

Научная статья

УДК 004.032.6:519.87

<https://doi.org/10.31854/1813-324X-2026-12-4-105-117>

EDN:TYZAFD



Метод оценки готовности распределенной подсистемы хранения туманного уровня к обслуживанию операций в телекоммуникационной сети

Анастасия Андреевна Савельева, saa@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность. В телекоммуникационных системах распределенные подсистемы хранения непосредственно влияют на доступность и качество обслуживания сервисов, что особенно важно в условиях развития высокодоступных сетей и систем связи 5G и последующих поколений, где выполнение операций зависит не только от состояния сетевой подсистемы, но и от узлов хранения и их параметров. Среди таких операций запись требует отдельного анализа, поскольку в распределенных средах, в частности на туманном уровне, запись связана с передачей данных на несколько узлов хранения и получением подтверждений о фиксации результата, что повышает требования к доступности элементов инфраструктуры.

Цель исследования: разработка метода оценки готовности распределенной подсистемы хранения туманного уровня к обслуживанию операций записи в телекоммуникационной сети с учетом параметров репликации, режима подтверждения записи и состояния инфраструктурных элементов.

В ходе исследования были использованы **методы** теории надежности и готовности, вероятностный анализ и сравнительное исследование конфигураций распределенной подсистемы хранения.

Решение: получены расчетные соотношения для определения коэффициента готовности подсистемы к обслуживанию операций записи с учетом уровня избыточности, порога подтверждения записи и состояния элементов цепочки обслуживания операции. Предложена классификация трафика и данных, ориентированная на выбор параметров репликации и подтверждения записи.

Новизна работы определяется переходом от оценки готовности узлов и кластера в целом к оценке готовности выполнения операций записи в распределенной подсистеме хранения туманного уровня.

Теоретическая значимость заключается в развитии методического аппарата оценки готовности распределенных подсистем хранения в телекоммуникационных системах.

Практическая значимость состоит в возможности использования предложенного метода при выборе параметров репликации и режима подтверждения записи для подсистем хранения туманного уровня.

Ключевые слова: распределенная подсистема хранения данных, туманные вычисления, доступность, качество обслуживания, сети связи 5G

Финансирование: Исследование выполнено при финансовой поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, соглашение № 071-03-2026-010, «Разработка фрагмента модельной гибридной орбитально-наземной сети связи и проведение прикладных научных исследований на ее базе».

Ссылка для цитирования: Савельева А.А. Метод оценки готовности распределенной подсистемы хранения туманного уровня к обслуживанию операций в телекоммуникационной сети // Труды учебных заведений связи. 2026. Т. 12. № 4. С. 105–117. DOI:10.31854/1813-324X-2026-12-4-105-117. EDN:TYZAFD

Original research

<https://doi.org/10.31854/1813-324X-2026-12-4-105-117>

EDN:TYZAFD

A Method for Assessing the Availability of a Fog-Level Distributed Storage Subsystem for Servicing Operations in a Telecommunication Network

 Anastasia A. Saveleva, saa@sut.ru

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

The relevance. In telecommunication systems, distributed storage subsystems directly affect service availability and quality of service, which is particularly important in the context of the development of highly available 5G and beyond communication networks and systems, where the execution of operations depends not only on the state of the network subsystem, but also on the storage nodes and their parameters.

The purpose of the study: to develop a method for assessing the availability of a Fog-level distributed storage subsystem for servicing operations in a telecommunication network, taking into account replication parameters, the write acknowledgment mode, and the condition of infrastructure elements.

Methods of reliability and availability theory, probabilistic analysis, and a comparative study of distributed storage subsystem configurations were used.

Results. Analytical relationships were obtained for determining the availability coefficient for servicing write operations, taking into account the level of redundancy, the write acknowledgment threshold, and the condition of critical-path elements. A classification of traffic and data oriented toward the selection of replication parameters and write acknowledgment modes was proposed.

The novelty of the study is determined by the transition from assessing the availability of individual nodes and the cluster as a whole to assessing the availability of operation execution in a Fog-level distributed storage subsystem.

The theoretical significance lies in the development of the methodological framework for assessing the availability of distributed storage subsystems in telecommunication systems.

The practical significance consists in the possibility of using the proposed method when selecting replication parameters and the write acknowledgment mode for Fog-level storage subsystems.

Keywords: distributed storage subsystem, Fog computing, availability, quality of service, 5G networks

Funding: The study was carried out with the financial support of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation under Agreement No. 071-03-2026-010, "Development of a fragment of a model hybrid orbital-terrestrial communication network and applied scientific research based on it".

For citation: Saveleva A.A. A Method for Assessing the Availability of a Fog-Level Distributed Storage Subsystem for Servicing Operations in a Telecommunication Network. *Proceedings of Telecommunication Universities*. 2026; 12(4):105–117. (in Russ.) DOI:10.31854/1813-324X-2026-12-4-105-117. EDN:TYZAFD

Введение

Развитие телекоммуникационных систем туманного (от англ. Fog) и пограничного (от англ. Edge) уровня сопровождается переносом вычислительных и информационных ресурсов к границе сети, вследствие чего подсистемы хранения перестают быть исключительно вспомогательным компонентом и становятся частью контура предоставления

сервиса. В архитектуре мобильных периферийных вычислений с множественным доступом (МЕС, аббр. от англ. Multi-access Edge Computing) узел МЕС рассматривается как сущность, включающая платформу и инфраструктуру виртуализации ресурсов, предоставляющую вычислительные, сетевые и запоминающие ресурсы для выполнения приложений [1]. В дальнейшем МЕС предлагается

рассматривать как стандартизованный телекоммуникационный вариант Edge-уровня, тогда как Fog-уровень трактуется как более широкий промежуточный уровень, на котором могут размещаться сервисные функции, координация и распределенные подсистемы хранения [2]. При этом состояние распределенной подсистемы хранения начинает непосредственно влиять на доступность и качество обслуживания сетевых сервисов, а оценка ее готовности приобретает значение не только для вычислительной, но и для телекоммуникационной инфраструктуры. В данной постановке объект исследования находится на Fog-уровне. Параметры доступности также входят в состав характеристик IP-сервиса в рекомендациях ITU-T, а понятия надежность (*от англ. Dependability*) и доступность (*от англ. Availability*) рассматриваются применительно к телекоммуникационным услугам и сетям [3, 4].

В распределенной подсистеме хранения Fog-уровня обслуживается не одна изолированная функция, а совокупность операций, обеспечивающих жизненный цикл данных в сети и предоставления сервиса на стороне клиентов. К числу таких операций относятся прием и размещение данных, чтение, обновление, удаление, обмен служебными метаданными, поддержание копий (реплик), а также процедуры восстановления после отказов. Для Edge- и Fog-среды данная совокупность операций должна рассматриваться с учетом ограниченности ресурсов узлов, неоднородности нагрузки и требований приложений к задержке и качеству обслуживания (QoS, *аббр. от англ. Quality of Service*) [5, 6]. Кроме того, в современной литературе репликация данных рассматривается как один из базовых механизмов повышения доступности и устойчивости хранения в облачных, туманных и пограничных вычислениях [7].

