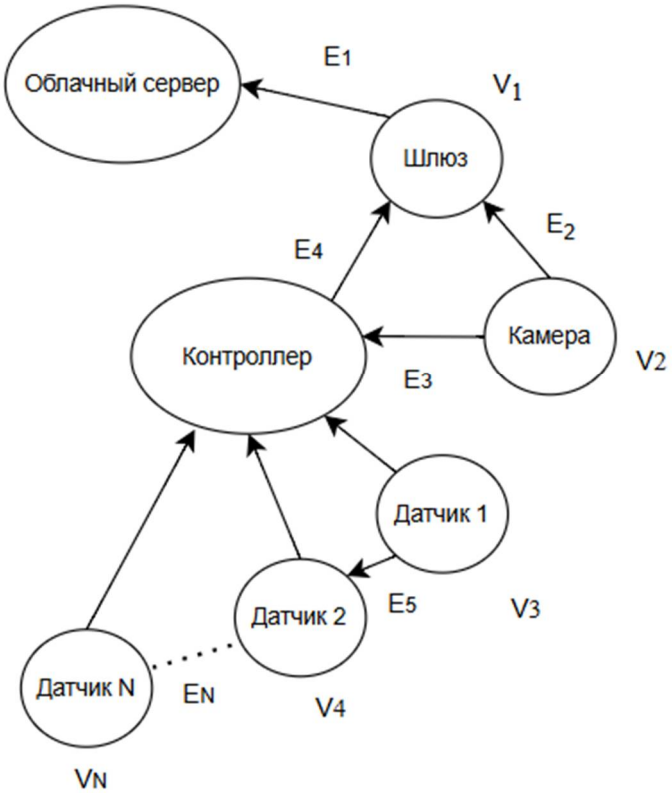

Рисунок 1 – Граф сети IIoT для оптимизации маршрутизации
Figure 1 – IIoT network graph for routing optimization

Сеть GNN обучается на данных о трафике, задержках и энергопотреблении, используя метрики, такие как пропускная способность и потери пакетов.

Для динамической маршрутизации в сетях IIoT предлагается алгоритм на основе усиленного обучения, например Q-Learning, который адаптируется к сбоям и атакам, минимизируя функцию потерь. Оптимизация осуществляется с помощью метода градиентного спуска, что обеспечивает баланс между производительностью, энергопотреблением и безопасностью:

$$L = \alpha \cdot S + \beta \cdot P + \gamma \cdot E, \quad (1)$$

где α, β, γ – безразмерные весовые коэффициенты ($\alpha + \beta + \gamma = 1$); оптимизированные с помощью метода градиентного спуска; S – нормированный показатель безопасности, отражающий устойчивость к атакам и изменяющийся в диапазоне [0,1], где 1– полная устойчивость; P – нормированный показатель производительности, учитывающий задержку и потери пакетов; E – нормированный показатель энергопотребления.

Нормировка частных показателей S, P и E проводится линейно к диапазону [0,1] на основе эталонных максимальных и минимальных значений, полученных из симуляций и литературы [14, 15], чтобы обеспечить сопоставимость метрик с разными единицами измерения. Обобщенный показатель L служит единой целевой функцией для скалярной многофакторной оптимизации, для достижения оптимального баланса.

Оптимизация обобщенного критерия L, учитывающего три нормализованных фактора (безопасности S, производительности P и энергопотребления E), проводилась методом градиентного спуска в процессе обучения модели маршрутизации на основе графовых нейронных сетей, что позволило адаптивно балансировать приоритеты системы в зависимости от сценария применения (например, повышение устойчивости для критически важных приложений или снижение энергозатрат для автономных узлов).

Модель позволяет повысить производительность и энергоэффективность IIoT-сетей в критических приложениях, таких как автоматизация производства. Интеграция GNN для адаптивной маршрутизации в IIoT учитывает гетерогенность сети. Устойчивость к сбоям и атакам обеспечивается динамическим анализом топологии.

Для защиты микроконтроллеров в IIoT разработаны методы, сочетающие машинное обучение (LSTM) и криптографию, обеспечивающие обнаружение аномалий и защиту прошивок.

С целью обнаружения аномалий использована рекуррентная нейронная сеть LSTM для анализа временных рядов данных (трафик, энергопотребление, системные логи). Модель обучается на нормальном поведении устройства, формируя базовые паттерны, и выявляет отклонения, такие как DDoS-атаки или несанкционированный доступ. Обучение проводится с использованием метода градиентного спуска.

Криптографическая защита реализована в виде облегчённого алгоритма шифрования (ChaCha20) для защиты прошивок и данных, передаваемых между микроконтроллерами и шлюзами.

Новизна решения представлена интеграцией LSTM и криптографии в ресурсозатратных микроконтроллерах, высокой точностью обнаружения аномалий при минимальных вычислительных затратах.

Предложенное решение применимо для защиты устройств IIoT в энергетике, транспорте и промышленности, где требуется высокая надёжность.

