

Научная статья

DOI 10.66424/2071-8217-2026-3-15

УДК 004.056.53

АЛГОРИТМ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ В РАСПРЕДЕЛЕННЫХ ХРАНИЛИЩАХ С КОМПЕНСАЦИЕЙ РЕЗУЛЬТАТОВ ВОЗДЕЙСТВИЙ ДЕСТАБИЛИЗИРУЮЩИХ ФАКТОРОВ И ПРОВЕРКОЙ ДОСТОВЕРНОСТИ РЕЗУЛЬТАТОВ ВОССТАНОВЛЕНИЯ

Г. Е. Русов*, С. А. Диченко

Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознаменное училище имени генерала армии С. М. Штеменко
Министерства обороны Российской Федерации, Краснодар, Россия

✉ *grusov1999@gmail.com

ДЛЯ ЦИТИРОВАНИЯ

Русов Г. Е., Диченко С. А.
Алгоритм обеспечения целостности
данных в распределенных
хранилищах с компенсацией
результатов воздействий
дестабилизирующих факторов
и проверкой достоверности
результатов восстановления // Проблемы информационной безопасности. Компьютерные системы. 2026. № 3. С. 204–215.
DOI: 10.66424/2071-8217-2026-3-15

ПОСТУПИЛА 27.04.2026

ПРИНЯТА 25.08.2026

ОПУБЛИКОВАНА 13.10.2026

© Русов Г. Е., Диченко С. А.

Издатель: Санкт-Петербургский
политехнический университет
Петра Великого

АННОТАЦИЯ

Рассматривается алгоритм обеспечения целостности данных в распределенных хранилищах, ориентированный на контроль целостности хранимых данных и компенсацию результатов случайных и преднамеренных воздействий дестабилизирующих факторов с проверкой достоверности результатов восстановления. Алгоритм предназначен для обеспечения операций записи и чтения массивов данных в условиях отказов узлов хранения, искажений подблоков, сетевой деградации и попыток согласованной подмены эталонов целостности хранимых массивов данных. Математическую основу алгоритма образуют методы модулярной арифметики, китайская теорема об остатках и криптографическое хеширование. Массив данных представляется в виде вектора вычетов с разделением информационных и контрольных модулей системы. Проверка достоверности результата обеспечения целостности данных достигается за счет независимого глобального эталона исходного массива и локальных эталонов подблоков, размещаемых с трехкратной репликацией в обособленном кластере узлов хранения. В случае отсутствия признаков нарушения целостности данных алгоритм реализует чтение по минимальному необходимому числу подблоков и одну глобальную криптографическую проверку. При обнаружении признаков нарушения целостности данных реализуется проверка по локальным эталонам, формируется минимальное достаточное множество корректных подблоков, по которому выполняется восстановление исходного массива по китайской теореме об остатках, после чего результат проверяется путем криптографического контроля целостности и поврежденные подблоки перезаписываются, при этом локальные эталоны целостности обновляются совместно с метаданными. Предложенный алгоритм обеспечивает целостность обрабатываемых данных, локализацию подблоков с признаками нарушения целостности, раннее завершение процедур контроля и восстановления целостности данных в распределенных хранилищах.

КЛЮЧЕВЫЕ СЛОВА

Целостность данных, распределенное хранилище, модулярная арифметика, китайская теорема об остатках, криптографическая хеш-функция

Original article

DOI 10.66424/2071-8217-2026-3-15

ALGORITHM FOR DATA INTEGRITY ASSURANCE IN DISTRIBUTED STORAGES WITH COMPENSATION FOR THE RESULTS OF DESTABILIZING IMPACTS AND VERIFICATION OF RECOVERY RESULTS

G. E. Rusov*, S. A. Dichenko

Krasnodar Higher Military awarded by the Order of Zhukov and by the Orders of October Revolution and the Red Banner School named after the general of the Army S. M. Shtemenko of the Department of Defense of Russian Federation, Krasnodar, Russia

✉ *grusov1999@gmail.com

FOR CITATION

Rusov G. E., Dichenko S. A. Algorithm for data integrity assurance in distributed storages with compensation for the results of destabilizing impacts and verification of recovery results. *Problems of information security. Computer systems*. 2026. No. 3, pp. 204–215. DOI: 10.66424/2071-8217-2026-3-15 (In Russian)

RECEIVED 27.04.2026

ACCEPTED 25.08.2026

PUBLICATION 13.10.2026

ABSTRACT

An algorithm for ensuring data integrity in distributed storage systems is considered. The algorithm is aimed at monitoring the integrity of stored data and compensating for the effects of random and deliberate destabilizing factors, with verification of the reliability of recovery results. It is intended to support write and read operations for data arrays under conditions of storage node failures, sub-block corruption, network degradation, and attempts at coordinated substitution of integrity reference values for stored data arrays. The mathematical basis of the algorithm consists of modular arithmetic methods, the Chinese Remainder Theorem, and cryptographic hashing. A data array is represented as a vector of residues with separation of the system's informational and control modules. Verification of the reliability of the data integrity assurance result is achieved by means of an independent global reference value of the original array and local reference values of its sub-blocks, placed with threefold replication in an isolated cluster of storage nodes. In the absence of signs of integrity violation, the algorithm performs reading using the minimum required number of sub-blocks and a single global cryptographic check. When signs of integrity violation are detected, verification against local reference values is performed, a minimally sufficient set of correct sub-blocks is formed, and the original array is reconstructed according to the Chinese Remainder Theorem. The result is then verified by cryptographic integrity control, after which the corrupted sub-blocks are rewritten and the metadata are updated. The proposed algorithm ensures the integrity of processed data, localization of sub-blocks exhibiting signs of integrity violation, and early completion of integrity control and recovery procedures in distributed storage systems.