Однако различные операции неодинаковы по структуре обслуживания и по чувствительности к состоянию инфраструктуры. Операции чтения в ряде случаев могут быть выполнены при наличии доступа хотя бы к одной согласованной копии данных, тогда как операции записи требуют маршрутизации запроса, выбора реплик, передачи данных, фиксации изменений и формирования подтверждения в соответствии с принятой политикой обслуживания. При наличии репликации именно запись первой начинает зависеть от межузлового обмена, топологии размещения копий, режима согласования и числа необходимых подтверждений. По этой причине для распределенной подсистемы хранения Fog-уровня операцию записи целесообразно рассматривать как наиболее чувствительную к архитектуре и наиболее ресурсоемкую в части сетевого и координационного взаимодействия. Такой вывод согласуется с исследованиями Fog-инфраструктуры [8, 9], где повышение доступности дости-

гается ценой дополнительного обмена данными и необходимости учитывать задержку и сетевую нагрузку при размещении и поддержании реплик.

Особую значимость данная постановка приобретает в сетях 5G и последующих поколений. Услуги телеприсутствия в сетях IMT-2030 рассматриваются как сервисы, формируемые в условиях глубокой интеграции сетевых и вычислительных технологий. Указанное означает, что при исследовании архитектур сетей будущих поколений необходимо учитывать не только собственно сетевые механизмы, но и принципы построения высоконагруженных распределенных приложений, включая взаимодействие микросервисов, их внутренние процессы, а также системные и несистемные требования к функционированию [10]. В такой постановке подсистемы хранения и обслуживания операций над данными становятся частью общего контура предоставления сервиса, а их состояние начинает непосредственно влиять на доступность и качество обслуживания.

При этом в системе 5G обслуживание строится на основе потоков QoS и значений 5QI (*аббр. от англ. 5G QoS Indicator*) [11, 12], то есть сеть изначально ориентирована на сосуществование потоков с различными требованиями к задержке, приоритету и допустимому уровню потерь. Одновременно требования MEC-приложений включают не только вычислительные и сетевые, но и запоминающие ресурсы, а также ограничения по задержке [13]. Следовательно, при анализе распределенной подсистемы хранения туманного уровня необходимо учитывать, что нарушения в обслуживании операций над данными могут проявляться как деградация сетевого сервиса, а не только как локальная проблема хранилища. Анализ научной литературы [7, 8, 14] показывает, что в настоящее время достаточно подробно изучены задачи репликации данных и оптимизации хранения в Cloud- и Fog-инфраструктурах. В процессе исследования выявлены обзорные и прикладные работы, посвященные размещению реплик, снижению задержки, повышению доступности и учету QoS-ограничений в распределенных средах [8, 9, 14]. Вместе с тем соответствующие исследования, как правило, сосредоточены либо на оптимизации размещения копий, либо на сравнении систем хранения по производительности, тогда как оценка готовности именно к выполнению операции записи с одновременным учетом уровня избыточности (*от англ. Redundancy*), режима подтверждения и состояния инфраструктурных элементов цепочки обслуживания операции проработана существенно слабее.

Таким образом, в настоящей статье предлагается перейти от общей характеристики распределенной подсистемы хранения к локальной, но практически значимой задаче – оценке готовности

к обслуживанию операций записи в телекоммуникационной сети. Такой переход представляется обоснованным по двум причинам. Во-первых, запись является операцией, в наибольшей степени зависящей от совместного состояния координатора, сетевой составляющей, узлов хранения и параметров подтверждения. Во-вторых, именно доступность записи определяет способность туманного узла поддерживать актуальное состояние сервисов, журналов, контекстов и иных данных, от которых зависит непрерывность функционирования приложений.

В рамках данной постановки распределенная подсистема хранения рассматривается как часть телекоммуникационной инфраструктуры, а коэффициент готовности – как характеристика возможности завершения операции записи при заданных параметрах репликации и состоянии элементов цепочки обслуживания операций. В отличие от подходов, ориентированных на оценку готовности отдельного узла или кластера в целом, предметом анализа становится готовность выполнения операции, то есть способность системы обеспечить запись и сформировать подтверждение клиенту в соответствии с принятой политикой обслуживания. Целью статьи является разработка метода оценки готовности распределенной подсистемы хранения Fog-уровня к обслуживанию операций записи в телекоммуникационной сети с учетом параметров

избыточности, режима подтверждения записи и состояния инфраструктурных элементов. Для достижения указанной цели в работе формализуется структура цепочки обслуживания операции записи, выводятся расчетные соотношения для коэффициента готовности в общем и частных случаях, а также предлагается классификация трафика и данных, ориентированная на выбор параметров репликации и подтверждения записи в зависимости от требований сервисов 5G и последующих поколений.

На рисунке 1 показано положение объекта исследования в иерархической архитектуре телекоммуникационной сети. Под узлами Fog-уровня в данном случае понимаются узлы распределенной подсистемы хранения, обеспечивающие обслуживание операций записи, чтения и межузлового взаимодействия. Под межузловым обменом далее понимается совокупность служебных потоков между указанными узлами, связанных с репликацией данных, передачей подтверждений, синхронизацией состояния реплик и выполнением восстановительных процедур. Пограничный уровень рассматривается как уровень, непосредственно примыкающий к источникам данных и сети доступа и обеспечивающий локальную предварительную обработку и передачу данных, тогда как облачный уровень выполняет функции централизованного управления, аналитики и долговременного хранения.

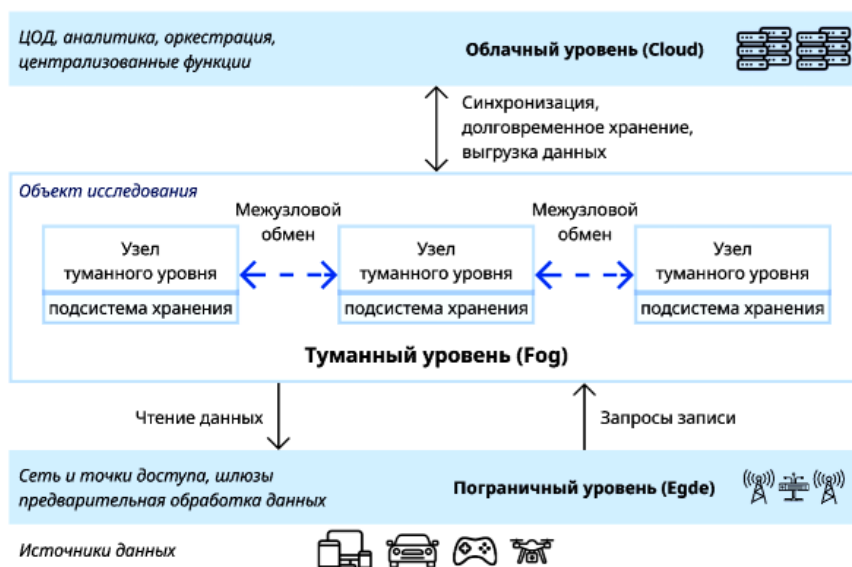


Рис. 1. Положение объекта исследования в иерархической архитектуре телекоммуникационной сети

Fig. 1. Position of the Research Object in the Cloud-Fog-Edge Hierarchical Architecture of a Telecommunication Network

Подходы к организации обслуживания операций

Пусть для каждой операции записи в системе формируется R реплик данных, а успешное завершение операции определяется получением подтверждений не менее чем от W реплик, где $1 \leq W \leq R$, при этом параметр R далее интерпретируется как уро-

вень избыточности, а параметр W – как порог подтверждения записи.

При равных значениях $R = W$ реализуется строгий режим подтверждения, при $W < R$ – ослабленный либо кворумный режим. Тогда коэффициент готовности должен характеризовать не готовность

хранилища, а вероятность того, что в произвольный момент времени система способна завершить операцию записи в соответствии с заданными значениями R и W .

