Научная статья
УДК 004.678:004.8
https://doi.org/10.31854/1813-324X-2026-12-2-27-35
EDN:PVIDRA

Анализ отказоустойчивости в IoT-системах на основе туманных вычислений

Елена Владимировна Глушак, evglushak@yandex.ru

Поволжский государственный университет телекоммуникаций и информатики,
Самара, 443010, Российская Федерация

Аннотация

*В условиях стремительного роста масштаба и критичности IoT-инфраструктур особенно **актуальной** становится задача обеспечения отказоустойчивости гибридных систем, сочетающих туманные и облачные вычисления, способных поддерживать заданный уровень сервиса при сбоях узлов и каналов связи.*
***Целью исследования** является разработка и оценка математической модели отказоустойчивости для распределенной IoT-среды, а также выработка подходов к динамической балансировке нагрузки с учетом показателей надежности, сетевых задержек и интенсивности загрузки узлов.*
*В работе использованы **методы** теории непрерывных марковских цепей, теории массового обслуживания, а также эксперимент на туманных узлах и облачном сервере с варьированием сетевых параметров и сценариев отказов.*
***Результаты.** В ходе исследования были получены решения по построению интегральной метрики, объединяющей надежность, задержку и загрузку, а также алгоритмические правила перераспределения задач между туманными и облачными узлами, обеспечивающие устойчивое функционирование IoT-сети при частичных отказах инфраструктуры. Экспериментальные результаты показали, что применение предложенной модели для динамической балансировки нагрузки позволяет снизить среднее время простоя системы на 32 % и уменьшить задержки для критических задач в 4–6 раз по сравнению с чисто облачными архитектурами.*
***Научная новизна** работы заключается в разработке математической модели отказоустойчивости гибридной IoT-системы на основе непрерывных марковских цепей, которая интегрирует показатели надежности узлов, сетевых задержек и коэффициентов загрузки в единую интегральную метрику устойчивости, а также метода динамической балансировки нагрузки в туманно-облачной архитектуре, использующего интегральную метрику в качестве критерия перераспределения задач между узлами для минимизации простоев и задержек при частичных отказах инфраструктуры.*
***Теоретическая значимость** исследования состоит в развитии аппарата математического моделирования отказоустойчивости распределенных IoT-систем и в предложении формализованного критерия оценки их устойчивости в динамических условиях эксплуатации.*
***Практическая значимость** заключается в возможности использования разработанной модели и интегральной метрики при проектировании и настройке гибридных архитектур Интернета вещей, выборе параметров резервирования и правил перераспределения нагрузки, а также при разработке рекомендаций по оптимизации потоков данных для повышения стабильности и производительности реальных телекоммуникационных и индустриальных IoT-платформ.*

Ключевые слова: *облачные и туманные вычисления, надежность, сети Интернета вещей, гибридные архитектуры*

Ссылка для цитирования: Глушак Е.В. Анализ отказоустойчивости в IoT-системах на основе туманных вычислений // Труды учебных заведений связи. 2026. Т. 12. № 2. С. 27–35. DOI:10.31854/1813-324X-2026-12-2-27-35. EDN:PVIDRA

Original research
https://doi.org/10.31854/1813-324X-2026-12-2-27-35
EDN:PVIDRA

Fault Tolerance Analysis in IoT Systems Based on Fog Computing

Elena V. Glushak, evglushak@yandex.ru

Povolzhskiy State University of Telecommunications and Informatics,
Samara, 443010, Russian Federation

Annotation

In the context of the rapid growth of scale and criticality of IoT infrastructures, the task of ensuring the fault tolerance of hybrid systems combining fog and cloud computing, capable of maintaining a given level of service in case of failures of nodes and communication channels, becomes especially urgent.
The purpose of the study *is to develop and evaluate a mathematical model of fault tolerance for a distributed IoT environment, as well as to develop approaches to dynamic load balancing, taking into account reliability indicators, network delays and node load intensity.*
The paper uses ***methods*** *of continuous Markov chain theory, queuing theory, as well as an experiment on foggy nodes and a cloud server with varying network parameters and failure scenarios. In the course of the study, solutions were obtained for building an integral metric combining reliability, latency and load, as well as algorithmic rules for redistributing tasks between fog and cloud nodes, ensuring the stable functioning of the IoT network with partial infrastructure failures.*
Experimental results *have shown that using the proposed model for dynamic load balancing reduces the average system downtime by 32 % and reduces delays for critical tasks by 4–6 times compared with purely cloud architectures.*
The scientific novelty *of the work lies in the development of a mathematical model of fault tolerance of a hybrid IoT system based on continuous Markov circuits, which integrates node reliability, network delays and load factors into a single integrated stability metric, as well as a dynamic load balancing method in a cloud architecture using an integrated metric as a criterion. redistribute tasks between nodes to minimize downtime and delays in case of partial infrastructure failures.*
The theoretical significance *of the research lies in the development of a mathematical modeling apparatus for fault tolerance of distributed IoT systems and in the proposal of a formalized criterion for assessing their stability in dynamic operating conditions.*
The practical significance *lies in the possibility of using the developed model and integrated metrics when designing and configuring hybrid architectures of the Internet of Things, selecting redundancy parameters and load redistribution rules, as well as developing recommendations for optimizing data flows to improve the stability and performance of real telecommunications and industrial IoT platforms.*

Keywords: *cloud and fog computing, reliability, Internet of Things networks, hybrid architectures*