KEYWORDS

Data integrity, distributed storage, modular arithmetic, Chinese remainder theorem, cryptographic hash function

1. ВВЕДЕНИЕ

Для распределенных хранилищ данных, функционирующих в интересах центров обработки данных, облачных платформ и объектов критической информационной

инфраструктуры нарушение целостности данных является одним из определяющих факторов снижения доступности подключаемых к ним автоматизированных систем и сервисов [1, 2]. В отличие от локальных систем хранения, в распределенной среде

нарушения целостности данных могут быть обусловлены не только деградацией носителей информации и программными сбоями, но и частичными отказами узлов хранения, а также преднамеренными подменами эталонов целостности и искажениями данных со стороны нарушителя [1–4].

Особую сложность обеспечения целостности данных в распределенных хранилищах представляют не только полные отказы, проявляющиеся как недоступность отдельных подблоков, но и скрытые нарушения целостности, при которых массив данных остается формально доступным, однако содержит искаженные фрагменты. В таких условиях механизм обеспечения целостности данных должен обеспечивать не только выявление признаков нарушения, но и формирование достоверного результата восстановления, допускающего предоставление доступа пользователю.

Известные подходы к обеспечению целостности данных в распределенных хранилищах условно могут быть разделены на три группы:

1. Группа, основанная на резервировании и репликации данных. Обеспечивает высокую вероятность доступности хранимых данных, однако сопровождается высоким уровнем избыточности и не исключает дальнейшую обработку поврежденных массивов данных [5, 6].

2. Включает криптографические средства, использующие хеш-функции и механизмы контроля целостности данных. Такие методы позволяют обнаружить признаки нарушения целостности хранимых данных, но не решают задачу локализации поврежденных подблоков и последующего восстановления исходных массивов [7–11].

3. Основывается на алгебраических методах, в основном на применении аппарата модулярной арифметики и китайской теоремы об остатках. Указанные методы обеспечивают контроль и восстановление целостности данных при сравнительно малом уровне вводимой избыточности, однако в условиях функционирования объектов критической информационной инфраструктуры должны быть дополнены криптографическими средствами, для

подтверждения достоверности результатов восстановления [12, 13].

Для применения в распределенных хранилищах необходим алгоритм, который объединяет механизмы контроля целостности данных, локализации поврежденных подблоков данных, алгебраическое восстановление их целостности, а также возможность проверки результата восстановления с криптографической стойкостью, что обеспечивает компенсацию результатов возмущений дестабилизирующих факторов [1–4, 6, 12–15]. При отсутствии признаков нарушения целостности данных алгоритм должен ограничиваться минимально необходимым числом обращений к узлам хранения, поскольку это приводит к неоправданному росту вычислительной и сетевой нагрузки, а при выявлении искажений должен завершать процедуру после получения достоверно подтвержденного результата восстановления [1–4].

Целью исследования является разработка алгоритма обеспечения целостности данных в распределенных хранилищах, реализующего регламент обработки операций записи и чтения, поддержку подтвержденной целостности, локализацию подблоков с признаками нарушения целостности и проверку достоверности результатов восстановления. Статья задает последовательность действий, подлежащих реализации в подсистеме обеспечения целостности данных распределенных хранилищ.

2. МЕТОДЫ

Исходные данные. Рассматривается распределенное хранилище со множеством узлов хранения $S = \{s_1, s_2, \dots, s_{|S|}\}$ и выделенным кластером хранения эталонов $H = H''$, логически и физически отделенным от S . На вход поступает массив данных M , подлежащий размещению в распределенном хранилище. Целесообразность выделения отдельного кластера эталонов целостности определяется необходимостью исключения согласованной подмены самих данных и их эталонов целостности в одном домене хранения [7–11, 15].

К алгоритму предъявляется ряд требований:

- доступ к массиву данных должен предоставляться только при соблюдении условия подтверждения результата восстановления целостности исходного массива данных;

- при выявлении признаков нарушения целостности данных должна обеспечиваться локализация искаженных подблоков без полного перебора подблоков массива данных;

- компенсация результатов воздействия дестабилизирующих факторов должна приводить не только к получению корректного массива данных, но и восстановлению рабочего состояния распределенного хранилища за счет перезаписи поврежденных подблоков и сохранения корректирующей способности.

С учетом изложенного алгоритм целесообразно представить в виде двух взаимосвязанных контуров. Подготовительный контур реализуется при записи массива данных и вводит избыточность для последующего обеспечения целостности: вектор вычетов, независимые глобальный и локальные эталоны целостности, метаданные размещения подблоков на узлах хранения. Эксплуатационный контур применяется при чтении запрашиваемого массива данных и включает процедуру, предусматривающую первичное восстановление по минимальному достаточному числу подблоков с последующей глобальной проверкой, а при выявлении признаков нарушения целостности – адресную диагностику, повторное восстановление и проверку достоверности полученного результата [3, 4, 6, 12, 14, 15].

Используемые обозначения: M – массив данных, подлежащий размещению и обработке в распределенном хранилище; S' – множество узлов хранения основных данных и выделенный кластер хранения эталонов; p_i – попарно взаимно простые основания системы; k, n – число информационных оснований и общее число оснований системы; m_i – остаток, соответствующий i -му подблоку данных; H, H_i – глобальный эталон массива и локаль-

ный эталон i -го подблока; M', M'' – массив данных с восстановленной целостностью после исключения искаженных подблоков; H', H'' – хеш-код от массива данных после восстановления его целостности; P_k – рабочий диапазон системы; B_i – ортогональный базис.