Для формализации этой вероятности вводится понятие цепочки обслуживания операции записи. Под цепочкой обслуживания далее понимается совокупность инфраструктурных элементов, отказ любого из которых делает невозможным завершение операции записи и формирование подтверждения. В состав таких элементов могут входить: функция координации записи, сетевой сегмент доставки запроса от клиента, вычислительная платформа узла хранения, локальная подсистема ввода-вывода, журнальный накопитель, а также межузловые соединения, обеспечивающие передачу данных и подтверждений между репликами. Тем самым в модель включаются не только узлы хранения, но и элементы телекоммуникационной инфраструктуры, определяющие доступность сервиса записи.

Пусть Ω_0 – множество общих элементов цепочки обслуживания операции записи, используемых всеми вариантами ее выполнения, а Ω_i – множество элементов ветви обслуживания записи на i -й узел, где i принимает значения от 1 до R включительно, причем при этом указанные выше множества считаются непересекающимися. Для каждого элемента инфраструктуры вводится коэффициент готовности A_m (далее коэффициент готовности обозначается через A в соответствии с ГОСТ [15], устанавливающим математические выражения для показателей безотказности, готовности и ремонтпригодности).

Тогда коэффициент готовности общей части цепочки обслуживания операции записи определяется как:

$$A_0 = \prod_{m \in \Omega_0} A_m, \quad (1)$$

где m – элемент инфраструктуры (сеть, сервер, диск), а коэффициент готовности ветви обслуживания операции записи на i -й узел как:

$$A_i^{(wr)} = \prod_{m \in \Omega_i} A_m. \quad (2)$$

В этой связи локальная задача исследования формулируется следующим образом: при заданных значениях R и W , а также при известных коэффициентах готовности инфраструктурных элементов A_m требуется получить расчетное соотношение для коэффициента готовности распределенной подсистемы хранения к обслуживанию операций записи в телекоммуникационной сети. Искомый коэффициент должен отражать совместное влияние уровня избыточности, режима подтверждения записи и состояния общих и частных элементов цепочки обслуживания операции. Дополнительно в

работе предполагается, что полученные расчетные соотношения могут использоваться для сопоставления различных конфигураций распределенной подсистемы хранения и для выбора режимов обслуживания операции в зависимости от профиля трафика и требований сервиса. Такая интерпретация особенно важна для Fog-уровня, где распределенная подсистема хранения должна обслуживать потоки с различными требованиями к задержке, допустимой потере данных и др. Следовательно, результатом решения поставленной задачи должны стать не только формулы для вычисления коэффициента готовности, но и основа для последующей классификации трафика и выбора параметров R и W по условиям эксплуатации сети 5G и последующих поколений.

Метод расчета коэффициента готовности

В соответствии с постановкой задачи коэффициент готовности распределенной подсистемы хранения должен характеризовать возможность завершения операции записи в телекоммуникационной сети при заданных параметрах репликации и подтверждения. В рамках предлагаемого подхода готовность рассматривается как характеристика функционирования телекоммуникационного сервиса, обеспечиваемого совокупностью взаимосвязанных инфраструктурных элементов, а не как свойство отдельного узла. При этом данный подход соответствует используемым в литературе моделям Edge-, Fog-, Cloud-инфраструктур и телекоммуникационной трактовке доступности, при которой оценка выполняется на уровне составного сервиса, а не отдельного элемента [14, 16, 17].

Для каждого элемента принимается стандартное соотношение:

$$A_m = \frac{MTBF_m}{MTBF_m + MTTR_m}, \quad (3)$$

где $MTBF_m$ – средняя наработка до отказа для элемента m ; $MTTR_m$ – среднее время восстановления.

Такое представление удобно для включения в расчет как сетевых, так и вычислительных и запоминающих компонентов, влияющих на завершение операции.

На рисунке 2 представлена обобщенная структурная схема обслуживания операции записи в распределенной подсистеме хранения Fog-уровня. В ней выделены общая часть цепочки обслуживания, включающая источник запроса, сетевой сегмент и координатор записи, а также ветви записи к узлам, на которых размещаются реплики. Координатор записи в данном случае рассматривается как логическая функция управления операцией и проверки условия ее завершения, а не как признак обязательного наличия постоянно выделенного

ведущего узла хранения. Успешное завершение операции определяется доступностью общей части обслуживания и доступностью не менее W ветвей записи из R возможных, что на уровне взаимодействия проявляется в получении не менее W подтверждений.

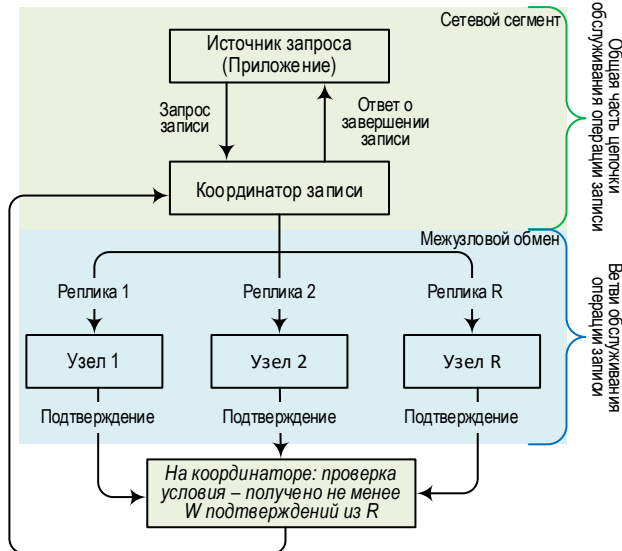


Рис. 2. Структурная схема обслуживания операции записи в распределенной подсистеме хранения Fog-уровня

Fig. 2. Structural Diagram of Write-Operation Servicing in a Fog-Level Distributed Storage Subsystem

Указанные свойства позволяют использовать полученное выражение как основу для анализа типовых режимов записи и для практического выбора параметров R и W .

Следовательно, коэффициент готовности системы к обслуживанию операции записи в общем случае определяется как вероятность доступности общей части цепочки обслуживания операции записи и не менее W ветвей обслуживания операции записи к узлам, на которых размещаются реплики, из R возможных:

$$A^{(wr)}(R, W) = A_0 \sum_{\substack{M \subseteq \{1, \dots, R\} \\ |M| \geq W}} \prod_{i \in M} A_i^{(wr)} \prod_{j \notin M} (1 - A_j^{(wr)}), \quad (4)$$

где M – множество ветвей обслуживания записи к узлам репликации, доступных в рассматриваемом сочетании; i и j – индексы доступных и недоступных ветвей обслуживания записи.

Полученное выражение является общим и применимо для неоднородной инфраструктуры, когда ветви обслуживания записи к различным репликам отличаются по составу и по коэффициентам готовности. Такой случай характерен для Fog-уровня, где отдельные реплики могут быть размещены на узлах с различной надежностью и разными сетевыми условиями. Исследования [9] также показывают, что доступность распределенного сервиса

определяется не только числом копий, но и их размещением в инфраструктуре (под которым понимается выбор узлов хранения, их сетевой связности и разнесения по доменам отказа).