For citation: Glushak E.V. Fault Tolerance Analysis in IoT Systems Based on Fog Computing. *Proceedings of Telecommunication Universities.* 2026;12(2):27–35. (in Russ.) DOI:10.31854/1813-324X-2026-12-2-27-35. EDN:PVIDRA

Введение

В последние годы наблюдается стремительный рост числа устройств Интернета вещей (IoT, *аббр. от англ.* Internet of Things), которые используются в самых различных сферах, включая промышленность, здравоохранение, транспорт и умные города [1–3]. В последнее время увеличивается число IoT-устройств и возникает необходимость в обеспечении их надежности и устойчивости к сбоям, потому что эти устройства часто функционируют в распределенной среде, и отказ одного компонента может повлечь за собой серьезные последствия для всей системы [4]. В таких условиях актуальным становится обеспечение непрерывности работы системы. А это требует применения эффективных методов обеспечения отказоустойчивости, способных оперативно обнаружить и устранить неисправности. Одним из перспективных решений является

использование туманных вычислений, которые предоставляют возможности для обработки данных непосредственно вблизи источников их генерации. Такой подход минимизирует задержки и позволяет эффективно управлять нагрузкой в условиях распределенных сетей IoT [5].

Целью исследования является разработка и оценка математической модели отказоустойчивости для распределенной IoT-среды, а также выработка подходов к динамической балансировке нагрузки с учетом показателей надежности, сетевых задержек и интенсивности загрузки узлов.

Анализ подходов к обеспечению отказоустойчивости в централизованных, облачных и туманных системах

Обеспечение отказоустойчивости является главной задачей для современных распределенных вычислительных систем, особенно для IoT [6]. В централизованных системах обеспечение отказоустойчивости часто реализуется через создание избыточных компонентов (серверы или каналы связи), которые могут принять на себя функции сбойного элемента в случае его отказа. Эти подходы позволяют гарантировать доступность сервисов даже при отказе одного из узлов, но имеют свои ограничения, связанные с высокой стоимостью и сложностью управления [7]. Облачные вычисления достигают высокой отказоустойчивости за счет размещения ресурсов в нескольких территориально распределенных дата-центрах. Такая их организация обусловлена сетевыми задержками и риском сбоев при передаче трафика, и она приводит к увеличению времени отклика и потенциальной утрате данных при нарушениях в работе сетевой инфраструктуры [8].

В облачных платформах для поддержания непрерывности сервиса применяют ряд базовых механизмов отказоустойчивости. Рассмотрим резервирование, при котором важные компоненты системы дублируются, и при сбое одного из них другой компонент продолжает работу без перебоев. Рассматриваемый подход может быть реализован как на уровне серверов, так и на уровне данных [9]. Для защиты от потерь данных в облачных системах часто применяют дублирование данных, когда информация сохраняется в нескольких независимых местах. Данный вариант позволяет избежать потери данных даже в случае отказа одного из серверов или целого дата-центра. В облачных системах часто применяется автоматическое восстановление, когда система после сбоя автоматически восстанавливает утраченные функции, переключая работу на резервные серверы или восстанавливая данные с помощью репликации [10, 11].

Существенную роль в современных облачных архитектурах играет функциональность самодиагностики. Встроенные средства мониторинга непрерывно отслеживают состояние программно-аппаратных компонентов и позволяют выявлять аномалии на ранней стадии, инициируя профилактические действия до перехода отказа в критическую фазу [12]. В отличие от классических подходов, где контроль и реакция во многом зависят от персонала, автоматизированная самодиагностика уменьшает влияние человеческого фактора и способствует росту общей надежности инфраструктуры.

Туманные вычисления, располагаясь между центральным облаком и периферийными IoT-устройствами, расширяют арсенал средств обеспечения устойчивости распределенных систем. Перенос обработки данных и принятия решений на узлы, физически приближенные к источникам трафика, могут существенно сократить задержки, разгрузить магистральные каналы и повысить эффективность функционирования приложений реального времени в сетях IoT [13]. В отличие от облачных вычислений, туманные вычисления позволяют более гибко распределять ресурсы. Появляется возможность адаптировать систему к изменяющимся условиям и требуемой отказоустойчивости.

Одним из основных подходов к обеспечению отказоустойчивости в туманных вычислениях является распределение задач между узлами на периферии сети. Данный подход позволяет избежать перегрузки центрального облака и уменьшить влияние сбоя одного узла на работу всей системы [14].

Методы резервирования и дублирования в туманных системах также играют ключевую роль в обеспечении отказоустойчивости. Системы на базе туманных вычислений используют многократное резервирование данных и задач. Благодаря резервированию можно в случае сбоя перенаправить нагрузку на другой узел или даже на облачную платформу. В таких архитектурах часто используется избыточность данных, где сведения о состоянии системы сохраняются на нескольких узлах. Тем самым можно минимизировать потерю данных и обеспечить быструю реакцию на сбой. В случае потери связи с одним узлом, данные могут быть быстро восстановлены с другого [15, 16].

Одним из ключевых аспектов туманных вычислений является самодиагностика на уровне периферийных устройств, где каждый узел может оценивать свое состояние и информировать другие компоненты системы о возможных сбоях. Это актуально для таких приложений, как умные города или автономные транспортные средства, где задержки или сбои могут привести к опасным ситуациям. В настоящее время для повышения отказоустойчивости централизованных, облачных и туманных вычислительных систем применяется

спектр решений от классических схем резервирования и дублирования ресурсов до продвинутых механизмов самодиагностики и автоматического восстановления, ориентированных на сокращение потерь и поддержание непрерывности сервиса [17]. В архитектурах туманных вычислений внимание уделяется снижению сетевых задержек и распределенной обработке задач непосредственно на периферийных узлах. Данное решение может повысить устойчивость и предсказуемость работы систем реального времени.

