УДК 004.056.55 **DOI: 10.34670/AR.2025.16.59.013**

Исследование эффективности хеш-функций для обеспечения целостности данных

Поначугин Александр Викторович

Кандидат экономических наук, доцент,
заведующий кафедрой прикладной информатики
и информационных технологий в образовании,
Нижегородский государственный
педагогический университет им. К. Минина,
603005,Российская Федерация, Нижний Новгород, ул. Ульянова, 1;
e-mail: Ponachygin_AV@mininuniver.ru

Базуева Александра Сергеевна

Студент,
кафедра прикладной информатики
и информационных технологий в образовании,
Нижегородский государственный
педагогический университет им. К. Минина,
603005,Российская Федерация, Нижний Новгород, ул. Ульянова, 1;
e-mail: bazueva_sasha@mail.ru

Батяев Никита Андреевич

Студент,
кафедра прикладной информатики
и информационных технологий в образовании,
Нижегородский государственный
педагогический университет им. К. Минина,
603005,Российская Федерация, Нижний Новгород, ул. Ульянова, 1;
e-mail: neket.1992@mail.ru

Аннотация

Современные цифровые технологии предъявляют высокие требования к защите данных, ключевым элементом которой выступает контроль целостности. В статье представлен всесторонний анализ популярных хеш-функций, выявляющий их сильные и слабые стороны в контексте обеспечения безопасности данных. Предлагается методология, позволяющая проводить сопоставимый анализ производительности, устойчивости к коллизиям и чувствительности к изменениям данных. Полученные результаты служат основой для выработки практических рекомендаций по выбору подходящей хеш-функции в различных классах информационных систем.

Для цитирования в научных исследованиях

Поначугин А.В., Базуева А.С., Батяев Н.А. Исследование эффективности хеш-функций для обеспечения целостности данных // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 10А. С. 150-160. DOI: 10.34670/AR.2025.16.59.013

Ключевые слова

Хеш-функции, целостность данных, криптография, защита информации, устойчивость к коллизиям, информационная безопасность, алгоритмы шифрования, сравнительный анализ.

Введение

Рост цифровой экономики приводит к увеличению внимания к вопросам защиты данных, особенно в контексте обеспечения их целостности. В теории информационной безопасности и в ряде регулирующих предметную область стандартов под целостностью понимается неизменность внесенной информации, ее соответствие логике, структуре, правилам работы с ней. Если администратором вводится новое правило работы, связанное с возможностью несанкционированной модификации данных, например, неоправданное расширение привилегий пользователей, это признается ограничением целостности.

Целостность данных — это понятие, подразумевающее защиту информации от любых несанкционированных изменений, возникающих намеренно или случайно. Нарушения целостности ставят под угрозу конфиденциальность хранимых и передаваемых данных, что негативно сказывается на работоспособность отдельных компаний или даже целых секторов экономики.

Вопросу поддержания целостности данных уделяется большое внимание, для этого особое место занимает группа методов, направленных на распознавание и регистрацию данных. Среди этих методов как раз выделяют криптографические хеш-функции.

Если говорить про принцип работы хеш-функций, то его можно выразить в следующей формулировке - получая некоторые исходные данные, хеш-функции на выходе дают уникальные цифровые отпечатки, которые называются хеш-значениями. При этом, каждое изменение входных данных, даже самое незначительное, будет приводить к изменению конечного значения хеш-значения. Это свойство позволяет обнаружить факт вмешательства или факт повреждения данных.

Одной из актуальнейших для подобных систем задач является организация безопасного хранения данных, а с учетом таких условий функционирования – обеспечение их целостности. Обеспечение целостности данных является сложной задачей, ввиду своей комплексности, так как включает в себя и восстановление, и контроль целостности данных. Одним из известных и широко используемых способов контроля целостности данных является применение криптографических методов, в частности, функции хэширования. Однако, несмотря на повсеместное применение хэш-функций, они крайне мало исследованы, а практические предложения по их применению весьма немногочисленны и характеризуются рядом недостатков, связанных, с необходимостью введения высокой избыточности контрольной информации. В условиях ограничения на существующий ресурс систем хранения данных это может привести к снижению вероятности выполнения задачи их функционирования или вообще к ее невыполнению.

Таким образом, это исследование направлено на устранение пробелов в понимании характеристик хеш-функций и способствует улучшению уровня информационной безопасности в условиях современного цифрового преобразования.

Основная часть

Развитие цифровой экономики выдвигает особые требования к информационной безопасности, одной из центральных составляющих которой является гарантия сохранения целостности данных. Нарушение целостности информации угрожает конфиденциальности и надежности хранящихся и передаваемых данных, что негативно сказывается на функционировании как отдельных организаций, так и целых отраслей экономики.