Для дальнейшего анализа рассмотрим случай однородной конфигурации, в котором ветви обслуживания записи предполагаются одинаковыми по составу и значениям коэффициентов готовности входящих в них элементов:

$$p = A_i^{(wr)}, i = 1, \dots, R. \quad (5)$$

Тогда коэффициент готовности упрощается до биномиальной формы:

$$A^{(wr)}(R, W) = A_0 \sum_{i=W}^R \binom{R}{i} p^i (1-p)^{R-i}. \quad (6)$$

Полученное выражение позволяет выполнять сравнительный анализ режимов записи при варьировании параметров R и W . В частности, для наиболее типичных конфигураций имеем:

$$\begin{aligned} A^{(wr)}(2, 2) &= A_0 p^2, \\ A^{(wr)}(3, 2) &= A_0 (3p^2 - 2p^3), \\ A^{(wr)}(3, 3) &= A_0 p^3, \\ A^{(wr)}(5, 3) &= A_0 (10p^3(1-p)^2 + 5p^4(1-p) + p^5). \end{aligned} \quad (7)$$

Из приведенных соотношений следуют несколько методически важных выводов. При фиксированном уровне избыточности R уменьшение порога подтверждения W приводит к росту коэффициента готовности записи, поскольку ослабляется требование к числу одновременно доступных реплик. При фиксированном W увеличение R в общем случае расширяет число допустимых сочетаний доступных ветвей обслуживания записи и может повышать готовность. Однако в строгом режиме $W = R$ рост числа реплик, напротив, усиливает требование к одновременной доступности всех ветвей обслуживания записи и может привести к уменьшению готовности записи. Поэтому влияние репликации на готовность не является однозначным и должно анализироваться совместно с режимом подтверждения. Для практического применения метода расчет рекомендуется выполнять в следующей последовательности. Сначала определяется состав общих элементов цепочки обслуживания операции записи и ветвей обслуживания. Затем по исходным данным надежности и восстанавливаемости вычисляются коэффициенты готовности отдельных элементов A_m . После этого определяются значения A_0 и $A_i^{(wr)}$, а затем по общему или упрощенному выражению рассчитывается итоговый коэффициент $A^{(wr)}(R, W)$. На заключительном этапе выполняется сопоставление различных конфигураций по значениям R , W и параметрам инфраструктуры. Такая последовательность позволяет использовать предложенный

метод не только для оценки текущего состояния распределенной подсистемы хранения, но и при исследовании, моделировании и проектировании распределенных подсистем хранения Fog-уровня как элементов сетей и систем телекоммуникаций, обеспечивающих обслуживание информационных потоков и доступность сервисов в сетях 5G и последующих поколений.

Сопоставление режимов репликации и подтверждения записи

Полученные расчетные соотношения позволяют перейти от формального выражения коэффициента готовности к сопоставлению типовых конфигураций распределенной подсистемы хранения. Для Fog-уровня такой анализ особенно важен, поскольку увеличение числа реплик и повышение порога подтверждения записи усиливают требования к межузловому обмену, а следовательно, влияют не только на устойчивость хранения, но и на сетевую нагрузку и время завершения операции, соответственно – и на качество предоставляемого сервиса. В работах по Edge-, Fog-репликации также отмечается, что выбор числа копий и их размещения связан с компромиссом между доступностью, стоимостью обслуживания и производительностью распределенной среды [8, 9].

Базовые режимы записи

Для практического анализа целесообразно рассмотреть несколько типовых конфигураций:

$$(R, W) \in \{(1,1), (2,2), (3,2), (3,3), (5,3)\}. \quad (8)$$

Режим (1,1) соответствует отсутствию репликации и минимальному числу подтверждений, особенностью является минимальный объем служебного взаимодействия, однако готовность записи в этом случае полностью определяется состоянием одной единственной цепочки обслуживания. Формально можно записать в следующем виде:

$$A^{(wr)}(1,1) = K_0 p. \quad (9)$$

Режим (2,2) отражает наличие двух реплик при строгом подтверждении от обеих копий:

$$A^{(wr)}(2,2) = K_0 p^2. \quad (10)$$

В этой конфигурации устойчивость к потере одной реплики при выполнении операции записи отсутствует, поскольку отказ любой из двух ветвей обслуживания приводит к невозможности подтверждения.

Режим (3,2) соответствует кворумной записи при трех репликах:

$$A^{(wr)}(3,2) = A_0(3p^2 - 2p^3). \quad (11)$$

Именно данный вариант представляет наибольший практический интерес, поскольку допускает

отказ одной из ветвей обслуживания операции записи и при этом не требует подтверждения от всех трех реплик.

Режим (3,3) реализует строгую синхронную запись на три реплики:

$$A^{(wr)}(3,3) = A_0 p^3. \quad (12)$$

Для данного режима выполнение операции записи возможно только при подтверждении от всех реплик, что предъявляет наиболее высокие требования к одновременной доступности всех ветвей обслуживания операции.

Режим (5,3) отражает повышенную избыточность при сохранении кворумного порога:

$$A^{(wr)}(5,3) = A_0(10p^3(1-p)^2 + 5p^4(1-p) + p^5). \quad (13)$$

В данной конфигурации увеличивается число сочетаний доступных реплик, что теоретически повышает готовность записи, но одновременно увеличивает ресурсоемкость хранения и нагрузку, создаваемую служебным межузловым трафиком.

Влияние порога подтверждения

При фиксированном уровне избыточности R коэффициент готовности определяется степенью строгости условия подтверждения записи.

Для одного и того же $R = 3$ сравнение режимов (3,2) и (3,3) показывает, что:

$$\begin{aligned} A^{(wr)}(3,2) - A^{(wr)}(3,3) &= A_0(3p^2 - 3p^3) = \\ &= 3A_0p^2(1-p) > 0, \text{ при } 0 < p < 1. \end{aligned} \quad (14)$$

Следовательно, при одинаковой инфраструктуре кворумный режим подтверждения обеспечивает более высокий коэффициент готовности, чем строгий режим, поскольку операция может быть завершена даже при недоступности одной из реплик. Полученный результат показывает, что уменьшение порога подтверждения повышает вероятность завершения записи, но снижает требования к синхронности фиксации результата, поэтому выбор W должен определяться одновременно целевым уровнем доступности и принятой политической подтверждению записи.

В дальнейшем анализ сосредоточен на кворумном режиме подтверждения, поскольку данный подход обеспечивает практически значимый компромисс, при этом предпочтение отдается конфигурациям с нечетным числом реплик, поскольку для них кворум определяется правилом большинства, что делает выбор порога подтверждения методически более обоснованным.

Влияние уровня избыточности

При фиксированном пороге подтверждения рост числа реплик не всегда приводит к одинаковому эффекту. Если сравнить режимы (3,2) и (5,3), то

второй вариант обеспечивает большее число сочетаний доступных реплик и, как правило, более высокий коэффициент готовности. Однако такое повышение достигается ценой увеличения числа копий и, следовательно, роста затрат на хранение, служебных операций и нагрузки на сеть. Для туманных систем такое ограничение является принципиальным, поскольку узлы и межузловые соединения часто обладают ограниченными ресурсами, а оптимизация размещения реплик рассматривается как задача поиска компромисса между доступностью и ресурсными затратами.

Противоположная ситуация наблюдается в строгих режимах. Например, при переходе от (2,2) к (3,3) формально увеличивается уровень избыточности, однако коэффициент готовности становится ниже:

$$A^{(wr)}(3,3) = A_0 p^3 < A_0 p^2 = A^{(wr)}(2,2), \quad (15)$$

при $0 < p < 1$.

Следовательно, в случае строгого синхронного подтверждения увеличение числа реплик не повышает, а снижает готовность записи, так как усиливает условие одновременной доступности всех ветвей обслуживания операции. Полученный результат показывает, что готовность определяется не общим числом копий, а конкретной комбинацией R и W . Таким образом, наиболее показательной является группа кворумных конфигураций с нечетным числом реплик, для которых порог подтверждения задается по правилу большинства.