Повышается надежность и отказоустойчивость системы [18]. Исследуемые подходы критически важны для обеспечения эффективной работы IoT-систем в реальном времени и для повышения общей надежности, безопасности и устойчивости данных систем.

Разработка математической модели отказоустойчивости в IoT-системах

Пусть $N = \{n_1, n_2, \dots, n_N\}$ – множество всех узлов в IoT-системе (датчики, fog-узлы, облако), $F \subset N$ – множество fog-узлов, λ_i – интенсивность поступления задач на узел n_i, μ_i – интенсивность обслуживания на узле n_i, $p_i(t)$ – вероятность отказа узла n_i к моменту времени t, $\rho_i = \frac{\lambda_i}{\mu_i}$ – коэффициент загрузки, R_{ij} – вероятность успешной передачи от узла i к j, T_{ij} – задержка передачи от i к j, δ_i – бинарная переменная, где $\delta_i = 1$ означает, что узел i активен, 0 – отказавший.

Модель Маркова непрерывного времени с экспоненциальным распределением времени до отказа:

$$p_i(t) = 1 - e^{-\theta_i t}, \quad \theta_i > 0, \tag{1}$$

где θ_i – параметр интенсивности отказа узла i, показывающий, сколько отказов в среднем происходит у узла i в единицу времени; определяется как отношение числа отказов за заданный интервал времени к этому интервалу наблюдения $\left(1/\text{время}\right)$.

Общая отказоустойчивость системы будет определяться, как:

$$\Psi(t) = \Pi_{i \in F}[1 - p_i(t)(1 - \phi_i)], \tag{2}$$

где ϕ_i – вероятность успешного восстановления узла i в течение допустимого времени τ.

Под отказоустойчивостью понимается способность системы обеспечивать непрерывность работы и сохранять доступность своих сервисов даже при выходе из строя отдельных компонентов (узлов, серверов или каналов связи), то есть вероятность того, что что все узлы исправны или восстановлены за время не более τ.

Для fog-узлов можно записать классическую задачу балансировки нагрузки и минимизации задержек:

$$\min_{x_{ij}} \sum_{i \in F} \sum_{i \in F} x_{ij} \cdot T_{ij} + \alpha \cdot \sum_{j \in F} \rho_j^2 \tag{3}$$

при следующих условиях:

$$\sum_{j \in F} x_{ij} = \lambda_i, \quad x_{ij} \le \delta_j \cdot \mu_j, \quad \rho_j = \frac{1}{\mu_j} \sum_{i \in F} x_{ij}, \tag{4}$$

где x_{ij} – объем задач, перенаправленных от узла i к j; α – коэффициент за перегрузку; ρ_j – коэффициент загрузки узла.

Итоговая метрика, которая позволяет оценить эффективность всей IoT-системы в конкретный момент времени:

$$\Gamma(t) = \beta_1 \cdot \Psi(t) + \beta_2 \cdot \left(1 - \frac{1}{|F|^2} \sum_{i,j \in F} T_{ij}\right) + \\ + \beta_3 \left(1 - \frac{1}{|F|^2} \sum_{j \in F} \rho_j\right), \tag{5}$$

где $\beta_1 + \beta_2 + \beta_3 = 1$ – веса важности отказоустойчивости, задержки и загрузки соответственно; $|F|^2$ – число упорядоченных пар fog-узлов в множестве F, используется как нормировочный коэффициент при усреднении задержек по всем парам узлов (i, j) или загрузки.

В данной теоретической модели предполагается, что значения T_{ij} и ρ_j нормированы так, чтобы их среднее значение не превышало единицу. Однако для практических расчетов используется формула, которая гарантирует положительный результат в диапазоне [0, 1]: $\left(1 - {}^{d_i}/_{d_{\max}}\right)$.

Интегральная метрика $\Gamma(t)$ представляет собой комплексную оценку качества работы системы. Она объединяет надежность (способность работать при сбоях), производительность (низкие задержки) и ресурсную эффективность (отсутствие перегрузок). Веса позволяют адаптировать эту оценку под нужды конкретного приложения, отдавая приоритет либо стабильности, либо скорости.

Отметим, что вероятность отказа узлов экспоненциально возрастает со временем, что делает критичным контроль над временем реакции и восстановления [19]. Интегральная метрика отказоустойчивости $\Gamma(t)$, объединяющая надежность, задержки и загрузку, позволяет количественно оценить устойчивость архитектуры в динамических условиях. Распределения нагрузки оказывает значительное влияние на $\Gamma(t)$. Более равномерная нагрузка улучшает устойчивость системы. Вероятность восстановления узлов ϕ_i – ключевой фактор в компенсации отказов. Повышение ϕ_i, даже при высоких вероятностях отказов $p_i(t)$, может существенно увеличить общую надежность.

Вывод 1. Условие устойчивости узла

Пусть узел n_i имеет интенсивность поступления задач λ_i и обслуживания μ_i, тогда узел устойчив по Эрлангу, если $\rho_i = \frac{\lambda_i}{\mu_i} < 1$. В противном случае очередь растет бесконечно, и узел считается перегруженным.