«Целостность данных — это сложный процесс, который состоит из двух компонентов, которые взаимосвязаны межу собой. Первый компонент связан с предотвращением любых несанкционированных манипуляций над информацией» [Аблаев, Зиятдинов, 2020, 14]. Эта задача подразумевает поддержание первоначальных характеристик данных на протяжении всего жизненного цикла, начиная от момента их создания и заканчивая архивированием либо удалением. Это значит, что «любая попытка внесения изменений, независимо от мотивов инициатора (случайность или злонамеренность), должна быть пресечена», как пишет Ф. М. Аблаев [Аблаев, Зиятдинов, 2020, с. 16]. Достижение такого эффекта возможно исключительно при наличии высокоэффективных механизмов аутентификации и защиты данных, неотъемлемой частью которых выступают специальные методы и алгоритмы.

Вторая важная задача — это гарантированное обнаружение фактов нарушения целостности данных. Независимо от природы произошедшего события (умышленное вмешательство или случайная ошибка), необходимо иметь инструменты для оперативного распознавания изменений. Только при наличии надежного средства, которое способно немедленно зафиксировать малейшие отклонения, удается минимизировать последствия подобных инцидентов и принять соответствующие меры для устранения последствий.

Решению обеих задач способствуют специализированные алгоритмы и техники, важнейшую роль среди которых занимают хеш-функции. Суть их работы сводится к переводу исходных данных в компактные, однозначно идентифицируемые цифровые отпечатки, называемые хэш-значениями. Каждый набор данных преобразуется в уникальное значение фиксированной длины, что позволяет сравнивать состояние данных в разные моменты времени и оперативно определять наличие изменений.

Современная среда информационных технологий ставит повышенные требования к вопросам защиты данных, среди которых ключевой задачей является поддержание их целостности. Согласно ряду исследователей, эффективным решением данной проблемы выступают криптографические хеш-функции, позволяющие быстро и надежно проверять состояние данных.

Ф. М. Аблаев и М. Т. Зиятдинов подчеркивают важное качество хеш-функций – «устойчивость к созданию коллизий, достигнутое благодаря внедрению инновационных квантовых процедур» [Аблаев, Зиятдинов, 2020, с. 20]. Тем не менее, существует проблема совместимости классических методов хеширования с квантовыми технологиями, что выделяет необходимость дальнейшего изучения данной тематики.

Другими авторами отмечается растущая угроза безопасности традиционных криптографических схем вследствие развития квантовых компьютеров. Так, А. О. Бахарев

описывает новую «модель квантового оракула, предназначенную для оценки стойкости постквантовых криптосистем» [Бахарев, 2024, с. 29].

Проблематика выбора оптимальной хеш-функции рассмотрена М. А. Заболотниковой и коллегами, которые указывают на «трудности при принятии решений в условиях роста разнообразия предлагаемых алгоритмов» [Заболотникова и др., 2020, с. 125].

Кроме того, вклад А. С. Ким и коллег направлен на оценку роли хеш-функций в практике «этичного хакинга, демонстрируя потенциал этих инструментов для выявления слабых мест в инфраструктуре ИТ» [Ким и др., 2023, с. 58].

Также труды К. В. Торгашова посвящены развитию оригинальных подходов к формированию криптографических методов контроля целостности данных, основываясь на геометрическом принципе построения хеш-функций [Торгашов и др., 2022, с. 40], а М. А. Хорошев рассматривает интеграцию хеш-функций в схему шифрования RSA для увеличения безопасности промышленных систем управления SCADA [Хорошев и др., 2023, с. 113].

Так, в современном мире обеспечение целостности данных и, главное, их безопасности имеют огромную важность, потому, согласно исследованию А. В. Поначугина, В. Д. Степанова, А. С. Базуевой, «применение искусственного интеллекта способствует повышению безопасности и производительности информационно- телекоммуникационным сетей» [Поначугин и др., 2025, с. 119], а это значит, что грамотный и правильный выбор хеш-функций может гарантировать сохранность данных и обезопасить от несанкционированных изменений.

Перед тем как приступить к основному исследованию и сравнительному обзору хеш-функций, важно обратить внимание на признаки классификации и ключевые характеристики, присущие каждой группе методов, поэтому понимание различий между типами хеш-функций позволит глубже вникнуть в принципы их работы и обосновать дальнейшие выводы. Одним из начальных этапов станет анализ методов, которые базируются на формировании единого хэш-кода для множества данных, состоящих из разных блоков.