Влияние инфраструктуры

При фиксированных значениях R и W коэффициент готовности определяется не только параметрами репликации, но и состоянием инфраструктуры, обеспечивающей выполнение операции записи. Вследствие этого изменение характеристик отдельных элементов цепочки обслуживания операции может заметно повлиять на доступность сервиса записи без изменения самой схемы избыточности в телекоммуникационной сети.

Из данного положения следует, что повышение готовности записи не во всех случаях требует увеличения числа реплик или изменения порога подтверждения. В ряде случаев сопоставимый или более выраженный эффект может быть достигнут за счет сокращения времени восстановления инфраструктурных элементов, резервирования функции координации, повышения устойчивости сетевых соединений или разнесения реплик по различным доменам отказа [14, 16, 18].

Таким образом, параметры R и W должны рассматриваться совместно с характеристиками инфраструктуры обслуживания записи, что позволяет интерпретировать коэффициент готовности не только как характеристику выбранного режима

репликации, но и как интегральный показатель условий выполнения операции записи в распределенной подсистеме хранения Fog-уровня как элементе телекоммуникационной инфраструктуры.

Интерпретация результатов для дальнейшей классификации

Сопоставление режимов (R, W) показывает, что параметры репликации и подтверждения записи следует рассматривать во взаимосвязи с профилем обслуживаемого трафика. При одинаковом числе реплик изменение порога подтверждения существенно влияет на вероятность завершения операции, а увеличение избыточности в строгих режимах может повышать требования к одновременной доступности всех ветвей обслуживания. Следовательно, выбор параметров R и W должен учитывать назначение сохраняемых данных, допустимость потери отдельных записей, требования к задержке подтверждения и роль операции записи в обеспечении непрерывности работы сервиса. Такой подход согласуется с архитектурой сетей 5G и последующих поколений, в которых потоки QoS и значения 5QI задают неоднородные требования к обслуживанию, а Fog-приложения классифицируются в том числе по требованиям к QoS [19].

Тем самым предложенный метод позволяет не только вычислять коэффициент готовности записи, но и использовать его как основу для выбора политики репликации и подтверждения записи в зависимости от профиля обслуживаемого трафика.

На рисунке 3 показано, что для кворумных конфигураций с нечетным числом реплик увеличение числа узлов хранения сопровождается ростом коэффициента готовности записи $A^{(wr)}$ во всем рассматриваемом диапазоне значений A_i , что объясняется тем, что при переходе к конфигурациям (3,2), (5,3), (7,4), (9,5) расширяется множество сочетаний доступных узлов, при которых операция записи может быть успешно завершена. Вместе с тем для всех кривых наблюдается приближение к верхней границе A_0 , что указывает на ограничивающее влияние общей части цепочки обслуживания операции записи. Следовательно, увеличение числа реплик в кворумной схеме может повышать готовность записи, однако максимально достижимое значение $A^{(wr)}$ определяется не только параметрами R и W , но и состоянием общих инфраструктурных элементов.

Рисунок 4 показывает, что коэффициент готовности записи $A^{(wr)}$ определяется не только готовностью отдельных узлов A_i , но и структурой обслуживания операции записи, задаваемой параметрами R , W и общей частью цепочки обслуживания операции записи A_0 . При одинаковых значениях A_i кворумные режимы с меньшим порогом подтверждения обеспечивают более высокую готовность,

чем режимы с подтверждением от большего числа реплик, а увеличение числа реплик при фиксированном W расширяет множество допустимых сочетаний доступных узлов и тем самым повышает $A^{(wr)}$. Вместе с тем для всех конфигураций наблюдается асимптотическое приближение к верхней границе A_0 , что указывает на принципиально ограничивающее влияние общей части цепочки обслуживания операции записи. Следовательно, повышение готовности отдельных узлов само по себе не гарантирует пропорционального роста готовности записи и должно рассматриваться совместно с выбором режима подтверждения и состоянием общих инфраструктурных элементов.

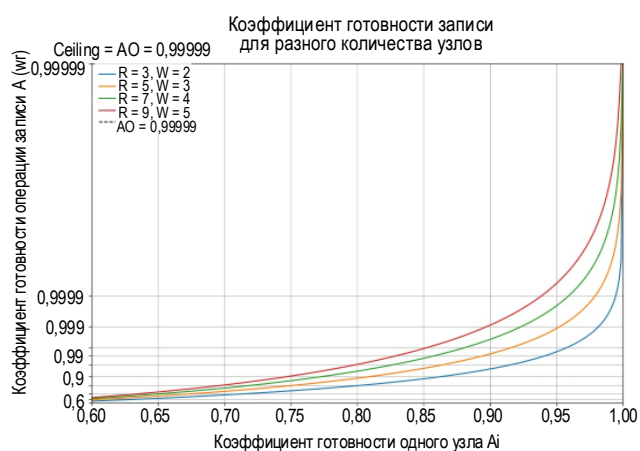


Рис. 3. Влияние увеличения числа реплик в кворумных конфигурациях (R, W) на коэффициент готовности записи
Fig. 3. Influence of Increasing the Replication Factor in Quorum (R, W) Configurations on the Write-Operation Availability Coefficient

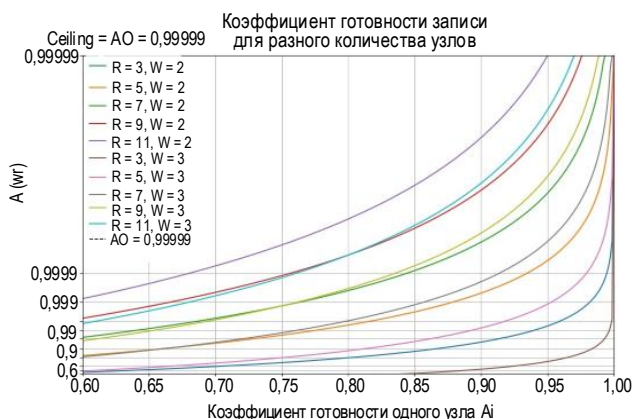


Рис. 4. Влияние параметров на коэффициент готовности записи при ограничении со стороны общей части цепочки обслуживания операции

Fig. 4. Influence of Parameters on the Write Availability Factor with Constraints from the General Part of the Operation Service Chain

Отображенная на рисунке 5 зависимость позволяет сделать вывод о том, что с ростом времени восстановления преимущества кворумных режимов становятся устойчиво выраженными, что до-

полнительно подтверждает – при оценке готовности операции записи параметры R и W должны рассматриваться совместно.

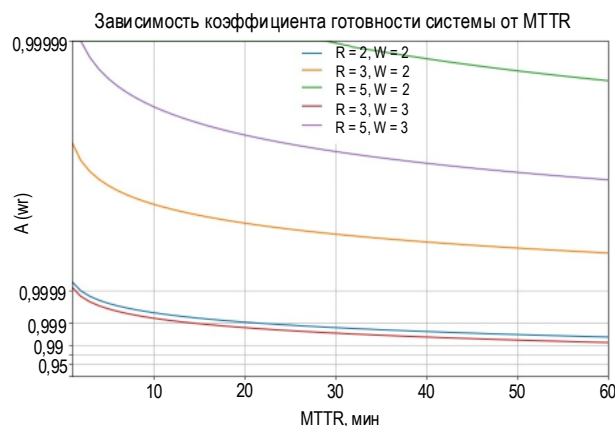


Рис. 5. Зависимость коэффициента готовности операции записи от среднего времени восстановления (MTTR) при различных сочетаниях параметров R и W

Fig. 5. Dependence of the write operation readiness coefficient on the mean time to restore (MTTR) for different combinations of the R and W parameters

Классификация трафика и данных по требованиям к репликации и подтверждению записи