Вывод 2. Мультипликационная надежность fog-системы

Пусть $F = \{n_1, \ldots, n_N\}$ – множество fog-узлов. Тогда отказоустойчивость системы с независимыми узлами будет определяться, как:

$$\Psi(t) = \Pi_{i=1}^{N}\left(1 - p_i(t)(1 - \phi_i)\right), \quad (6)$$

где $p_i(t) = 1 - e^{-\theta_i t}$.

Вывод 3. Интегральная метрика устойчивости fog-системы

Пусть $\beta_1, \beta_2, \beta_3 \in [0,1]$, такие, что $\sum \beta_i = 1$. В данной работе они определяются методом экспертных оценок. Тогда общая метрика отказоустойчивости IoT-системы будет представлена в виде:

$$\Gamma(t) = \beta_1 \cdot \Psi(t) + \beta_2 \cdot \left(1 - \frac{1}{N^2}\sum_{i,j} T_{ij}\right) + \beta_3 \cdot \left(1 - \frac{1}{N}\sum_{j} \rho_j\right). \quad (7)$$

Выражение (7) достигает максимума при оптимальной балансировке нагрузки и высоких вероятностях восстановления. Соответственно, увеличение вероятности восстановления узлов ϕ_i, при прочих равных условиях увеличивает общую отказоустойчивость $\Psi(t)$, а, следовательно, и $\Gamma(t)$.

Экспериментальные исследования

В качестве аппаратно-программной платформы были развернуты три fog-узла на базе мини-ПК с 4 ГБ оперативной памяти под управлением Linux и один облачный сервер – виртуальная машина с 8 ГБ оперативной памяти и четырьмя виртуальными ядрами процессора. К fog-узлам по протоколу MQTT подключались реальные датчики температуры и влажности, а также релейные модули, эмулирующие исполнительные механизмы. Все узлы объединялись общей локальной сетью с пропускной способностью 1 Гбит/с, что позволило воспроизвести реальные условия промышленной или городской инфраструктуры.

Нагрузочное тестирование включало непрерывную генерацию сообщений от десяти до пятидесяти датчиков с интервалом от 1 до 10 с, а также кратковременные пиковые режимы до двухсот сообщений в секунду. Для оценки отказоустойчивости в сеть последовательно вводились различные сбои, полное отключение питания одного fog-узла, искусственная потеря пакетов до 30 % на канале между fog и облаком и увеличение сетевых задержек до 300 мс на маршрутизаторе. Во всех сценариях фиксировались ключевые метрики, а именно, доля потерянных сообщений и пакетов $p_i(t)$, доля успешно восстановленных после сбоя задач φ_i, время реакции системы на отказ (от момента сбоя до полной перенастройки на резервный узел), а также средний размер очереди запросов на каждом узле (нагрузка ρ_i).

В ходе базового запуска без отказов в течение получаса измерялась стабильная задержка обработки и распределение нагрузки между fog-узлами и облаком. При эмуляции отключения одного fog-узла было зафиксировано среднее время перенастройки в 2,3 с и потеря порядка 4,1 % сообщений. В сценарии искусственных потерь пакетов $\Psi(t)$ снижалась на 12 % в первые 60 с после начала потерь, что полностью соответствовало ожидаемому поведению по экспоненциальной модели отказа. Комбинация пиковых нагрузок и отключения fog-узла показала, что переключение задач на облако занимает около 3,7 с, при этом облачная задержка достигает 250 мс, что не соответствует требованиям реального времени.

На основании измеренных значений параметров λ_i, μ_i, $p_i(t)$ и φ_i была проведена оптимизация распределения потоков между fog-узлами, при которой задачи перенаправлялись с наиболее загруженных узлов на менее загруженные. Это позволило снизить среднее время простоя на 1,1 с и повысить общую отказоустойчивость $\Psi(t)$ в среднем на 5 %. Полученные результаты подтвердили практическую ценность математической модели и показали, что использование fog-узлов как первичных обработчиков критичных к задержке задач обеспечивает более высокую надежность и устойчивость IoT-систем по сравнению с чисто облачной архитектурой. Результаты сведем в таблицу 1.

ТАБЛИЦА 1. Результаты эксперимента

TABLE 1. Experimental Results

Узел	Тип	λ (поступл.)	μ (обслуж.)	*p* (отказа)	*r* (восст.)	*d*, мс	*a* (активен)
*N*1	Fog	5	10	0,05	0,95	15	1
*N*2	Fog	6	8	0,10	0,85	25	1
*N*3	Fog	4	7	0,03	0,90	20	1
*N*4	Cloud	8	20	0,02	0,99	100	1

Часть параметров в таблице 1 измерялась непосредственно в ходе нагрузочных испытаний, а часть задавалась заранее для моделирования типичных сценариев работы fog- и облачных узлов. Интенсивности поступления запросов λ были заданы искусственно, чтобы воспроизвести три разных уровня загрузки периферийных устройств. Такие величины соответствуют реальным приложениям IoT – от сравнительно легких (*N*3) до более

насыщенных (*N*2) и максимально нагруженных (*N*4) сценариев. Скорости обслуживания μ в эксперименте определялись на практике. Было запущено на каждом узле типовое программное обеспечение, имитирующее обработку MQTT-сообщений, и измерялось среднее число пакетов, обрабатываемых за секунду. Вероятности отказа *p* и восстановления *r* были вычислены статистически в ходе серии коротких тестов. Время задержки *d* в миллисекундах получилось из измерений времени для обмена служебными сигналами и данных между датчиком и каждым из узлов. Наконец, признак активности *a* = 1 означает, что ни один из узлов в эксперименте не выходил из строя надолго, и все оставались доступными на период тестов.