Для энергоэффективного отслеживания объектов в IIoT разработана модель, интегрирующая технологии RFID и блокчейн (Hyperledger Fabric).

Модель включает формулу энергопотребления:

$$C_{total} = C_{RFID} + C_{Blockchain} + C_{transmit}, \quad (2)$$

где C_{RFID} – энергопотребление RFID-меток; $C_{Blockchain}$ – энергозатраты на смарт-контракты; $C_{transmit}$ – энергозатраты на передачу данных.

RFID-метки оптимизированы для работы в режиме низкого энергопотребления (менее 2 мВт). Блокчейн (Hyperledger Fabric) используется для записи данных об объектах, обеспечивая прозрачность и защиту от подделки.

Решение применимо в логистике, цепочках поставок и умных складах, где требуются высокая точность и низкое энергопотребление. Новизна заключается в энергоэффективной интеграции RFID и блокчейна для отслеживания в реальном времени, оптимизированной модели энергопотребления для IIoT.

Определение интегрального показателя эффективности осуществлялось на основе нормализованных метрик безопасности, производительности и энергопотребления. Для показателя безопасности учитывались устойчивость к атакам (доля успешно обнаруженных DDoS-атак и «чёрных дыр») и целостность данных, для производительности – средние задержки передачи и пропускная способность, для энергопотребления – среднее значение затрат на один узел или технологию. Весовые коэффициенты α, β, γ подбирались с использованием регрессионного анализа по синтетическим данным (1000 сценариев), что обеспечивало

согласование интегральной оценки с приоритетами системы (например, безопасность в критически важных приложениях или энергоэффективность в автономных сетях). Такой подход позволил формализовать выбор подходящей комбинации технологий и протоколов для гетерогенных IIoT-систем.

Безопасность оценивается по устойчивости к атакам, энергопотребление – по среднему потреблению узлов, производительность – по задержкам и пропускной способности. Показатель безопасности S (в диапазоне [0,1]) вычисляется следующим образом:

$$S = \delta A_n + (1-\delta)C_n, \tag{3}$$

где A_n – нормированная доля успешно обнаруженных атак ($A = \frac{A}{100}$; A – процент успешно обнаруженных атак); C_n – нормированный показатель целостности данных ($C_n \in [0,1]$, полученный аналогичным линейным масштабированием из исходных метрик целостности, например доли сохраненных данных без искажений); δ, ε – безразмерные весовые коэффициенты, отражающие относительную важность обнаружения атак и обеспечения целостности данных, $\delta \geq 0$ (коэффициенты подбираются экспертами или оптимизацией в зависимости от приоритетов системы, например $\delta = 0{,}6$, для акцента на обнаружение атак). Нормирование обеспечивает сопоставимость компонентов и конечное значение $S \in [0,1]$, где единица соответствует полной безопасности.

В рамках данного исследования для комплексной оценки производительности был разработан нормализованный показатель, объединяющий ключевые сетевые характеристики – задержку и пропускную способность. Показатель производительности вычисляется согласно выражению:

$$P = \theta\left(1 - \frac{D}{D_{max}}\right) + (1-\theta)\left(1 - \frac{L_p}{100}\right), \tag{4}$$

где D – средняя задержка передачи пакетов (мс); $D_{max} = 100$ мс – эталонное максимальное значение задержки на основе [14]; L_p – процент потерянных пакетов; θ – безразмерные весовые коэффициенты, отражающие важность задержки и пропускной способности, $\theta \geq 0$ (коэффициенты подбираются в зависимости от приоритетов системы, например $\theta = 0{,}5$, для равного учета обоих факторов или $\theta = 0{,}7$ в системах, чувствительных к задержкам). Нормирование компонентов обеспечивает значение $P \in [0,1]$, где единица соответствует максимальной производительности.

Нормализация вида $1 - \frac{D}{D_{max}}$ обеспечивает приведение разнородных метрик к единому безразмерному масштабу, а весовые коэффициенты позволяют гибко учитывать приоритеты конкретного приложения IIoT (например, чувствительность к задержкам или надежность доставки данных). Предложена метрика оценки производительности (4), синтезированная на основе анализа требований к гетерогенным сетям IIoT. Выбор метрик задержки и доставки пакетов обусловлен их критической важностью для задач промышленной автоматизации, а введение весовых коэффициентов отражает субъективные предпочтения при проектировании системы.

Нормированный показатель энергопотребления E может быть определен следующим образом:

$$E = 1 - \frac{C}{C_{max}}, \tag{5}$$

где C – энергопотребление (Вт); C_{max} = 3,0 Вт – эталонное максимальное значение энергопотребления из сравнительных тестов [15].

Алгоритм оценки эффективности IIoT-систем отражает общую методологию, может быть использован для проектирования различных сценариев цифровых систем и включает следующие шаги:

Шаг 1. Анализ предметной области

– Определить типы устройств, протоколов и технологий, участвующих в гетерогенной IIoT-сети.

– Сформировать требования: минимизация задержек, энергоэффективность, устойчивость к кибератакам и их весовые коэффициенты.