Математическое описание алгоритма. Математическую основу алгоритма образуют: модулярная арифметика, китайская теорема об остатках и криптографическая хеш-функция. Пусть задана система попарно взаимно простых модулей $(p_1, p_2, \dots, p_k, p_{k+1}, \dots, p_n)$, в которой $(p_1, p_2, \dots, p_k)$ – информационные модули системы, $(p_{k+1}, \dots, p_n)$ – контрольные модули системы, $P_k = \prod_{i=1}^k p_i$ – рабочий диапазон системы [7–11, 12, 13].

Переход от исходного вида массива данных M к набору подблоков m_i , которые далее размещаются в распределенном хранилище задается формулой

$$m_i = M \bmod p_i, \quad i = 1, 2, \dots, n. \quad (1)$$

Для обеспечения однозначного восстановления целостности данных по правилам модулярной арифметики должно выполняться условие:

$$M < P_k. \quad (2)$$

Полученные значения m_i рассматриваются как подблоки поступающего на хранение массива данных M , размещаемые на узлах распределенного хранилища. Наличие контрольных модулей обеспечивает корректирующую способность и делает возможным восстановление массива данных по минимальному достаточному числу корректных подблоков:

$$M' = \left(\sum_{i=1}^k m_i k_i B_i' \right) \bmod P_k, \quad (3)$$

где $B_i = \frac{P_k}{p_i}$, $k_i = B_i^{-1} \pmod{p_i}$.

Формула (3) отражает принцип восстановления исходного массива по достаточному множеству корректных подблоков [12, 13]. Вычисления выполняются по китайской теореме об остатках.

$$H = h(M), H_i = h(m_i),$$

где $i=1,2,...,n$; h – криптографическая хеш-функция. Глобальный эталон H предназначен для контроля целостности запрашиваемого массива данных, тогда как локальные эталоны H_i используются для адресной диагностики подблоков, участвующих в восстановлении. Эталонные значения хранятся в кластере S' с трехкратной репликацией [9–11, 15]:

$$h(M') = H'. \quad (4)$$

Проверка условия $H = H'$ после первичного восстановления исходного значения M' , или $H = H''$ при условии обнаружения признаков нарушения целостности данных при $H \neq H'$, задаваемого выражением (4), обеспечивает подтверждение достоверности результата восстановления. При невыполнении данного условия полученный результат не может рассматриваться как подтвержденный и, следовательно, не подлежит предоставлению пользователю.

Подготовительный контур алгоритма. Подготовительный контур алгоритма выполняется при поступлении массива данных M на хранение и выполняет преобразования, необходимые для дальнейшего обеспечения целостности. В отличие от схемы кругового размещения подблоков данных на узлы хранения, рассматриваемый алгоритм на этапе записи заранее формирует как алгебраическую, так и криптографическую основу последующих операций восстановления.

Контур записи включает восемь последовательно выполняемых блоков (рис. 1):

1. Задается система модулей p_i и параметры k, n , определяющие объем рабочего диапазона и корректирующую способность алгоритма.

2. Массив данных M поступает в распределенное хранилище.

3. Для массива M вычисляется значение глобального криптографического эталона целостности $H = h(M)$. Далее формируются три реплики эталона и размещаются на различных узлах выделенного кластера S' .

4. Выполняется кодирование массива M в вектор вычетов $M = (m_1, m_2, ..., m_n)$ по формуле (1).

5. Для каждого подблока m_i вычисляется локальный криптографический эталон целостности $H_i = h(m_i)$. Локальные эталоны также сохраняются в трех копиях и размещаются в S' .

6. Подблоки m_i размещаются на узлах хранения в соответствии с правилом выбора узла, учитывающим текущее состояние ресурса, сетевую задержку, вычислительную нагрузку, долю свободного пространства и эксплуатационную активность узла.

7. Формируются и фиксируются метаданные: адреса размещения подблоков, сведения о копиях эталонов целостности и параметры корректирующей способности.

8. После завершения процедур подготовки массив данных сохраняется в распределенном хранилище, а его последующее чтение и восстановление выполняются в рамках алгоритма обеспечения подтвержденной целостности.

Таким образом, подготовительный контур не ограничивается размещением данных в хранилище, а формирует условия, в которых каждый массив данных сопровождается средствами подтверждения корректности для последующего восстановления его целостности. За счет вынесения криптографических эталонов в обособленный кластер достигается их обособление от основных данных, что принципиально важно для противодействия согласованным подменам.