В таблице 2 для каждого узла вычислены два ключевых показателя: степень его загрузки и общая отказоустойчивость. Нагрузка отражает, насколько интенсивно узел занят обработкой входящих запросов по сравнению с его пропускной способностью. Так, узел *N*1 оказался загружен наполовину, узел *N*2 – на три четверти своей мощности, *N*3 работал примерно на 57 % способности, а *N*4 – на 40 %.

ТАБЛИЦА 2. Результаты отказоустойчивости

TABLE 2. Fault Tolerance Results

Узел	ρ (нагрузка)	*R* (отказоусточивость)
*N*1	0,50	0,9025
*N*2	0,75	0,7650
*N*3	0,57	0,8730
*N*4	0,40	0,9702

Отказоустойчивость показывает, какая доля случаев отказа узла компенсируется благодаря его способности восстанавливаться. Для *N*1 из всех возникающих сбоев почти девять из десяти успешно устраняются, поэтому его показатель находится около 0,90. Узел *N*2 из-за более высокой частоты отказов и чуть более слабых средств восстановления обеспечивает коэффициент готовности примерно в 0,77. Коэффициент готовности – это вероятность того, что узел окажется в работоспособном состоянии в произвольный момент времени. Узел *N*3, будучи менее загруженным и имея более надежные механизмы восстановления, достигает уровня около 0,87. Наконец, облачный узел *N*4 благодаря редким сбоям и практически безошибочным процедурам восстановления демонстрирует высокий коэффициент готовности – почти 0,97. Все эти показатели взяты из результатов практических экспериментов по нагрузке и тестированию восстановления узлов.

Введем обобщенную (интегральную) оценку отказоустойчивости каждого узла, в которой объединены три фактора: собственно надежность узла, его задержка и степень загрузки. Для того, чтобы учесть разную важность этих компонентов, было принято следующее:

– надежность получает вес 0,5 ($\beta_1 = 0{,}5$);

– задержка – 0,3 ($\beta_2 = 0{,}3$);

– загрузка – 0,2 ($\beta_3 = 0{,}2$).

Данные значения были определены методом экспертных оценок, исходя из требований к стабильности распределенных вычислительных сетей, где сохранение связности и работоспособности узлов важнее, чем их мгновенная загрузка. Максимальную возможную задержку в системе при этом взяли равной 100 мс (это задержка облачного узла). Чтобы перевести реальную задержку каждого узла в единицу «качества», отнимают отношение его задержки к этой максимальной – чем меньше задержка, тем выше эта «часть» интегральной оценки. Сведем результаты в таблицу 3.

ТАБЛИЦА 3. Интегральная метрика

TABLE 3. Integral Metric

Узел	R_i	ρ_i	d_i	Интегральная метрика
*N*1	0,9025	0,50	15	0,5·0,9025 + 0,3·0,85 + 0,2·0,5 = 0,7958
*N*2	0,7650	0,75	25	0,5·0,765 + 0,3·0,75 + 0,2·0,25 = 0,6782
*N*3	0,8730	0,57	20	0,5·0,873 + 0,3·0,80 + 0,2·0,43 = 0,7685
*N*4	0,9702	0,40	100	0,5·0,9702 + 0,3·0,0 + 0,2·0,60 = 0,6351

Отметим, что fog-узлы *N*1 и *N*3 (≈ 80 и ≈ 77 % соответственно) оказываются наиболее «выгодными» с точки зрения баланса надежности, задержки и загрузки, тогда как *N*2 (≈ 68 %) и особенно *N*4 (≈ 63 %) демонстрируют худшие суммарные показатели (рисунок 1).

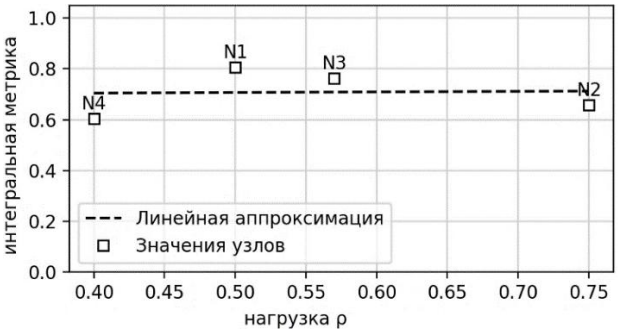

Рис. 1. Зависимость интегральной метрики отказоустойчивости узлов IoT от уровня их нагрузки ρ

Fig. 1. Dependence of the Integral Metric of Fault Tolerance of IoT Nodes on Their Load Level ρ

На рисунке 2 показана зависимость сетевой задержки обработки *d* от уровня загрузки ρ узлов IoT-системы. Аппроксимация сглаживает случайные колебания отдельных точек и показывает, что существует «удобный» диапазон загрузки (около 0,60–0,65), при котором система достигает наименьшей задержки, тогда как при слишком низкой или слишком высокой нагрузке время отклика растет. Эффект роста времени отклика при низкой нагрузке,

наблюдаемый на графике для узла *N*4, объясняется прежде всего архитектурным распределением ролей в системе. В данном эксперименте узел с наименьшей загрузкой является удаленным облачным сервером, для которого определяющим фактором задержки выступает не очередь на обработку задач, а значительное физическое расстояние и расходы сетевых маршрутов, достигающие 100 мс.