Для начала рассмотрим универсальное хеширование. При таком подходе используется не одна конкретная хеш-функция, а происходит выбор из заданного семейства по случайному алгоритму. Некоторые преимущества универсального хеширования: обычно обеспечивается низкое число коллизий. Такой метод имеет множество применений, например, в реализации хеш-таблиц и криптографии. Однако у универсального хеширования есть и недостаток — это утрата детализации при возникновении нарушений целостности данных, поскольку хэш-код охватывает сразу все блоки.

Еще одна базовая классификация методов хэширования основывается на внутреннем устройстве алгоритмов. Суть конструкции заключается в итеративном процессе последовательных преобразований, когда на вход каждой итерации поступает блок исходного текста и выход предыдущей итерации.

Более поздний подход, реализованный в SHA-3, основывается на концепции «губчатой конструкции» (sponge-construction), включающей фазы поглощения и выдавливания данных [Хорошев и др., 2023, с. 119]. Такой подход позволяет достичь большего разнообразия значений и тем самым обеспечить большую устойчивость к атакам.

Также возможна классификация по длине выходного хеша и назначению. «Одни хеш-функции формируют хеши фиксированной длины (например, 160 бит для SHA-1, 256 бит для SHA-256), другие поддерживают переменный размер, хотя такие варианты встречаются реже и обычно используются в узкоспециализированных задачах» [Бахарев, 2024, с. 47].

Далее рассмотрим характеристики трех конкретных хеш-функций, выбранных для этого

исследования: SHA-1 - 160-битный хэш, признан небезопасным с 2017 года; SHA-3 - новейшее поколение, основанное на алгоритме Keccak, который должен поддерживать семейство алгоритмов, реализующих хеш-суммы длиной 256 бит. Как минимум, одна функция из семейства должна поддерживать хеш-код аутентификации сообщений (HMAC) и рандомизированное хеширование. Кроме того, для всех n бит хеш-суммы алгоритм должен обеспечивать выполнение следующих условий:

– устойчивость к нахождению прообраза для n бит;
– устойчивость к нахождению второго прообраза для (n - L) бит, где первый прообраз имеет длину не более 2L блоков;
– устойчивость к коллизиям для n/2 бит;
– устойчивость к атакам дополнением сообщения;
– для любого m < n любое подмножество из m бит хеш-суммы длиной в n бит должно удовлетворять выше названным условиям, он отличается от предыдущих версий архитектурой «губки» вместо структуры Меркле-Дамгарда; SHA-256 - один из алгоритмов SHA-2, представленных в 2001 году. Он приобрел популярность благодаря значительному соотношению производительности и безопасности. Он широко используется в таких системах, как электронная почта, цифровые подписи и криптовалюты (например, Bitcoin) [Бахарев, 2024, с. 47].

Другая функция этого семейства, которую можно назвать довольно древней, - это SHA-1, разработанный еще в 1995 году. Он стал непопулярным из-за успешного обнаружения коллизий, что сделало его небезопасным для серьезного использования [Бахарев, 2024, с. 47]. Однако история этого процесса важна для понимания эволюции хеш-функций.

В центре внимания – исследование и сравнительный анализ различных хэш-функций, выявление их сильных и слабых сторон в условиях современных технологий. Основной целью данной работы является разработка единой методики оценки и выбора хэш-функций, соответствующих современному стандарту и требованиям информационной безопасности.

Мы разработали подход, состоящий из трех последовательных этапов, каждый из которых решает определенные критические проблемы в общем процессе анализа хеш-функции.

Первый этап исследования направлен на измерение времени вычисления хэш-значений при обработке данных различной длины. «Он начинается с подготовки набора входных данных разного размера - от небольших фрагментов до огромных объемов. Измеряется время вычисления множества хэш-значений, что позволяет рассчитать среднюю задержку для каждого исследуемого алгоритма» [Бахарев, 2024, с. 47]. Это позволит получить информацию о быстродействии или медленности различных хэш-функций и рекомендации по их выбору в зависимости от целевой системы. В высоконагруженных средах, крупных облачных сервисах или системах обработки транзакций и т. д. этот аспект производительности становится крайне важным.

Второй этап исследования сосредоточен на определении вероятности возникновения коллизий, то есть ситуаций, когда два разных набора данных приводят к одному и тому же хеш-значению. Такая ситуация крайне нежелательна, так как нарушает основное требование уникальности хешей и открывает пути для атак злоумышленников. Цель этапа - выявить частоту возникновения коллизий для каждой хеш-функции, тем самым оценив ее устойчивость к такому виду атак. Надежность хеш-функции напрямую зависит от того, насколько трудно создать два набора данных, дающих одинаковый хеш. Тестирование осуществляется путем массового параллельного запуска множественных экспериментов с большим числом уникальных данных,

чтобы получить репрезентативную картину частоты возникновения коллизий.