Эксплуатационный контур алгоритма. Эксплуатационный контур активируется при получении системой запроса на доступ к массиву данных и реализует обработку в двух режимах. Первый режим соответствует состоянию отсутствия признаков нарушения целостности при глобальной проверке. Второй режим реализуется только при обнаружении признаков нарушения целостности данных при глобальной проверке и предназначен для локализации искаженных подблоков,

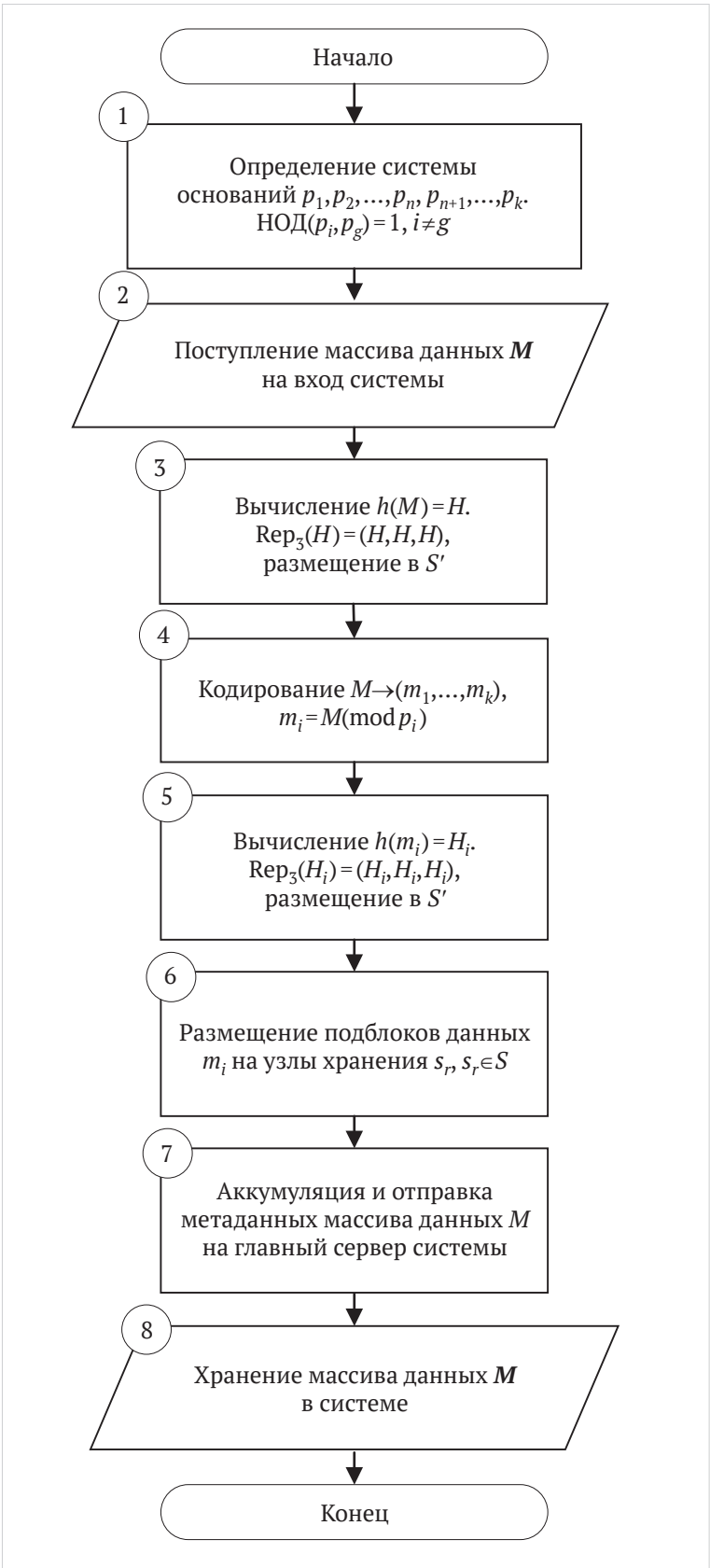


Рис. 1 | Функциональная схема подготовительного контура алгоритма

Fig. 1 | Functional diagram of the preparatory loop of the algorithm

восстановления массива и подтверждения достоверности полученного результата.

Структура предлагаемого алгоритма обеспечения целостности данных с компенсацией результатов воздействий дестабилизирующих факторов и проверкой достоверности результатов восстановления представлена на рис. 2.

Предлагаемый алгоритм целесообразно представить в виде последовательности четырех сегментов, реализующих инициализацию доступа к запрашиваемому массиву данных, первичное восстановление

и глобальную проверку целостности, локализацию результатов деструктивных воздействий, а также повторное восстановление массива данных с последующим подтверждением достоверности полученного результата. Указанный порядок обеспечивает однозначное понимание назначения отдельных блоков алгоритма и последовательности переходов между ними.

В первом сегменте осуществляется инициализация доступа к массиву данных M и определение эталонов целостности. В блоке 1 пользователь автоматизирован-