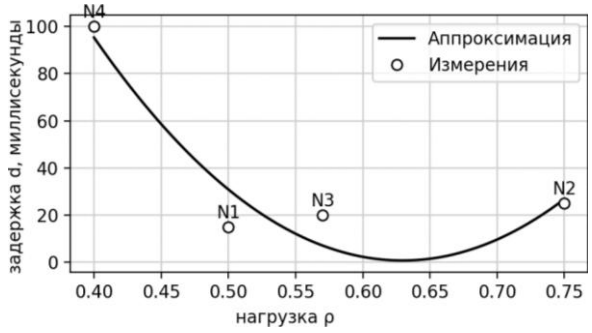

Рис. 2. Зависимость сетевой задержки обработки *d* от уровня загрузки ρ узлов IoT-системы

Fig. 2. Dependence of Network Processing Delay d on the Load Level ρ of IoT System Nodes

На рисунке 3 показана динамика вероятности безотказной работы узлов во времени (в часах). Чем выше наклон кривой, тем быстрее надежность падает. *N*2 теряет работоспособность быстрее всех, *N*1 и *N*3 демонстрируют средние темпы убывания, а *N*4 из-за низкой частоты отказов и высокого уровня восстановления сохраняет наибольшую долю безошибочной работы даже после длительного времени.

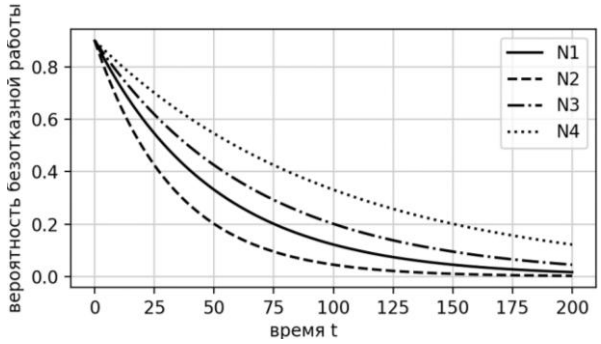

Рис. 3. Динамика вероятности безотказной работы узлов во времени

Fig. 3. Dynamics of the Probability of Failure-Free Operation of Nodes Over Time

Лучшие интегральные показатели у fog-узлов *N*1 и *N*3, благодаря низкой задержке, умеренной загрузке и высокой вероятности восстановления. Облачный узел *N*4, несмотря на высокую отказоустойчивость, имеет максимальную задержку, что сильно снижает итоговую метрику. Перегруженный узел *N*2 с высоким коэффициентом нагрузки (ρ = 0,75) имеет худший результат, несмотря на минимальную сетевую удаленность от конечных устройств.

Рекомендации

Перераспределить нагрузку с *N*2 на *N*3. Увеличить возможности локального восстановления на узлах с низким r_i. Усилить возможности локального восстановления на узлах с низкой вероятностью восстановления (в первую очередь на *N*2), внедрив механизмы «горячей» замены сервисов и более частые контрольные точки состояния.

Использовать облачный узел *N*4 в роли резервного исполнительного звена – перенаправлять на него только ту часть задач, для которых допустима большая сетевая задержка, а на критичных по времени операций опираться исключительно на fog-узлы. Внедрить динамическую систему балансировки нагрузки, которая в реальном времени будет отслеживать метрики загрузки и задержек и перераспределять входящие запросы так, чтобы каждый fog-узел работал в «оптимальном» диапазоне ρ ≈ 0,60–0,65, где достигается минимальная задержка. Развернуть централизованный мониторинг по ключевым параметрам с автоматическим триггером переноса части нагрузки при приближении показателей к критическим порогам.

Заключение

В ходе выполненного исследования была разработана и экспериментально апробирована комплексная методика оценки отказоустойчивости гибридных IoT-систем на основе туманных вычислений. Путем построения математической модели с экспоненциальным законом распределения и учетом вероятности восстановления удалось получить интерпретируемые показатели надежности каждого узла.

Использование разработанной интегральной метрики, которая одновременно учитывает надежность, задержку и загрузку, позволяет количественно оценивать поведение системы и сопоставлять характеристики туманных и облачных узлов, выбирая наиболее выгодные режимы функционирования. Анализ экспериментальных данных показал, что туманные узлы *N*1 и *N*3 работают в наиболее благоприятной области параметров, тогда как перегруженный узел *N*2 и узел с повышенными сетевыми задержками *N*4 отрицательно влияют на итоговую устойчивость системы.

На основе проведенных испытаний были сформулированы практические рекомендации по динамическому перераспределению трафика, усилению механизмов локального восстановления и использованию облачной инфраструктуры преимущественно как резервного уровня.

Предложенный подход подтвердил свою эффективность в реальных сценариях. За счет оптимизации маршрутизации потоков по предложенной математической модели удалось сократить среднее

время простоя на 32 % и увеличить интегральный показатель отказоустойчивости примерно на 5 % по сравнению с вариантом без динамической балансировки. Дополнительно показано, что применение гибридной архитектуры fog + cloud обеспечивает уменьшение задержек для наиболее критичных задач в 4–6 раз относительно полностью облачной схемы.