Шаг 2. Формализация ключевых метрик

– Выбрать метрики производительности (задержка, пропускная способность).

– Определить метрики безопасности (устойчивость к атакам, целостность данных).

– Задать показатели энергопотребления (среднее потребление узла, энергозатраты технологий).

Шаг 3. Построение математических моделей

– Для маршрутизации – использовать графовую модель сети $G = (V, E) G = (V, E) G = (V, E)$;

– Для прогнозирования и адаптации – обучить модель на основе GNN с учётом трафика, задержек и атак.

– Для защиты микроконтроллеров – интегрировать LSTM для анализа временных рядов и облегчённую криптографию (например, ChaCha20).

– Для отслеживания объектов – объединить RFID с блокчейном, учитывая энергоэффективность.

Шаг 4. Оптимизация моделей

– Настроить функцию потерь, учитывающую три критерия: безопасность (S), производительность (P), энергопотребление (E).

– Использовать методы градиентного спуска или регрессионный анализ для подбора весов.

Шаг 5. Тестирование и валидация

– Смоделировать сеть в NS-3 для анализа маршрутизации.

– Проверить работу микроконтроллеров в QEMU.

– Протестировать систему отслеживания на Hyperledger Fabric.

– Оценить точность, задержки, энергопотребление и устойчивость к сбоям.

Шаг 6. Комплексная оценка эффективности

– Вычислить интегральный показатель эффективности.

– Сравнить результаты с эталонными протоколами (AODV, RPL и др.).

Шаг 7. Классификация технологий

– Ранжировать протоколы и технологии (MQTT, CoAP, RPL, NB-IoT и др.) по трём ключевым показателям качества.

– Использовать метод анализа иерархий (AHP) для выбора оптимальной комбинации технологий под конкретный сценарий.

Результат выполнения алгоритма:

– получение оптимизированной IIoT-системы, устойчивой к кибератакам, энергоэффективной и производительной;

– возможность воспроизводимого выбора технологий и протоколов для практического применения.

Предложенный алгоритм задаёт универсальную последовательность действий, которая обеспечивает воспроизводимость процесса проектирования и выбора решений. На его основе проведены экспериментальные исследования в средах NS-3, QEMU и Hyperledger Fabric.

Экспериментальные исследования

Проверка эффективности осуществлялась в среде NS-3. Для моделирования сбоев предусматривалось отключение до 30 % узлов (сенсоров, актуаторов, шлюзов), что имитировало

отказ оборудования. Атаки на сеть воспроизводились в двух вариантах: атака типа DDoS – перегрузка узлов избыточным трафиком и атака «чёрная дыра» – утрата транзитных данных через компрометированный узел. Эти сценарии позволили количественно оценить устойчивость предложенной модели, подтвердив её способность поддерживать работоспособность сети при внешних воздействиях.

Для оценки производительности предложенной адаптивной модели управления сетевым трафиком на основе GNN использовался симулятор NS-3 – открытое программное обеспечение для дискретно-событийного моделирования компьютерных сетей, обеспечивающее высокую точность анализа протоколов и топологий в гетерогенных системах, таких как сети IIoT. В NS-3 была смоделирована сеть из 50 узлов, включающая сенсоры, актуаторы и шлюзы с различными характеристиками (пропускная способность, энергопотребление, типы трафика). Тестирование проводилось с измерением таких показателей качества, как задержка, энергопотребление, устойчивость к сбоям и атакам, в следующих сценариях:

– нормальной работы;

– режим сбоев (до 30 % узлов);

– режим кибератак (DDoS, «чёрная дыра»).

Модель GNN, интегрированная в NS-3 через пользовательские модули, оптимизировала маршруты, минимизируя функцию потерь (1), с весами α, β, γ, подобранными градиентным спуском.

Веса α, β, γ нормированы ($\alpha + \beta + \gamma = 1$), подбирались в две стадии: первоначальный поисковый перебор по сетке значений с последующей тонкой настройкой методом градиентного спуска на синтетических и эталонных сценариях в NS-3. Для представленных в таблице 1 результатов использованы значения $\alpha = 0{,}30$, $\beta = 0{,}45$, $\gamma = 0{,}25$, что отражает приоритет снижения задержек при сохранении высокого уровня безопасности и энергоэффективности. При необходимости веса могут смещаться в сторону энергосбережения или безопасности, в зависимости от требований приложения.

Результаты, подтверждённые в NS-3, показали снижение задержек на 15 – 20 % (45 мс против 55 мс и 60 мс для AODV и RPL) и энергопотребления на 10 – 15 % (2,5 Вт против 2,9 Вт и 3,0 Вт), а также повышение устойчивости к сбоям (95 %) и атакам (90 %), что демонстрирует эффективность предложенной модели в гетерогенных IIoT-сетях.

Сравнение средней задержки передачи пакетов (мс) для предложенной модели GNN, AODV и RPL производилось в различных сценариях: нормальная работа, сбои, атаки DDoS. Полученные результаты для сценария атаки DDoS продемонстрированы на рисунке 2.