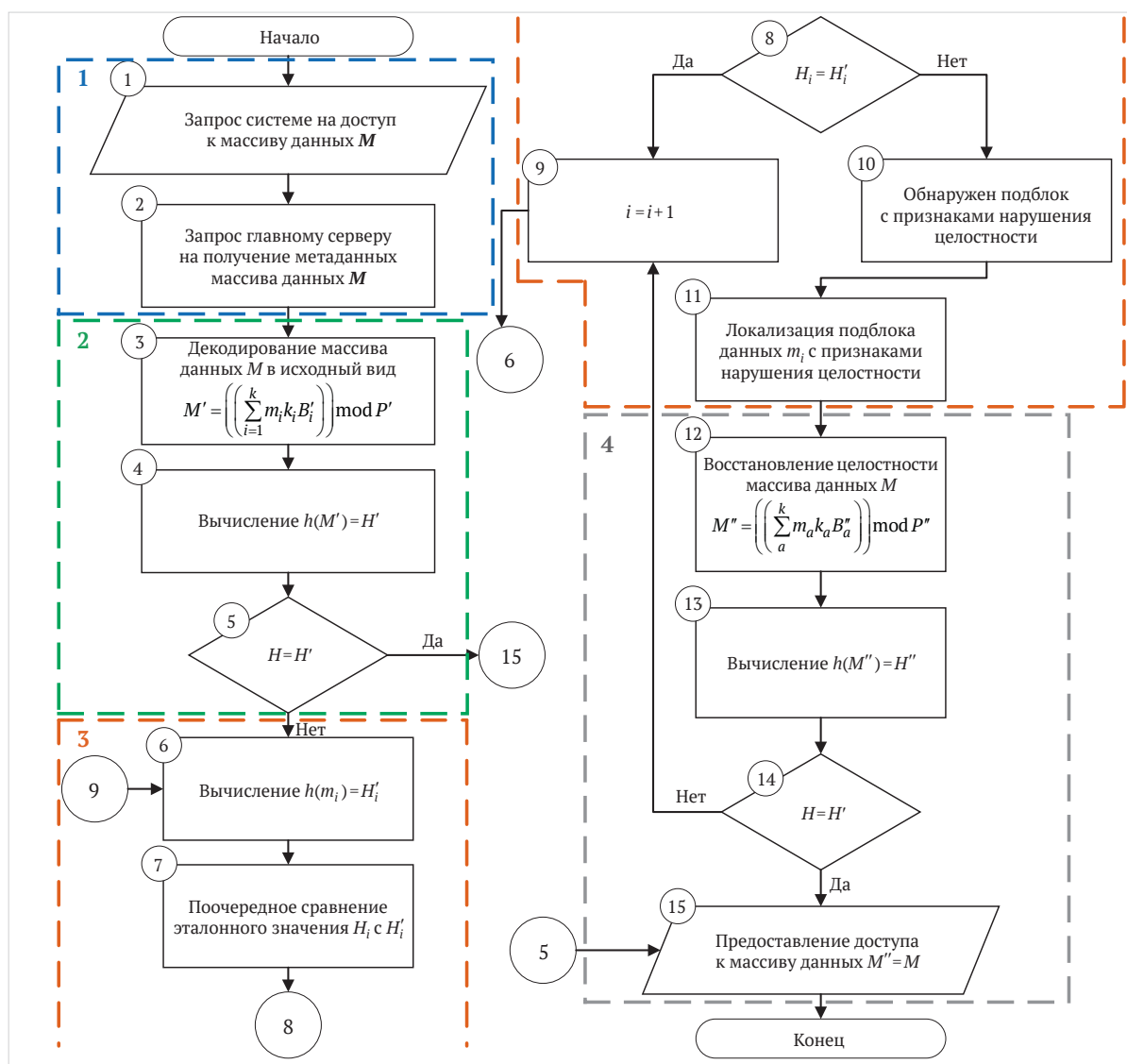


Рис. 2 | Функциональная схема эксплуатационного контура алгоритма

Fig. 2 | Functional diagram of the operational circuit of the algorithm

ной системы направляет запрос на получение массива данных. В блоке 2 главный сервер управления формирует и передает сведения о размещении подблоков массива данных на узлах хранения, а также значения эталонных хеш-кодов, соответствующих запрашиваемому массиву данных и его подблокам. Тем самым обеспечиваются условия для последующего восстановления массива данных и выполнения процедур контроля целостности.

Второй сегмент предназначен для первичного восстановления массива данных и выполнения глобального криптографического контроля целостности. В блоке 3 по минимальному необходимому множеству подблоков осуществляется восстановление массива данных M' в исходный вид с использованием аппарата модулярной арифметики и китайской теоремы об остатках. В блоке 4 для полученного значения вычисляется глобальный хеш-код H' . В блоке 5 вычисленное значение H' сопоставляется с эталонным значением H . При выполнении условия $H = H'$ делается вывод об отсутствии признаков нарушения целостности, после чего осуществляется переход к блоку 15, в котором пользователю предоставляется доступ к рассматриваемому массиву данных. В противном случае фиксируется наличие признаков нарушения целостности данных, и алгоритм переходит к контролю подблоков массива.

Третий сегмент реализует поэлементную проверку подблоков и локализацию результатов воздействий дестабилизирующих факторов. В блоке 6 для очередного подблока массива данных вычисляется текущее значение локального хеш-кода H_i' . В блоке 7 он сопоставляется с соответствующим эталонным значением H_i . Блок 8 предназначен для фиксации отсутствия признаков нарушения целостности в рассматриваемом подблоке. В этом случае в блоке 9 осуществляется переход к следующему подблоку массива данных. При выявлении несоответствия $H_i \neq H_i'$ в блоке 10 фиксируется наличие искаженного подблока, а в блоке 11 он исключается из дальнейших вычислений. Таким образом, на данном этапе обеспечивается лока-

лизация подблоков, содержащих признаки нарушения целостности, и формирование корректного подмножества данных, пригодного для последующего восстановления массива.

Четвертый сегмент предназначен для восстановления целостности запрашиваемого массива данных, проверки достоверности результата восстановления и компенсации последствий воздействий дестабилизирующих факторов. В блоке 12 по минимальному достаточному множеству подблоков, не исключенных на предыдущем этапе, повторно выполняется восстановление значения массива данных M'' . В блоке 13 вычисляется глобальный хеш-код H'' восстановленного массива. В блоке 14 осуществляется проверка условия $H = H''$, при выполнении которого результат восстановления признается достоверным, после чего в блоке 15 пользователю предоставляется доступ к массиву данных $M'' = M$. В противном случае восстановленный результат не может рассматриваться как достоверный, что исключает возможность предоставления пользователю формально восстановленного, но фактически искаженного массива данных.