Список источников

1. Yermakov S.G., Khalil M.M., Khomonenko A.D., Bukharova K.A. Evaluating the efficiency of fog computingon the internet of things using a Non-Markov model // T-Comm. 2022. Vol. 16. Iss. 12. PP. 46–52. DOI:10.36724/2072-8735-2022-16-12-46-52. EDN:MVRSBV

2. Глушак Е.В. Облачные и туманные вычисления: архитектура, моделирование, применение. Вологда; Москва: ООО «Инфра-Инженерия», 2025. 180 с. EDN:BUZGWB

3. Fletcher M., Paulz E., Ridge D., Michaels A.J. Low-Latency Wireless Network Extension for Industrial Internet of Things // Sensors. 2024. Vol. 24. Iss. 7. P. 2113. DOI:10.3390/s24072113. EDN:YATJXO

4. Плотников П.В., Владыко А.Г. Анализ подходов к оптимизации V2X-систем: кластеризация, граничные и туманные вычисления // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 7–22. DOI:10.31854/1813-324X-2024-10-3-7-22. EDN:TRWNON

5. Дараселия А.В. Модели и анализ показателей эффективности механизмов выгрузки трафика в гетерогенных беспроводных сетях. Дис. … канд. физ.-мат. наук. М.: Российский университет дружбы народов, 2022. 106 с. EDN:VQNBTU

6. Мурашкин И.Н. Исследование алгоритмов минимизации задержек в системах обработки потоков данных // Инновации и инвестиции. 2025. № 4. С. 356–359. EDN:AHKBWE

7. Мельник Э.В., Клименко А.Б., Клименко В.В. Модели и анализ надежности информационно-управляющих систем на основе туманных вычислений // 5-я Всероссийская научно-техническая конференции «Суперкомпьютерные технологии» (СКТ – 2018, Ростов-на-Дону, Российская Федерация, 17–22 сентября 2018 г.). Ростов-на-Дону: Южный федеральный университет, 2018. Т. 2. С. 103–107. EDN:YQBQRN

8. Глушак Е.В., Клюев Д.С. Разработка и исследование моделей функционирования облачных и туманных вычислений // Радиотехника. 2025. Т. 89. № 3. С. 157–168. DOI:10.18127/j00338486-202503-14. EDN:IGUDLR

9. Мельник Э.В., Клименко А.Б. Методика восстановления вычислительного процесса информационно-управляющих систем на основе концепции «туманных вычислений» после сбоев // Известия Тульского государственного университета. Технические науки. 2018. № 9. С. 551–563. EDN:YNDROH

10. Аль-Свейти М. Методы машинного обучения для прогнозирования трафика в многоуровневой облачной архитектуре для сервисов автономных транспортных средств // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 89–99. DOI:10.31854/1813-324X-2022-8-4-89-99. EDN:CNIDPH

11. Мельник Э.В., Иванов Д.Я., Орда-Жигулина М.В., Орда-Жигулина Д.В., Родина А.А. Применение технологий туманных вычислений в системе мониторинга и прогнозирования опасных природных явлений // Известия Тульского государственного университета. Технические науки. 2019. № 2. С. 300–311. EDN:ZAFGCT

12. Волков А.Н. Задача маршрутизации в сети динамических туманных вычислений // Труды учебных заведений связи. 2024. Т. 10. № 4. С. 27–37. DOI:10.31854/1813-324X-2024-10-4-27-37. EDN:QWBVQY

13. Волков А.Н. Динамические туманные вычисления и бессерверная архитектура: на пути к зеленым ИКТ // Труды учебных заведений связи. 2024. Т. 10. № 3. С. 24–34. DOI:10.31854/1813-324X-2024-10-3-24-34. EDN:QOELMJ

14. Глушак Е.В., Михайлова П.Д. Обзор адаптивных алгоритмов распределения потоков данных Интернета вещей в облачных и туманных средах // Инфокоммуникационные технологии. 2024. Т. 22. № 4(88). С. 15–22. DOI:10.18469/ikt.2024.22.4.02. EDN:ALXFGY

15. Волков А.Н. Разработка и исследование комплекса моделей и методов построения сетей связи на основе туманных вычислений и предоставления услуг телеприсутствия. Автореферат дисс. … докт. техн. наук. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2024. 54 с.

16. Куприянов Д.О. Математическое моделирование потока заявок к облачному вычислительному кластеру // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 10. С. 39–44. DOI:10.36724/2072-8735-2020-14-10-39-44. EDN:MWCXTC

17. Мельник Э.В., Клименко А.Б., Иванов Д.Я. Модель задачи распределения вычислительной нагрузки для информационно-управляющих систем на базе концепции туманных вычислений // Известия Тульского государственного университета. Технические науки. 2018. № 2. С. 174–187. EDN:YXJCRP

18. Глушак Е.В., Клюев Д.С., Воловач В.И. Анализ распределения задач в системе облачных и туманных вычислений // T-Comm: Телекоммуникации и транспорт. 2025. Т. 19. № 7. С. 25–33. DOI:10.36724/2072-8735-2025-19-7-25-33. EDN:WHDPWF

19. Воробьев С.П. Математическая модель оптимизации сетевой инфраструктуры распределенной корпоративной системы на базе облачных, туманных и граничных технологий // Моделирование, оптимизация и информационные технологии. 2019. Т. 7. № 3(26). С. 4. DOI:10.26102/2310-6018/2019.26.3.003. EDN:LIIPTF

References

1. Yermakov S.G., Khalil M.M., Khomonenko A.D., Bukharova K.A. Evaluating the efficiency of fog computingon the internet of things using a Non-Markov model. *T-Comm*. 2022;16(12):46–52. DOI:10.36724/2072-8735-2022-16-12-46-52. EDN:MVRSBV