С методической точки зрения прямая связь класса сетевого трафика с числом реплик не задается ни документами 3GPP, ни документами ITU-R. Однако профили обслуживания формируют ограничения по задержке и допустимой потере данных, которые должны учитываться при выборе параметров R и W . Поэтому в дальнейшем целесообразно использовать промежуточную логическую цепочку: класс трафика и сервисный сценарий, требования к операции записи, рекомендуемая комбинация репликации и подтверждения. Для сетей IMT-2030 такая постановка становится еще более актуальной, поскольку к традиционным eMBB (аббр. от англ. Enhanced Mobile BroadBand), mMTC (аббр. от англ. Massive Machine-Type Communications) и URLLC (аббр. от англ. Ultra-Reliable Low-Latency Communications) добавляются иммерсивные коммуникации, HURLLC (аббр. от англ. Hyper-Reliable Low-Latency Communications), AI (аббр. от англ. Artificial Intelligence), интегрированное зондирование и связь, а также повсеместная связность [20, 21]. Логика организации туманных вычислений и распределения функций обработки и хранения на периферии сети подробно рассматривается в русскоязычном обзоре [22], а актуальность таких задач для сетей связи 2030 подтверждается отечественными исследованиями развития сетей 5G и последующих поколений [23].

В рамках настоящей работы предлагается выделить четыре обобщенных класса трафика и данных.

Класс 1. Некритичные короткоживущие данные

К данному классу относятся потоки, для которых приоритетом являются масштабируемость и минимизация служебного обмена, а потеря части отдельных записей не приводит к существенной деградации сервиса. К этой группе могут быть отнесены массовая телеметрия, часть метрик мониторинга не критических событий системы, позволяющих производить обслуживание системы, данные сенсоров с последующей агрегацией, а также временные данные локального обслуживания. Для подобных нагрузок более рациональны режимы с минимальным уровнем избыточности и упрощенным подтверждением, поскольку избыточная репликация в данном случае создает дополнительную нагрузку на сеть и узлы без пропорционального роста полезного эффекта. Для таких потоков в качестве базовой рекомендации может использоваться режим $R = 1$, $W = 1$ либо $R = 2$, $W = 1$, если требуется ограниченная устойчивость к локальным отказам. Как показано в работе [5], Fog-приложения неоднородны по требованиям к хранению данных и надежности.

Также для не критичных короткоживущих данных допустимо локальное временное размещение на Edge-уровне без обязательного включения соответствующей копии в контур подтверждения записи, а последующая передача на Fog-уровень может выполняться по мере агрегации или при необходимости хранения на более высоком уровне.

Класс 2. Данные средней критичности

Ко второму классу относятся журналы диагностической информации, данные эксплуатационной аналитики, показатели QoS, часть данных мониторинга критических событий системы, позволяющих предотвращать сбои, а также, например, сведения о загрузке вычислительных и сетевых ресурсов туманного узла, записи о вариации задержки и потерях пакетов, журналы срабатывания механизмов восстановления и иные потоки, потеря которых нежелательна, но не приводит немедленно к нарушению работы сервиса. Для данной категории требуется компромисс между устойчивостью хранения и затратами сетевых и вычислительных ресурсов. В таких условиях целесообразно использовать кворумные режимы записи, обеспечивающие повышенную готовность операции без необходимости синхронного подтверждения всеми репликами. В качестве базового варианта может быть рекомендован режим $R = 3$, $W = 2$, который обеспечивает более высокий коэффициент готовности по сравнению со строгим режимом $R = 3$, $W = 3$ при той же архитектуре. Для Fog-приложений данный класс соответствует сервисам со средними требованиями к хранению, надежности и задержке. Конфигурация $R = 2$, $W = 2$ может рассматриваться как допустимый

упрощенный вариант для ресурсно-ограниченных туманных узлов и умеренных требований к доступности, однако не обеспечивает завершение записи при отказе одной из двух реплик и потому не является предпочтительной.

Класс 3. Критичные операционные данные

К этому классу относятся данные, обеспечивающие непрерывность функционирования телекоммуникационного сервиса: состояния приложений, служебные данные, данные координации Edge-сервисов, журналы событий, значимые для восстановления и последующего управления. Для таких потоков потеря возможности записи уже непосредственно влияет на доступность сервиса. В 5G-среде аналогичные нагрузки возникают в сценариях с повышенными требованиями к приоритету обслуживания и устойчивости, поскольку потоки QoS допускают различные уровни параметров для разных типов сетевого трафика. Для данного класса могут быть использованы режимы $R = 3$, $W = 2$ либо $R = 3$, $W = 3$. Первый вариант целесообразен при необходимости повысить готовность завершения записи, второй – при более строгих требованиях к синхронности фиксации результата. Выбор между ними должен определяться допустимой задержкой подтверждения и критичностью потери неподтвержденной копии.

Класс 4. Особо критичные данные высоконадежных сценариев

К четвертому классу относятся данные сервисов, для которых требуются одновременно высокая надежность, малая задержка и устойчивость к деградации инфраструктуры. В логике IMT-2030 к таким сценариям относятся HRLLC, иммерсивные коммуникации в интерактивной форме, ISAC (аббр. от англ. Integrated Sensing and Communications), а также иные приложения, где нарушение операции записи может привести к потере согласованного состояния, нарушению управления или деградации киберфизического взаимодействия. Для этой категории недостаточно повышать число копий – требуется сочетание повышенной избыточности с осмысленным выбором порога подтверждения и, при необходимости, разнесением по доменам отказа. В качестве разнесения по доменам отказа в том числе может быть рассмотрено асинхронное создание Cloud-копии для целей долговременного хранения, резервирования и последующего восстановления, однако основное подтверждение записи должно формироваться на Fog-уровне.

Для данного класса в качестве ориентировочного режима может рассматриваться конфигурация $R = 5$, $W = 3$, а для наиболее ответственных случаев – комбинированные схемы, где репликация сочетается с инфраструктурным резервированием и контролем

критических элементов цепочки обслуживания операции. Сценарии HRLLC, иммерсивные коммуникации и ISAC прямо названы в материалах по IMT-2030 как отдельные или новые варианты использования. Перспективные направления исследований в области сетей связи 2030 также связываются с новыми сервисными сценариями, распределенной обработкой и изменением требований к инфраструктуре предоставления услуг [24].

Для удобства дальнейшего использования предложенная классификация представлена в табличном виде (таблица 1).

ТАБЛИЦА 1. Классы трафика и рекомендуемые параметры репликации и подтверждения записи

TABLE 1. Traffic Classes and Recommended Replication and Write Acknowledgement Parameters

Класс сетевого трафика / характер формируемых данных	Примеры приложений и сервисов 5G и последующих поколений	Основные требования	Рекомендуемый режим
Массовый трафик с приоритетом масштабируемости / Некритичные короткоживущие данные	– IoT и сенсорная телеметрия – часть мониторинговых метрик – агрегируемые потоки	– масштабируемость – минимизация служебного обмена – допустимость частичной потери	$R = 1$, $W = 1$ или $R = 2$, $W = 1$
Трафик средней критичности со сбалансированными требованиями / Данные средней критичности, используемые для последующего анализа, диагностики и локального управления	– журналы платформы – эксплуатационная аналитика MEC-узла – QoS-мониторинг	– компромисс между устойчивостью и затратами ресурсов	$R = 3$, $W = 2$ или $R = 2$, $W = 2$
Чувствительный к непрерывности и отказам операционный трафик / Критичные операционные данные	– управление сетевыми функциями, хранение состояний сервисов – координация Edge-приложений – миссионно-критические коммуникации, – часть XR-сценариев с интерактивным взаимодействием	– повышенная доступность записи – контролируемая задержка подтверждения	$R = 3$, $W = 2$ или $R = 3$, $W = 3$
Особо критичный трафик высоконадежных сценариев / Данные высокой значимости, связанные критичными событиями, координацией и управлением	– коллаборативная робототехника – удаленное управление, отдельные HRLLC-сценарии IMT-2030	– высокая устойчивость – сохранение работоспособности при деградации инфраструктуры	$R = 5$, $W = 3$ или комбинированная схема