Следует отметить, что завершение четвертого сегмента не ограничивается восстановлением значения запрашиваемого массива. После подтверждения достоверности результата восстановления выполняются пересчет поврежденных подблоков, их повторная запись на узлы хранения и актуализация метаданных. За счет этого обеспечивается не только восстановление целостности запрашиваемых данных, но и компенсация последствий воздействий дестабилизирующих факторов.

Таким образом, предлагаемый алгоритм сочетает процедуры алгебраического восстановления данных с двухуровневым криптографическим контролем, что обеспечивает раннее завершение операций при отсутствии нарушений целостности, локализацию искаженных подблоков, подтверждение достоверности результатов восстановления и последующее приведение распределенного хранилища в состояние, допускающее его дальнейшее функционирование.

3. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Из рассмотренной последовательности действий следует, что предлагаемый алгоритм обладает рядом функциональных свойств, определяющих его применимость в распределенных хранилищах данных.

Первое свойство алгоритма состоит в обеспечении раннего завершения процедуры предоставления доступа к массиву данных при отсутствии признаков нарушения его целостности. Это достигается за счет того, что после первичного восстановления массива данных выполняется глобальная криптографическая проверка, и при совпадении вычисленного и эталонного хеш-кодов дальнейшие процедуры контроля не инициируются. За счет этого исключаются избыточные обращения к узлам хранения и уменьшается вычислительная нагрузка на распределенное хранилище [1–4].

Второе свойство алгоритма заключается в локализации результатов воздействий дестабилизирующих факторов. В случае нарушения условия глобальной проверки осуществляется переход к поэлементному контролю подблоков массива данных с использованием локальных эталонных хеш-кодов [3, 4, 12–14]. Это позволяет выявлять подблоки, содержащие признаки нарушения целостности, и исключать их из последующих вычислений. За счет этого исключается неоднозначность получаемых результатов, и уменьшается объем дополнительных вычислений, необходимых для восстановления массива данных.

Третье свойство алгоритма связано с подтверждением достоверности результатов восстановления. После локализации искаженных подблоков и повторного восстановления массива данных выполняется повторная глобальная криптографическая проверка полученного результата [7–11, 12, 13, 15]. Тем самым решение о корректности восстановления принимается не по факту завершения алгебраической процедуры, а на основе критерия достоверности. Это исключает получение результата, формально соответствующего процедуре восстановления, но неподтвержденного по признаку целостности.

Четвертое свойство алгоритма заключается в компенсации последствий воздействий дестабилизирующих факторов. После подтверждения достоверности результата восстановления выполняются пересчет поврежденных подблоков, их повторная запись на узлы хранения и актуализация служебной информации о размещении массива данных. Тем самым обеспечивается восстановление не только исходного массива данных, но и работоспособного состояния распределенного хранилища без прекращения ее функционирования.

Пятое свойство алгоритма состоит в согласованном использовании алгебраических и криптографических процедур в рамках обеспечения целостности данных. Аппарат модулярной арифметики обеспечивает возможность восстановления массива данных по корректному подмножеству подблоков, тогда как криптографический контроль позволяет подтвердить достоверность как промежуточных, так и итоговых результатов. Такое сочетание процедур обеспечивает требуемый уровень защищенности распределенного хранилища от различных дестабилизирующих воздействий без существенного увеличения объема вводимой избыточности (см. таблицу).

Следовательно, предлагаемый алгоритм ориентирован не только на обнаружение и устранение нарушений целостности данных, но и на обеспечение достоверности результатов восстановления, что имеет принципиальное значение для распределенных хранилищ, используемых в составе объектов критической информационной инфраструктуры.

К условиям применимости алгоритма относятся: взаимная простота оснований системы, выполнение ограничения $M < P_k$, достижимость достаточного числа корректных подблоков для восстановления, а также обособленность и доступность кластера эталонов S' . При соблюдении этих условий алгоритм может применяться как в хранилищах общего назначения, так и в системах, для которых существенное значение имеют достоверность результатов восстановления и ограничение времени простоя, в том числе в составе объектов критической информационной инфраструктуры [1–4, 6, 12, 13, 15].

Компенсация результатов воздействий дестабилизирующих факторов средствами алгоритма

Compensation for the effects of destabilizing factors using algorithmic means

Дестабилизирующий фактор	Процедура алгоритма	Результат
Частичная недоступность узлов хранения	Первичное или повторное восстановление массива по минимально достаточному множеству корректных подблоков с использованием корректирующей способности модулярного представления данных	Сохранение возможности восстановления массива данных при отказе части узлов хранения
Нарушение целостности отдельного подблока	Поэлементная криптографическая проверка подблоков, сопоставление локальных хеш-кодов с эталонными значениями и исключение искаженного подблока из дальнейших вычислений	Локализация искаженного подблока и исключение его влияния на результат восстановления
Согласованное искажение данных и контрольных признаков	Независимое хранение эталонных хеш-кодов в выделенном кластере и повторная глобальная криптографическая проверка результата восстановления	Подтверждение достоверности восстановленного массива данных
Рост времени доступа к узлам хранения и увеличение нагрузки распределенной среды	Использование минимально достаточного множества подблоков и завершение процедуры после первой успешной глобальной проверки	Уменьшение среднего времени доступа к массиву данных и снижение вычислительной нагрузки на систему
Сохранение последствий нарушения целостности после завершения восстановления	Пересчет поврежденных подблоков, их повторная запись в хранилище и актуализация метаданных размещения	Восстановление работоспособного состояния подсистемы хранения после компенсации последствий нарушения

Принципиальной особенностью алгоритма является то, что решение о корректности результата восстановления принимается не по факту завершения алгебраической процедуры как таковой, а по результатам независимой глобальной криптографической проверки. За счет этого исключается получение результата, формально соответствующего процедуре восстановления, но неподтвержденного по критерию достоверности.