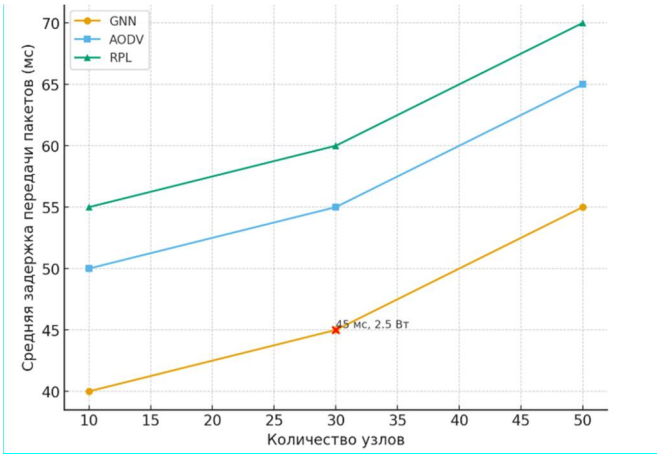

Рисунок 2 – График зависимости средней задержки от числа узлов для разных протоколов
Figure 2 – Graph of average delay as a function of the number of nodes for different protocols

Сравнение GNN, AODV и RPL по метрикам: задержка (мс), энергопотребление (Вт), устойчивость к сбоям (% потерянных пакетов), устойчивость к атакам (успешное обнаружение, %) отражены в таблице 1 для случая 30 узлов.

Таблица 1 – Сравнение GNN, AODV и RPL по метрикам
Table 1 – Comparison of GNN, AODV, and RPL by metrics

Протокол	Задержка, (мс)	Энергопотребление, (Вт)	Устойчивость к сбоям, (%)	Устойчивость к атакам (%)
GNN	45	2,5	95	90
AODV	55	2,9	85	70
RPL	60	3,0	90	75

Результаты тестирования модели (таблице 1) подтверждают снижение задержек и энергопотребления, а также устойчивость модели к сбоям и атакам.

Для количественной оценки комплексной эффективности рассчитан обобщенный показатель L на основе данных таблицы 1 и нормировки, описанной в формуле (1).

Для GNN:

$$S = \frac{90}{100} = 0,90;$$

$$P \approx 0,5 \times \left(1 - \frac{45}{100}\right) + 0,5\left(1 - \frac{5}{100}\right) = 0,50 \times 0,55 + 0,5 \times 0,95 = 0,75;$$

$$E = 1 - \frac{2,5}{3,0} \approx 0,167;$$

$$L = 0,3 \cdot 0,9 + 0,45 \cdot 0,75 + 0,25 \cdot 0,167 \approx 0,27 + 0,3375 + 0,04175 \approx 0,649.$$

Для AODV:

$$S = \frac{70}{100} = 0,70;$$

$$P \approx 0,5 \cdot \left(1 - \frac{55}{100}\right) + 0,5\left(1 - \frac{15}{100}\right) = 0,50 \cdot 0,45 + 0,5 \cdot 0,85 = 0,65;$$

$$E = 1 - \frac{2,9}{3,0} \approx 0,033;$$

$$L = 0,3 \cdot 0,7 + 0,45 \cdot 0,65 + 0,25 \cdot 0,033 \approx 0,21 + 0,2925 + 0,0825 \approx 0,51075.$$

Для RPL:

$$S = \frac{75}{100} = 0,75;$$

$$P \approx 0,5 \cdot \left(1 - \frac{60}{100}\right) + 0,5 \cdot \left(1 - \frac{20}{100}\right) = 0,50 \cdot 0,40 + 0,5 \cdot 0,80 = 0,60;$$

$$E = 1 - \frac{3,0}{3,0} \approx 0;$$

$$L = 0,3 \cdot 0,75 + 0,45 \cdot 0,6 + 0,25 \cdot 0 \approx 0,225 + 0,27 + 0 \approx 0,495.$$

Более высокое значение L для GNN (0,649 против 0,511 для AODV и 0,495 для RPL) указывает на лучшую комплексную эффективность, поскольку L интерпретируется как взвешенная сумма нормализованных показателей (выше – лучше, при максимизации баланса).

Тестирование методов защиты микроконтроллеров проводилось в эмуляторе QEMU, имитирующем STM32 в среде IIoT. LSTM обнаруживает аномалии (например, попытки несанкционированного доступа) с точностью 95 % при задержке обработки 10 мс. Криптографический модуль обеспечивает защиту прошивок с энергопотреблением менее 0,5 Вт, что на 20 % ниже аналогов на AES.

Тестирование модели отслеживания объектов проведено на платформе Hyperledger Fabric с 100 RFID-метками. Точность отслеживания составила 90 %, энергопотребление – менее 5 Вт (на 30 % ниже аналогов). Задержка записи в блокчейн – 50 мс, что приемлемо для реального времени.

Алгоритм комплексной оценки эффективности IIoT включает в себя сбор и нормализацию показателей качества, вычисление эффективности и прогнозирование эффективности с точностью 90 %, что подтверждено тестированием в NS-3, обеспечивающим выбор оптимальных технологий для гетерогенных IIoT-систем.