Класс сетевого трафика / характер формируемых данных	Примеры приложений и сервисов 5G и последующих поколений	Основные требования	Рекомендуемый режим
	– распределенные цифровые двойники – интеллектуальные транспортные и сенсорно-коммуникационные приложения		

Следует подчеркнуть, что указанная классификация носит методический характер, не заменяет собой стандартизованные профили QoS, а дополняет их на уровне туманной подсистемы хранения, позволяя интерпретировать сетевые требования в терминах архитектуры записи. Тем самым коэффициент готовности записи может использоваться как инструмент выбора параметров R и W в зависимости от профиля трафика, а не только как формальный показатель состояния распределенной системы хранения.

Содержательно полученный коэффициент следует интерпретировать как характеристику доступности сервиса записи, а не как интегральную оценку надежности подсистемы хранения в целом, что особенно важно для телекоммуникационных систем, в которых отказ сетевого сегмента, функции координации или межузловое взаимодействие может сделать операцию записи недоступной даже при формальной работоспособности локальных носителей. Тем самым метод позволяет перейти от локальной оценки готовности элементов к оценке готовности распределенной подсистемы хранения как части телекоммуникационного сервиса.

Заключение

В статье рассмотрена задача оценки готовности распределенной подсистемы хранения Fog-уровня к обслуживанию операций записи в телекоммуникационной сети. Показано, что в условиях туманных вычислений готовность такой подсистемы определяется не только состоянием узлов хранения, но и параметрами репликации, режимом подтверждения записи, а также доступностью инфраструктурных элементов, входящих в цепочку обслуживания операции. В рамках исследования предложен метод расчета коэффициента готовности к обслуживанию операций записи, учитывающий уровень избыточности, порог подтверждения записи и состояние общих элементов цепочки обслуживания, а также ветвей обслуживания, соответствующих отдельным репликам. Получены расчетные соотношения для общего и частных случаев, позволяющие сопоставлять различные кон-

фигурации распределенной подсистемы хранения по критерию готовности записи. Показано, что влияние параметров репликации на готовность не является однозначным и должно рассматриваться совместно с режимом подтверждения записи и характеристиками инфраструктуры. Практическим развитием предложенного подхода стала классификация трафика и данных, ориентированная на выбор параметров репликации и подтверждения записи в зависимости от требований сервисов 5G и последующих поколений. Полученные результаты

представляют интерес и в более широком контексте развития сетей будущих поколений, для которых потребуются более гибкие сетевые узлы, а также архитектуры виртуализации сетевых функций в целях оптимальной реализации функций узлов и повышения эксплуатационной эффективности сетей. Кроме того, они могут быть использованы при проектировании и сравнительном анализе распределенных подсистем хранения Fog-уровня как элементов телекоммуникационной инфраструктуры, обеспечивающих доступность и QoS сервисов.

Список источников

1. ETSI GS MEC 003 V4.2.1 (2020-12). Multi-access Edge Computing (MEC). Framework and Reference Architecture.
2. Iorga M., Feldman L., Barton R., Martin M.J., Goren N.S., Mahmoodi C. Fog Computing Conceptual Model // NIST Special Publication 500-325. Gaithersburg: National Institute of Standards and Technology, 2018. DOI:10.6028/NIST.SP.500-325
3. Rec. ITU-T Y.1540. Internet protocol data communication service – IP packet transfer and availability performance parameters. 2019.
4. Rec. ITU-T E.800. Definitions of terms related to quality of service, network performance including dependability. 1994.
5. Guevara J.C., Torres R.S., da Fonseca N.L.S. On the classification of fog computing applications: A machine learning perspective // Journal of Network and Computer Applications. 2020. Vol. 159. P. 102596. DOI:10.1016/j.jnca.2020.102596. EDN:ENTNEP
6. Makris A., Kontopoulos I., Psomakelis E., Xyalis S.N., Theodoropoulos T., Tserpes K. Performance Analysis of Storage Systems in Edge Computing Infrastructures // Applied Sciences. 2022. Vol. 12. Iss. 17. P. 8923. DOI:10.3390/app12178923. EDN:EGJOAP
7. Karamimirazizi F., Jameii S.M., Rahmani A.M. Data Replication Methods in Cloud, Fog, and Edge Computing: A Systematic Literature Review // Wireless Personal Communications. 2024. Vol. 135. PP. 531–561. DOI:10.1007/s11277-024-11082-7. EDN:FEIRZF
8. Torabi E., Ghobaei-Areni M., Shahidinejad A. Data replica placement approaches in Fog computing: a review // Cluster Computing. 2022. Vol. 25. PP. 3561–3589. DOI:10.1007/s10586-022-03575-6. EDN:BSVYJH
9. Li C., Zhang Y., Wang X. Flexible replica placement for enhancing the availability in Edge computing environment // Computer Communications. 2019. Vol. 146. PP. 1–14. DOI:10.1016/j.comcom.2019.07.013
10. Волков А.Н., Кучерявый А.Е. Туманные вычисления в сетях IMT-2030 для услуг телеприсутствия // Сборник научных трудов XIV Всероссийского совещания по проблемам управления (ВСПУ-2024, Москва, Российская Федерация, 17–20 июня 2024 г.). Институт проблем управления им. В.А. Трапезникова РАН, 2024. С. 2295–2297. EDN:JXYICQ
11. 3GPP TS 23.501 / ETSI TS 123 501. System architecture for the 5G System (5GS). 2024.
12. 3GPP TS 23.503 / ETSI TS 123 503. Policy and charging control framework for the 5G System (5GS). 2024.
13. ETSI White Paper No. 20. Developing Software for Multi-Access Edge Computing. 2019.
14. Pereira P., Melo C., Araujo J., Dantas J., Santos V., Maciel P. Availability model for edge-fog-cloud continuum: an evaluation of an end-to-end infrastructure of intelligent traffic management service // The Journal of Supercomputing. 2022. Vol. 78. PP. 4421–4448. DOI:10.1007/s11227-021-04033-7. EDN:ZNBKSO
15. ГОСТ Р 27.010-2019 (МЭК 61703:2016). Надежность в технике. Математические выражения для показателей безотказности, готовности, ремонтпригодности. М.: Стандартинформ, 2019.
16. Rec. ITU-T G.827. Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths. 2003.
17. Rec. ITU-T E.862. Dependability planning of telecommunication networks. 1992.
18. Зарубин А.А., Савельева А.А., Швидкий А.А. Моделирование нагрузки на распределенную систему хранения данных // Вестник связи. 2018. № 7. С. 13–16. EDN:XVQVZR
19. Ksentini A., Jebalia M., Tabbane S. IoT/cloud-enabled smart services: A review on QoS requirements in fog environment and a proposed approach based on priority classification technique // International Journal of Communication Systems. 2021. Vol. 34. Iss. 2. P. e4269. DOI:10.1002/dac.4269
20. Rec. ITU-R M.2160-0. Framework and overall objectives of the future development of IMT for 2030 and beyond. 2023.
21. Liu R., Zhang L., Li R. Y. -N., Di Renzo M. The ITU Vision and Framework for 6G: Scenarios, Capabilities, and Enablers // IEEE Vehicular Technology Magazine. 2025. Vol. 20. Iss. 2. PP. 114–122. DOI:10.1109/MVT.2025.3532887
22. Кирсанова А.А., Радченко Г.И., Черных А.Н. Обзор технологий организации туманных вычислений // Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика. 2020. Т. 9. № 3. С. 35–63. DOI:10.14529/cmse200303. EDN:OVFWXD
23. Волков А.Н., Мутханна А.С.А., Кучерявый А.Е. Сети связи пятого поколения: на пути к сетям 2030 // Информационные технологии и телекоммуникации. 2020. Т. 8. № 2. С. 32–43. DOI:10.31854/2307-1303-2020-8-2-32-43. EDN:ZWNTDB
24. Кучерявый А.Е., Киричек Р.В., Маколкина М.А., Парамонов А.И., Дунайцев Р.А., Пирмагомедов Р.Я., Бородин А.С., Владыко А.Г., Мутханна А.С.А., Выборнова А.И., Владимиров С.С., Гришин И.В. Новые перспективы научных исследований в области сетей связи на 2021-2024 годы // Информационные технологии и телекоммуникации. 2020. Т. 8. № 3. С. 1–19. DOI:10.31854/2307-1303-2020-8-3-1-19. EDN:XDGHAO