4. ЗАКЛЮЧЕНИЕ

Предложен алгоритм обеспечения целостности данных в распределенных хранилищах, ориентированный на работу в условиях случайных и преднамеренных воздействий дестабилизирующих факторов. В отличие от традиционного раздельного применения криптографических и алгебраических средств, алгоритм объединяет модулярное кодирование, независимый двухуровневый криптографический контроль целостности, адресную локали-

зацию подблоков с признаками нарушения целостности данных и обязательную проверку достоверности результата восстановления.

Алгоритм представлен в виде двух взаимосвязанных контуров. Подготовительный контур выполняет кодирование массива, формирование глобального и локальных эталонов целостности, а также размещение подблоков на узлы хранения и определение метаданных. Эксплуатационный контур реализует быстрое чтение по минимальному необходимому множеству подблоков, углубленную диагностику при обнаружении признаков нарушения целостности данных, восстановление массива по достаточному множеству корректных подблоков и последующую компенсацию результатов воздействий дестабилизирующих факторов.

Полученные результаты могут быть использованы при проектировании распределенных хранилищ различного назначения, в том числе в системах, для которых критичны достоверность результата восстановления целостности и минимизация времени простоя.

КОНФЛИКТ ИНТЕРЕСОВ / CONFLICT OF INTERESTS

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests.

СПИСОК ИСТОЧНИКОВ

1. Li A., Chen Y., Yan Z. et al. A Survey on Integrity Auditing for Data Storage in the Cloud: From Single Copy to Multiple Replicas // *IEEE Transactions on Big Data*. 2022. Vol. 8. № 5. P. 1428–1442. DOI: 10.1109/TBDATA.2020.3029209.
2. Zhao Y., Qu Y., Xiang Y. et al. A Comprehensive Survey on Edge Data Integrity Verification: Fundamentals and Future Trends // *ACM Computing Surveys*. 2025. Vol. 57. № 1. Art. 8. P. 1–34.
3. Liu D., Li Z., Jia D. Secure Distributed Data Integrity Auditing with High Efficiency in 5G-Enabled Software-Defined Edge Computing // *Cyber Security and Applications*. 2023. Vol. 1. Art. 100004. DOI: 10.1016/j.csa.2022.100004.
4. Ye J., Jiang Y. Data Integrity Verification for Edge Computing Environments // *Symmetry*. 2024. Vol. 16. № 12. Art. 1648. DOI: 10.3390/sym16121648.
5. Shen Z., Cai Y., Cheng K. et al. A Survey of the Past, Present, and Future of Erasure Coding for Storage Systems // *ACM Transactions on Storage*. 2025. Vol. 21. № 1. Art. 4. P. 1–39. DOI: 10.1145/3708994.
6. Chen G., Hao R. Enabling Flexible Multiple-Replica Cloud Storage Integrity Auditing for Cloud-Based IoT Data // *Journal of Systems Architecture*. 2025. Vol. 163. Art. 103404. DOI: 10.1016/j.sysarc.2025.103404.
7. Shen W., Qin J., Yu J. et al. Data Integrity Auditing without Private Key Storage for Secure Cloud Storage // *IEEE Transactions on Cloud Computing*. 2021. Vol. 9. № 4. P. 1408–1421.
8. Yang A., Xu J., Weng J. et al. Lightweight and Privacy-Preserving Delegatable Proofs of Storage with Data Dynamics in Cloud Storage // *IEEE Transactions on Cloud Computing*. 2021. Vol. 9. № 1. P. 212–225.
9. Li R., Wang X. A., Yang H. et al. Efficient Certificateless Public Integrity Auditing of Cloud Data with Designated Verifier for Batch Audit // *Journal of King Saud University – Computer and Information Sciences*. 2022. Vol. 34. № 10. Part A. P. 8079–8089.
10. Bian G., Zhang F., Li R., Shao B. Certificateless Remote Data Integrity Auditing with Access Control of Sensitive Information in Cloud Storage // *Electronics*. 2022. Vol. 11. № 19. Art. 3116. DOI: 10.3390/electronics11193116.
11. Wen J., Deng L. Certificateless Integrity Auditing Scheme for Sensitive Information Protection in Cloud Storage // *Journal of Systems Architecture*. 2024. Vol. 156. Art. 103267. DOI: 10.1016/j.sysarc.2024.103267.
12. Dichenko S. A. An Integrity Control Model for Multidimensional Data Arrays // *Automatic Control and Computer Sciences*. 2021. Vol. 55. № 8. P. 1188–1193. DOI: 10.3103/S0146411621080368.
13. Диченко С. А., Самойленко Д. В., Финько О. А., Рюмшин К. Ю. Метод параметрического синтеза крипто-кодированных структур для контроля и восстановления целостности информации // *Вопросы кибербезопасности*. 2023. № 2 (54). С. 36–51. DOI: 10.21681/2311-3456-2023-2-36-51.
14. Ding Y., Li Y., Yang W., Zhang K. Edge Data Integrity Verification Scheme Supporting Data Dynamics and Batch Auditing // *Journal of Systems Architecture*. 2022. Vol. 128. Art. 102560.
15. Wang H., Wan Z., He D., Yu J. Synchronous Blockchain-Based Distributed Provable Data Possession With Forward-Security // *IEEE Transactions on Services Computing*. 2024. Vol. 17. № 3. P. 1227–1238.