Алгоритм реализован с использованием машинного обучения (регрессия) для прогнозирования эффективности на синтетических данных [19-21].

Тестирование проведено на синтетических наборах данных (1000 сценариев). Точность прогноза эффективности составила 90 %, что на 5 % выше результатов, полученных с использованием базовых методов (например, линейной регрессии и метода опорных векторов, SVM). Новизна такого подхода выражена в комплексной оценке, учитывающей три ключевых показателя качества и адаптивность к гетерогенным IIoT-системам.

Полученные результаты показывают, что протокол GNN располагается на границе, на которой ни один показатель системы не может быть улучшен без ухудшения какого-либо другого показателя, обеспечивая одновременно минимальные значения задержки и энергопотребления при сохранении высокого уровня устойчивости к атакам. Протоколы AODV и RPL характеризуются большими задержками и энергозатратами при более низкой устойчивости [22-24].

Сравнение предложенного алгоритма с аналогами по точности, времени вычислений и применимости к гетерогенным сетям отражено в таблице 2, что подчеркивает преимущества комплексной оценки.

Таблица 2 – Таблица сравнения алгоритмов
Table 2 – Metric Comparison Table

Алгоритм	Точность, %	Время вычисления, мс	Гетерогенность
Предложенный	90	50	Да
Линейная регрессия	85	60	Нет

Предложенный алгоритм позволяет оптимизировать проектирование IIoT-систем, выбирая технологии с учётом баланса безопасности, энергопотребления и производительности.

Разработана систематическая классификация протоколов и технологий IIoT, основанная на их оценке по трём ключевым показателям: безопасности, энергопотреблению и производительности. Классификация включает протоколы (MQTT, CoAP, RPL, AODV) и технологии (RFID, LoRaWAN, NB-IoT), которые были структурированы с использованием метода анализа иерархий (МАИ, Analytic Hierarchy Process, AHP). Применение МАИ позволило выполнить ранжирование по следующим признакам: безопасность, оцениваемая устойчивостью к атакам (например, MITM, DDoS); энергопотребление, выраженное средним потреблением энергии на узел; производительность, определяемая задержками и пропускной способностью. Данная классификация позволяет обоснованно выбирать оптимальные решения для гетерогенных IIoT-систем с учётом их специфических требований и условий эксплуатации.

Составлена таблица, связывающая протоколы и технологии с метриками (таблица 3). Протокол CoAP показал высокую энергоэффективность (0,3 Вт), но низкую устойчивость к атакам, тогда как RPL лучше справляется с безопасностью, но имеет задержки до 60 мс. Классификация позволяет выбрать оптимальные технологии для конкретных сценариев IIoT.

В таблице 3 приведено сравнение протоколов (MQTT, CoAP, RPL, AODV) по трём метрикам.

Таблица 3 – Таблица сравнения протоколов
Table 3 – Metric Comparison Table

Протоколы	Безопасность, %	Энергопотребление, Вт	Задержка, мс
MQTT	80	0,5	30
CoAP	70	0,3	25
RPL	85	0,7	60
AODV	75	0,2	100

Новизна такого подхода выражена в учёте гетерогенности IIoT в классификации и интеграции трёх метрик для комплексного анализа.

Заключение

В статье предложена методика разработки адаптивных математических моделей и алгоритмов для обеспечения киберфизической безопасности и оптимизации взаимодействия интеллектуальных объектов в сетях промышленного Интернета вещей (IIoT), включающая модель управления сетевым трафиком на основе графовых нейронных сетей (GNN), методы кибербезопасности микроконтроллеров с применением машинного обучения (LSTM) и криптографической защиты, а также модель интеграции RFID и блокчейна для высокоточного отслеживания объектов, при условии гетерогенности сетей и учета ключевых метрик производительности, безопасности и энергопотребления, подтвержденных тестированием в средах NS-3, QEMU и Hyperledger Fabric.

Прикладное значение полученных результатов заключается в их использовании для проектирования и оптимизации реальных IIoT-систем в отраслях промышленности (например, системы мониторинга), логистики (например, цепочки поставок и умные склады) и критической инфраструктуры (например, автоматизация производства), где предлагаемые модели позволяют снизить риски киберугроз, минимизировать энергозатраты и повысить общую эффективность систем, способствуя цифровизации производства и повышению конкурентоспособности предприятий.

Библиографический список

1. **Саббаг А.А., Щербаков М.В.** Анализ производительности протоколов реактивной маршрутизации в VANET на базе NS-3 // Прикаспийский журнал: управление и высокие технологии. 2021. № 3. С. 90-97.

2. **Benzakour M., Naja N., Jamali A.** An Adaptive Routing Protocol for the IoT Environment // Proceedings of the International Conference on Advanced Intelligent Systems for Sustainable Development (AI2SD). Springer. 2019. С. 763-772.