References

1. ETSI GS MEC 003 V4.2.1 (2020-12). *Multi-access Edge Computing (MEC). Framework and Reference Architecture*.
2. Iorga M., Feldman L., Barton R., Martin M.J., Goren N.S., Mahmoodi C. Fog Computing Conceptual Model. *NIST Special Publication 500-325*. Gaithersburg: National Institute of Standards and Technology; 2018. DOI:10.6028/NIST.SP.500-325
3. Rec. ITU-T Y.1540. Internet Protocol Data Communication Service – IP Packet Transfer and Availability Performance Parameters. 2019.
4. Rec. ITU-T E.800. *Definitions of Terms Related to Quality of Service, Network Performance Including Dependability*. 1994.
5. Guevara J.C., Torres R.S., da Fonseca N.L.S. On the classification of fog computing applications: A machine learning perspective. *Journal of Network and Computer Applications*. 2020;159:102604. DOI:10.1016/j.jnca.2020.102596. EDN:ENTNEP
6. Makris A., Kontopoulos I., Psomakelis E., Xyalis S.N., Theodoropoulos T., Tserpes K. Performance Analysis of Storage Systems in Edge Computing Infrastructures. *Applied Sciences*. 2022;12(17):8923. DOI:10.3390/app12178923. EDN:EGJOAP
7. Karamimirazizi F., Jameii S.M., Rahmani A.M. Data Replication Methods in Cloud, Fog, and Edge Computing: A Systematic Literature Review. *Wireless Personal Communications*. 2024;135:531–561. DOI:10.1007/s11277-024-11082-7. EDN:FEIRZF
8. Torabi E., Ghobaei-Arani M., Shahidinejad A. Data Replica Placement Approaches in Fog Computing: A Review. *Cluster Computing*. 2022;25:3561–3589. DOI:10.1007/s10586-022-03575-6. EDN:BSVYJH
9. Li C., Zhang Y., Wang X. Flexible Replica Placement for Enhancing the Availability in Edge Computing Environment. *Computer Communications*. 2019;146:1–14. DOI:10.1016/j.comcom.2019.07.013
10. Volkov A.N., Kucheryavy A.E. Fog computing in IMT-2030 networks for telepresence services. *Proceedings of the XIV All-Russian Conference on Control Problems, VSPU-2024, Moscow, Russian Federation, 17–20 June 2024*. V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences Publ.; 2024. PP. 2295–2297. (in Russ.) EDN:JXYICQ
11. 3GPP TS 23.501 / ETSI TS 123 501. *System Architecture for the 5G System (5GS)*. 3GPP; ETSI; 2024.
12. 3GPP TS 23.503 / ETSI TS 123 503. *Policy and Charging Control Framework for the 5G System (5GS)*. 3GPP; ETSI; 2024.
13. ETSI White Paper No. 20. *Developing Software for Multi-Access Edge Computing*. 2019.
14. Pereira P., Melo C., Araujo J., Dantas J., Santos V., Maciel P. Availability Model for Edge-Fog-Cloud Continuum: An Evaluation of an End-to-End Infrastructure of Intelligent Traffic Management Service. *The Journal of Supercomputing*. 2022;78:4421–4448. DOI:10.1007/s11227-021-04033-7. EDN:ZNBKSO
15. GOST R 27.010-2019 (IEC 61703:2016). *Dependability in Technics. Mathematical Expressions for Reliability, Availability, Maintainability and Maintenance Support Measures*. Moscow: Standartinform Publ.; 2019. (in Russ.)
16. Rec. ITU-T G.827. *Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths*. 2003.
17. Rec. ITU-T E.862. *Dependability Planning of Telecommunication Networks*. 1992.
18. Zarubin A.A., Savelieva A.A., Shvidkiy A.A. Modeling the load on a distributed data storage system. *Vestnik svyazi*. 2018;7:13–16. (in Russ.) EDN:XVQVZR
19. Ksentini A., Jebalia M., Tabbane S. IoT/cloud-enabled smart services: A review on QoS requirements in fog environment and a proposed approach based on priority classification technique. *International Journal of Communication Systems*. 2021;34(2):e4269. DOI:10.1002/dac.4269
20. Rec. ITU-R M.2160-0. *Framework and Overall Objectives of the Future Development of IMT for 2030 and Beyond*. 2023.
21. Liu R., Zhang L., Li R. Y. -N., Di Renzo M. The ITU Vision and Framework for 6G: Scenarios, Capabilities, and Enablers. *IEEE Vehicular Technology Magazine*. 2025;20(2):114–122. DOI:10.1109/MVT.2025.3532887
22. Kirsanova A.A., Radchenko G.I., Chernykh A.N. Review of Fog Computing Technologies. *Bulletin of the South Ural State University. Series: Computational Mathematics and Software Engineering*. 2020;9(3):35–63. (in Russ.) DOI:10.14529/cmse200303. EDN:OVFWXD
23. Volkov A., Mutkhanna A., Koucheryavy A. Fifth Generation Communication Networks: On the Way to Networks 2030. *Telecom IT*. 2020;8(2):32–43. (in Russ.) DOI:10.31854/2307-1303-2020-8-2-32-43. EDN:ZWNTDB
24. Koucheryavy A., Kirichek R., Makolkina M., Paramonov A., Dunaitsev R., Pirmagomedov R., Borodin A., Vladyko A., Mutkhanna A., Vybornova A., Vladimirov S., Grishin I. Novel Prospects of Scientific Research in the Field of Telecommunications Networks for the 2021–2024 Years. *Telecom IT*. 2020;8(3):1–19. (in Russ.) DOI:10.31854/2307-1303-2020-8-3-1-19. EDN:XDGHAO

Статья поступила в редакцию 23.04.2026; одобрена после рецензирования 28.05.2026; принята к публикации 10.06.2026

The article was submitted 23.04.2026; approved after reviewing 28.05.2026; accepted for publication 10.06.2026

Информация об авторе:

САВЕЛЬЕВА
Анастасия Андреевна

старший преподаватель кафедры инфокоммуникационных систем
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0002-9393-3007>

Автор сообщает об отсутствии конфликтов интересов.

The author declares no conflicts of interests.