REFERENCES

1. Li A., Chen Y., Yan Z. et al. A Survey on Integrity Auditing for Data Storage in the Cloud: From Single Copy to Multiple Replicas. *IEEE Transactions on Big Data*. 2022. Vol. 8. No. 5, pp. 1428–1442. DOI: 10.1109/TBDATA.2020.3029209.

2. **Zhao Y., Qu Y., Xiang Y. et al.** A Comprehensive Survey on Edge Data Integrity Verification: Fundamentals and Future Trends. *ACM Computing Surveys*. 2025. Vol. 57. No. 1. Art. 8, pp. 1–34.
3. **Liu D., Li Z., Jia D.** Secure Distributed Data Integrity Auditing with High Efficiency in 5G-Enabled Software-Defined Edge Computing. *Cyber Security and Applications*. 2023. Vol. 1. Art. 100004. DOI: 10.1016/j.csa.2022.100004.
4. **Ye J., Jiang Y.** Data Integrity Verification for Edge Computing Environments. *Symmetry*. 2024. Vol. 16. No. 12. Art. 1648. DOI: 10.3390/sym16121648.
5. **Shen Z., Cai Y., Cheng K. et al.** A Survey of the Past, Present, and Future of Erasure Coding for Storage Systems. *ACM Transactions on Storage*. 2025. Vol. 21. No. 1. Art. 4, pp. 1–39. DOI: 10.1145/3708994.
6. **Chen G., Hao R.** Enabling Flexible Multiple-Replica Cloud Storage Integrity Auditing for Cloud-Based IoT Data. *Journal of Systems Architecture*. 2025. Vol. 163. Art. 103404. DOI: 10.1016/j.sysarc.2025.103404.
7. **Shen W., Qin J., Yu J. et al.** Data Integrity Auditing without Private Key Storage for Secure Cloud Storage. *IEEE Transactions on Cloud Computing*. 2021. Vol. 9. No. 4, pp. 1408–1421.
8. **Yang A., Xu J., Weng J. et al.** Lightweight and Privacy-Preserving Delegatable Proofs of Storage with Data Dynamics in Cloud Storage. *IEEE Transactions on Cloud Computing*. 2021. Vol. 9. No. 1, pp. 212–225.
9. **Li R., Wang X. A., Yang H. et al.** Efficient Certificateless Public Integrity Auditing of Cloud Data with Designated Verifier for Batch Audit. *Journal of King Saud University – Computer and Information Sciences*. 2022. Vol. 34. No. 10. Part A, pp. 8079–8089.
10. **Bian G., Zhang F., Li R., Shao B.** Certificateless Remote Data Integrity Auditing with Access Control of Sensitive Information in Cloud Storage. *Electronics*. 2022. Vol. 11. No. 19. Art. 3116. DOI: 10.3390/electronics11193116.
11. **Wen J., Deng L.** Certificateless Integrity Auditing Scheme for Sensitive Information Protection in Cloud Storage. *Journal of Systems Architecture*. 2024. Vol. 156. Art. 103267. DOI: 10.1016/j.sysarc.2024.103267.
12. **Dichenko S. A.** An Integrity Control Model for Multidimensional Data Arrays. *Automatic Control and Computer Sciences*. 2021. Vol. 55. No. 8, pp. 1188–1193. DOI: 10.3103/S0146411621080368.
13. **Dichenko S. A., Samoylenko D. V., Finko O. A., Ryumshin K. Yu.** A method of parametric synthesis of crypto-code structures for monitoring and restoring the integrity of information. *Voprosy kiberbezopasnosti*. 2023. No. 2 (54), pp. 36–51. DOI: 10.21681/2311-3456-2023-2-36-51. (In Russian)
14. **Ding Y., Li Y., Yang W., Zhang K.** Edge Data Integrity Verification Scheme Supporting Data Dynamics and Batch Auditing. *Journal of Systems Architecture*. 2022. Vol. 128. Art. 102560.
15. **Wang H., Wan Z., He D., Yu J.** Synchronous Blockchain-Based Distributed Provable Data Possession With Forward-Security. *IEEE Transactions on Services Computing*. 2024. Vol. 17. No. 3, pp. 1227–1238.

СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

РУСОВ Герман Евгеньевич – адъюнкт, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко Министерства обороны Российской Федерации, Россия, 350063, Краснодар, Красина ул., д. 4
E-mail: grusov1999@gmail.com
ORCID: 0009-0005-4352-9099

ДИЧЕНКО Сергей Александрович – д-р техн. наук, начальник первого управления научно-исследовательского центра, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко Министерства обороны Российской Федерации, Россия, 350063, Краснодар, Красина ул., д. 4
E-mail: dichenko.sa@yandex.ru
ORCID: 0000-0002-0644-4353

RUSOV German E. – Adjunct, Krasnodar Higher Military awarded by the Order of Zhukov and by the Orders of October Revolution and the Red Banner School named after the general of the Army S. M. Shtemenko of the Department of Defense of Russian Federation, Russia, 350063, Krasnodar, Krasina str., 4

DICHENKO Sergey A. – Doctor of Engineering Sciences, Head of the 1st Directorate of the Research Center, Krasnodar Higher Military awarded by the Order of Zhukov and by the Orders of October Revolution and the Red Banner School named after the general of the Army S. M. Shtemenko of the Department of Defense of Russian Federation, Russia, 350063, Krasnodar, Krasina str., 4