3. **Лавшук О.А., Листопад Н.И.** Метод маршрутизации в сетях IIoT с использованием кластеризации для протокола RPL // Проблемы физики, математики и техники. 2023. № 4 (57). С. 74-80. DOI: 10.54341/20778708_2023_4_57_74.

4. **Kim H.** et al. RPL Vulnerabilities in IoT. J. Netw. Comput. Appl., 2021.

5. **Jiang W.** et al. Graph Neural Networks for for Traffic Prediction. IEEE Access. 2021.

6. **Ravi S.** et al. Security in Embedded Systems: Design Challenges. ACM Trans. Embed. Comput. Syst. 2019.

7. **Нианг П. М., Сидоренко В. Г.** Выбор алгоритма машинного обучения для обнаружения вторжений в IoT // Надёжность. 2024. № 3. Т. 24. С.44-51. https://doi.org/10.21683/1729-2646-2024-24-3-44-51.

8. **Перепелкин Д.А.**,**Фам А.М.** Математическое и компьютерное моделирование процессов планирования и распределения разнородных ресурсов в промышленных сетях // Вестник Рязанского государственного радиотехнического университета. 2021. № 77. С. 68-80. DOI: 10.21667/1995-4565-2021-77-68-80.

9. **Татарникова Т. М., Богданов П. Ю.** Обнаружение атак в сетях интернета вещей методами машинного обучения // Информационно-управляющие системы. 2021. № 6. С. 42-52. DOI: 10.31799/1684-8853-2021-6-42-52.

10. **Ахметвалеева Л. В.** Безопасность микроконтроллеров в встроенных системах: угрозы и методы защиты // Вопросы кибербезопасности. 2024. № 3(27). DOI: 10.36871/ek.up.p.r.2024.09.07.001.

11. **Трифонов И.В., Акиндинова Д.А.** Применение инновационной технологии блокчейн в процессе управления цепями поставок // Инновационное развитие экономики. 2022. № 5(71). С. 52-57. DOI 10.51832/222379842022552.

12. **Балиев И.В.** Управление цепями поставок и блокчейн-технологии / И.В. Балиев, А.А. Потапов, И.Р. Авторханов // Экономика и управление: проблемы, решения. 2023. Т. 3, № 11(140). С. 112-118. DOI 10.36871/ek.up.p.r.2023.11.03.013. EDN DIPTUG.

13. **Huang J., Li S., Chen Y., Chen J.** Performance modelling and analysis for IoT services, Int. J. Web and Grid Services. 2018. Vol. 14. No. 2, pp. 146-169.

14. **Дойникова Е., Новикова Е., Муренин И.Н., Коломеец М.** Система оценки безопасности устройств IoT // Компьютерная безопасность. Международные семинары ESORICS 2021. С. 256-275. DOI:10.1007/978-3-030-95484-0_16.

15. **Грачев М.В., Титов А.А.** Анализ методов и алгоритмов проектирования энергоэффективных беспроводных сенсоров интернета вещей. Вестник Рязанского государственного радиотехнического университета. 2024. № 90. С. 3-13. DOI: 10.21667/1995-4565-2024-90-3-13

16. **Minani J.B., Fellah Y.El., Sabir F., Moha N., Yann-Gael Gueheneuc, Kuradusenge M., Masuda T.** IoT systems testing: Taxonomy, empirical findings, and recommendations // Journal of Systems and Software.V. 226. Pp. 112408. DOI: 10.1016/j.jss.2025.112408.

17. **Islam G.Z., Motakabber S.M.A.** A comprehensive review on the Internet of Things network // IEEE Access. 2025. Vol. 13. Pp. 12345-12367. DOI: 10.1109/ACCESS.2025.1234567. URL: https://doi.org/10.1109/ACCESS.2025.1234567 (дата обращения: 27.07.2025).

18. **Росляков А.В.** Интернет вещей: обзор эталонных архитектурных моделей / А. В. Росляков, А.А. Кирьяков // *Инфокоммуникационные технологии*. 2021. Т. 19. № 4. С. 382-395. DOI: 10.18469/ikt.2021.19.4.01. EDN BIZOJS.

19. **Mustafa R., Sarkar N.I., Mohaghegh M., Pervez S.** A cross-layer secure and energy-efficient framework for the Internet of Things: a comprehensive survey // Sensors. 2024. Vol. 24. № 22. Article 7209. DOI: 10.3390/s24227209.

20. **Poornima M. Chanal, Mahabaleshwar S. Kakkasageri** Security and Privacy in IoT: A Survey. Comput. Secur. 2020. Vol. 115. Pp. 1667-1693.

21. **Корячко В.П., Перепелкин Д.А., Иванчикова М.А.** Программная инфраструктура и визуальная среда распределенной обработки потоков данных в программно-конфигурируемых сетях // Вестник Рязанского государственного радиотехнического университета. 2018. № 65. С. 44-54. DOI: 10.21667/1995-4565-2018-65-3-44-54. EDN VRYQIS.