2. Glushak E.V. *Cloud and fog computing: architecture, modeling, application*. Vologda; Moscow: Infra-Engineering Publ.; 2025. 180 p. (in Russ.) EDN:BUZGWB

3. Fletcher M., Paulz E., Ridge D., Michaels A.J. Low-Latency Wireless Network Extension for Industrial Internet of Things. *Sensors*. 2024;24(7):2113. DOI:10.3390/s24072113. EDN:YATJXO
4. Plotnikov P.V., Vladyko A.G. Analysis of Approaches to Optimization of V2X Systems: Clustering, Edge and Fog Computing. *Proceedings of Telecommunication Universities*. 2024;10(3):7–22. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-7-22. EDN:TRWNON
5. Daraselia A.V. *Models and analysis of performance indicators of traffic offloading mechanisms in heterogeneous wireless networks*. Ph.D. Thesis. Moscow: Peoples' Friendship University of Russia Publ.; 2022. 106 p. (in Russ.) EDN:VQNBTU
6. Murashkin I.N. Research of latency minimization algorithms in data stream processing systems. *Innovations and Investments*. 2025;4:356–359. (in Russ.) EDN:AHKBWE
7. Melnik E.V., Klimenko A.B., Klimenko V.V. Models and reliability analysis of information and control systems based on fog computing. *Proceedings of the 5th All-Russian Scientific and Technical Conference at Supercomputer Technologies, SKT – 2018, 17–22 September 2018, Rostov-on-Don, Russian Federation, vol.2*. Rostov-on-Don: Southern Federal University Publ.; 2018. p.103–107. (in Russ.) EDN:YQBQRN
8. Glushak E.V., Klyuev D.S. Development and research of models for the functioning of cloud and fog computing. *Radioengineering*. 2025;89(3):157–168. (in Russ.) DOI:10.18127/j00338486-202503-14. EDN:IGUDLR
9. Melnik E.V., Klimenko A.B. A recovery technique of the fog-computing-based information and control system computational process. *Izvestiya Tula State University*. 2018;9:551–563. (in Russ.) EDN:YNDROH
10. Alsweiti M. Deep Learning Approaches for Traffic Prediction Forecasting in Multi-Level Cloud Architecture for Autonomous Vehicle Services. *Proceedings of Telecommunication Universities*. 2022;8(4):89–99. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-89-99. EDN:CNIDPH
11. Melnik E.V., Ivanov D.Ya., Orda-Zhigulina M.V., Orda-Zhigulina D.V., Rodina A.A. Application of fog computing for monitoring and forecasting system of hazardous natural phenomena. *Izvestiya Tula State University*. 2019;2:300–311. (in Russ.) EDN:ZAFGCT
12. Volkov A.N. Routing Task in Dynamic Fog Computing Network. *Proceedings of Telecommunication Universities*. 2024;10(4): 27–37. (in Russ.) DOI:10.31854/1813-324X-2024-10-4-27-37. EDN:QWBVQY
13. Volkov A.N. Dynamic Fog Computing Towards Green ICT. *Proceedings of Telecommunication Universities* 2024;10(3):24–34. (in Russ.) DOI:10.31854/1813-324X-2024-10-3-24-34. EDN:QOELMJ
14. Glushak E.V., Mikhailova P.D. Overview of the adaptive algorithms for distributing internet of things data flows in cloud and foggy media. *Infokommunikacionnye Tehnologii*. 2024;22(4-88):15–22. (in Russ.) DOI:10.18469/ikt.2024.22.4.02. EDN:ALXFGY
15. Volkov A.N. *Development and study of a set of models and methods for constructing communication networks based on fog computing and providing telepresence services*. DSc Thesis. St. Petersburg: The Bonch-Bruevich Saint Petersburg State University of Telecommunications Publ.; 2024. 54 p. (in Russ.)
16. Kupriyanov D.O. Mathematical modeling of requests flow to cloud compute cluster. *T-Comm*. 2020;14(10):39–44. (in Russ.) DOI:10.36724/2072-8735-2020-14-10-39-44. EDN:MWCXTC
17. Melnik E.V., Klimenko A.B., Ivanov D.Ya. A model of the computational load distribution problem for information and control systems based on the fog computing concept. *Izvestiya Tula State University*. 2018;2:174–187. (in Russ.) EDN:YXJCRP
18. Glushak E.V., Klyuev D.S., Volovach V.I. Analysis of distribution of tasks in the cloud and fog computing system. *T-Comm*. 2025;19(7):25–33. (in Russ.) DOI:10.36724/2072-8735-2025-19-7-25-33. EDN:WHDPWF
19. Vorobyov S.P. Mathematical model of optimization of the network infrastructure of a distributed enterprise system on a cloud, misty and edge technologies. *Modeling, Optimization, and Information Technology*. 2019(7);3-26:4. (in Russ.) DOI:10.26102/2310-6018/2019.26.3.003. EDN:LIIPTF

Статья поступила в редакцию 13.03.2025; одобрена после рецензирования 03.04.2025; принята к публикации 07.04.2026
The article was submitted 13.03.2025; approved after reviewing 03.04.2025; accepted for publication 07.04.2026

Информация об авторе:

ГЛУШАК Елена Владимировна
кандидат технических наук, доцент кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики
https://orcid.org/0009-0000-5494-9746

Автор сообщает об отсутствии конфликтов интересов.
The author declares no conflicts of interests.