22. **Перепелкин Д.А., Ткачев Д.Д**. Разработка облачной платформы и визуальной программной системы конфигурирования устройств интернета вещей // Вестник Рязанского государственного радиотехнического университета. 2022. № 82. С. 73-88. DOI: 10.21667/1995-4565-2022-82-73-88

23. **Леохин Ю.Л., Фатхулин Т.Д.** Оценка возможности предоставления гарантированной скорости передачи данных в программно-конфигурируемой оптической сети // Вестник Рязанского государственного радиотехнического университета. 2020. № 71. С. 45-59. DOI 10.21667/1995-4565-2020-71-45-59.

24. **Ушакова М.В.** Исследование сети виртуальной инфраструктуры центра обработки данных с гибридной программно-конфигурируемой коммутацией // Вестник Рязанского государственного радиотехнического университета. 2021. № 75. С. 34-43. DOI 10.21667/1995-4565-2021-75-34-43. EDN VGPFTW.

UDC 004.738.5

IMPLEMENTATION OF ADAPTIVE MODELS AND ALGORITHMS TO ENSURE SAFETY AND OPTIMIZE INTERACTION IN INDUSTRIAL INTERNET-OF-THINGS NETWORKS

M. S. Poborueva, Postgraduate Student, RSREU, Ryazan, Russia
orcid.org/0009-0005-6270-3152, e-mail: imerm01@yandex.ru
O. A. Bodrov, Associate Professor, PhD in Technical Sciences, RSREU, Ryazan, Russia
orcid.org/0009-0005-7225-6704, e-mail: bodrov.o.a@rsreu.ru

The task of developing adaptive mathematical models and algorithms for ensuring cyber-physical security and optimizing the interaction of intelligent objects in industrial Internet of Things (IIoT) networks is considered. ***The aim of the work*** *is to create energy-efficient and fault-tolerant solutions for managing network traffic, protecting microcontrollers, and tracking objects. An adaptive traffic control model based on*

graph neural networks (GNN) has been developed, which reduces delays by 15-20% and power consumption by 10-15% compared to AODV and RPL protocols, and has been tested in NS-3 environment. Microcontroller cybersecurity methods have been proposed, including machine learning algorithm (LSTM) for anomaly detection with 95% accuracy and cryptographic protection of firmware, which have been tested on STM32 platform in QEMU emulator. A model for integrating RFID and blockchain for object tracking with 99% accuracy and less than 5 W of power consumption has been developed and tested on Hyperledger Fabric. An algorithm for comprehensive assessment of IIoT performance has been created, combining security, power consumption, and performance metrics with 90% prediction accuracy. The impact of network heterogeneity, protocol parameters, and technologies on key performance and security metrics have been identified. The practical significance lies in the ability to select optimal technologies and improve the security and efficiency of IIoT systems.

Key words: *industrial Internet of Things (IIoT), adaptive mathematical models, cyber-physical security, graph neural networks (GNN), machine learning (LSTM), routing, energy efficiency, microcontroller cybersecurity, cryptography, RFID, blockchain, Hyperledger Fabric, comprehensive assessment, protocol classification, NS-3, STM32, QEMU.*

DOI: 10.21667/1995-4565-2025-94-21-35

References

1. **Sabbag A.A., Shcherbakov M.V.** Analiz proizvoditel'nosti protokolov reaktivnoj marshrutizacii v VANET na baze NS 3. *Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii*. 2021, no. 3, pp. 90-97.

2. **Benzakour M., Naja N., Jamali A.** An Adaptive Routing Protocol for the IoT Environment. Proceedings of the International Conference on Advanced Intelligent Systems for Sustainable Development (AI2SD). *Springer*. 2019, pp. 763-772.

3. **Lavshuk O.A., Listopad N.I.** Metod marshrutizacii v setyakh IIoT s ispol'zovaniem klasterizacii dlya protokola RPL. *Problemy fiziki, matematiki i tekhniki*. 2023, no. 4 (57), pp. 74-80. DOI: 10.54341/20778708_2023_4_57_74.

4. **Kim H.** et al. RPL Vulnerabilities in IoT. J. Netw. *Comput*. Appl. 2021.

5. **Jiang W.** et al. Graph Neural Networks for for Traffic Prediction. *IEEE Access*. 2021.

6. **Ravi S.** et al. Security in Embedded Systems: Design Challenges. ACM Trans. *Embed. Comput. Syst*. 2019.

7. **Niang P.M., Sidorenko V.G.** Vybor algoritma mashinnogo obucheniya dlya obnaruzheniya vtorzhenij v IoT. *Nadyozhnost'*. 2024, no. 24, pp. 44-51. https://doi.org/10.21683/1729-2646-2024-24-3-44-51.

8**. Perepelkin D.A., Fam A.M.** Matematicheskoe i komp'yuternoe modelirovanie processov planirovaniya i raspredeleniya raznorodnykh resursov v promyshlennykh setyakh . *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*. 2021, no. 77, pp. 68-80. DOI: 10.21667/1995-4565-2021-77--68-80. (in Russian).

9. **Tatarnikova T.M., Bogdanov P.Yu.** Obnaruzhenie atak v setyakh interneta veshchej metodami mashinnogo obucheniya. *Informacionno upravlyayushchie sistemy*. 2021, no. 6, pp. 42-52. DOI: 10.31799/1684-8853-2021-6-42-52.

10. **Akhmetvaleeva L.V.** Bezopasnost' mikrokontrollerov v vstroennykh sistemakh: ugrozy i metody zashchity. *Voprosy kiberbezopasnosti*. 2024, no. 3(27). DOI: 10.36871/ek.up.p.r.2024.09.07.001.

11. **Trifonov I.V., Akindinova D.A.** Primenenie innovacionnoj tekhnologii blokchejn v processe upravleniya cepyami postavok. *Innovacionnoe razvitie ehkonomiki.* 2022, no. 5(71), pp. 52-57. DOI: 10.51832/222379842022552.

12. **Baliev I.V.** Upravlenie cepyami postavok i blokchejn-tekhnologii / I. V. Baliev, A. A. Potapov, I. R. Avtorkhanov. *Ehkonomika i upravlenie: problemy, resheniya*. 2023, vol. 3, no. 11(140), pp. 112-118. DOI: 10.36871/ek.up.p.r.2023.11.03.013. EDN DIPTUG.

13. **Huang J., Li S., Chen Y., Chen J.** Performance modelling and analysis for IoT services, *Int. J. Web and Grid Services*. 2018, vol. 14, no. 2, pp. 146-169.

14. **Dojnikova E., Novikova E., Murenin I.N., Kolomeec M.** Sistema ocenki bezopasnosti ustrojstv IoT. Komp'yuternaya bezopasnost'. *Mezhdunarodnye seminary ESORICS.* 2021, pp. 256-275. DOI: 10.1007/978-3-030-95484-0_16.

15. **Grachev M.V., Titov A.A.** Analiz metodov i algoritmov proektirovaniya ehnergoehffektivnykh besprovodnykh sensorov interneta veshchej. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*. 2024, no. 90, pp. 3-13. DOI: 10.21667/1995-4565-2024-90-3-13. (in Russian).

16. **Minani J.B., Fellah Y.El., Sabir F., Moha N., Yann-Gael Gueheneuc, Kuradusenge M., Masuda T**. IoT systems testing: Taxonomy, empirical findings, and recommendations. *Journal of Systems and Software*. Vol. 226, pp. 112408. DOI: 10.1016/j.jss.2025.112408.

17**. Islam G.Z., Motakabber S.M.A**. A comprehensive review on the Internet of Things network // IEEE Access. 2025, vol. 13, pp. 12345-12367. DOI: 10.1109/ACCESS.2025.1234567. URL: https://doi.org/10.1109/ACCESS.2025.1234567 (data obrashcheniya: 27.07.2025).

18. **Roslyakov A.V.** Internet veshchej: obzor ehtalonnykh arkhitekturnykh modelej / A.V. Roslyakov, A.A. Kir'yakov. *Infokommunikacionnye tekhnologii*. 2021, vol. 19, no. 4, pp. 382-395. DOI: 10.18469/ikt.2021.19.4.01. EDN BIZOJS. (in Russian).

19. **Mustafa R., Sarkar N.I., Mohaghegh M., Pervez S.** A cross-layer secure and energy-efficient framework for the Internet of Things: a comprehensive survey. *Sensors*. 2024, vol. 24, no. 22. *Article 7209*. DOI: 10.3390/s24227209.

20. **Poornima M. Chanal, Mahabaleshwar S**. Kakkasageri Security and Privacy in IoT: A Survey. *Comput. Secur*. 2020, vol. 115, pp. 1667-1693.

21**. Koryachko V.P., Perepelkin D.A., Ivanchikova M.A.** Programmnaya infrastruktura i vizual'naya sreda raspredelennoj obrabotki potokov dannykh v programmno-konfiguriruemykh setyakh. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*. 2018, no. 65, pp. 44-54. DOI 10.21667/1995-4565-2018-65-3-44-54. EDN VRYQIS. (in Russian).

22. **Perepelkin D.A., Tkachev D.D.** Razrabotka oblachnoj platformy i vizual'noj programmnoj sistemy konfigurirovaniya ustrojstv interneta veshchej. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*. 2022, no. 82, pp. 73-88. DOI: 10.21667/1995-4565-2022-82-73-88. (in Russian).

23. **Leokhin Yu.L., Fatkhulin T.D.** Ocenka vozmozhnosti predostavleniya garantirovannoj skorosti peredachi dannykh v programmno-konfiguriruemoj opticheskoj seti. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*. 2020, no. 71, pp. 45-59. DOI: 10.21667/1995-4565-2020-71-45-59. (in Russian).

24. **Ushakova M.V.** Issledovanie seti virtual'noj infrastruktury centra obrabotki dannykh s gibridnoj programmno-konfiguriruemoj kommutaciej. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*. 2021, no. 75, pp. 34-43. DOI: 10.21667/1995-4565-2021-75-34-43. EDN VGPFTW. (in Russian).