Заключительный этап направлен на изучение так называемого лавинообразного эффекта - способности хеш-функции резко изменять хеш-значение при внесении сколь угодно малого изменения в исходные данные. Это свойство чрезвычайно важно для защиты от атак методом перебора или мутации данных. Изменение даже одного бита в исходных данных должно вызывать максимальное отклонение в конечном хеш-значении. Для оценки данного параметра производятся массовые манипуляции с тестовыми файлами, где вносится минимальный разрыв (например, одиночная ошибка бита), и фиксируется степень отклонения в хеш-значении. Идеальная хеш-функция должна демонстрировать максимальную разницу в «хешах» даже при самом маленьком изменении входных данных.

Такая структура методологии позволяет глубоко исследовать ключевые характеристики хеш-функций, составить взвешенные заключения и разработать рекомендации по их практическому применению в различных условиях.

Далее представим результаты исследования.

Производительность хеш-функций определялась по среднему времени, затрачиваемому на выполнение процедуры хеширования. Применялись разнообразные объемы данных, варьирующиеся от небольших файлов до массивов большого размера. Средний показатель времени вычислялся по формуле:

$$\mathrm{Tcp} = \frac{\mathrm{n}\sum \mathrm{i} = 1\mathrm{T}i}{\mathrm{n}}$$

где:

*T*ср - среднее время вычисления хеш-значения,

n - количество выполненных операций,

Ti - время вычисления хеш-значения на *i*-той итерации.

Таблица 1 - Сравнительный анализ производительности хеш-функций (время вычислений)

Время вычислений (мс)	Количество измерений
1.1	5
1.2	5
1.3	5

Расчет:

$$Tcp = \frac{n1.1 \times 5) + (1.2 \times 5) + (1.3 \times 5)}{15} = 1.2ms$$

Аналогичным образом были проведены измерения для остальных хеш-функций. Экспериментальные данные позволили получить следующие средние времена вычисления хеш-значений:

SHA-3: 1.2 мс.

SHA-256: 1.8 мс.

SHA-1: 2.1 мс.

MD5: 1.5 мс.

Проведенная серия испытаний однозначно продемонстрировала, что алгоритм SHA-3 обладает наименьшим средним временем вычисления хеш-значений, что позволяет рекомендовать его для применения в системах, испытывающих значительные нагрузки на процессор и имеющих высокие требования к быстроте обработки данных.

Вторым этапом было исследование устойчивости к коллизиям. Коллизии возникают, когда различные данные приводят к одним и тем же хеш-значениям. Чтобы избежать таких ситуаций, необходима высокая устойчивость к этому типу атак. Количественно устойчивость выражалась через коэффициент коллизий, рассчитываемый следующим образом:

$$Kc = \frac{Nk}{Np} \times 100\%$$

где:

Kc - коэффициент коллизий,

Nk - количество зафиксированных коллизий,

Np - общее количество проверок.

Пример расчета для SHA-3:

Количество коллизий (Nk) = 1

Всего испытаний (Np) = 1 000 000

Коэффициент коллизий:

$$Kc = \frac{1}{1\,000\,000} \times 100 \approx 0.0001\%$$

Проведение обширного численного эксперимента позволило установить следующие результаты:

SHA-3: коэффициент коллизий составляет порядка 0.0001%.

SHA-256: коэффициент коллизий равен примерно 0.0002%.

SHA-1: наблюдается значительный рост показателя - около 0.05%.

В то же время, из полученного выше анализа следует, что алгоритмы SHA-3 и SHA-256 значительно более устойчивы к коллизиям, чем SHA-1. Иными словами, полученные выше исследования подтвердают, что более новые алгоритмы хеширования лучше используют свои основные функции в пределах коллизий. Целью последнего этапа нашего исследования является изучение способности конкретной хеш-функции быстро изменять созданные для ее данных даже при минимальных изменениях в данных. Поскольку такое свойство является одним из показателей захватывающей способности хеш-функции, оно известно как лавинообразный эффект, что означает, что даже самое незначительное изменение входных данных приведет к обрыву в будущем хеш.

Чувствительность к изменениям измерялась посредством следующего показателя:

$$Pr = \frac{Db}{Lh} \times 100\%$$

где:

Pr - процент различающихся битов,

Db - количество изменившихся битов,

Lh - полная длина хеш-значения.

Пример расчета для SHA-3:

Длина хеш-значения (*Lh*) = 256 бит

Количество различающихся битов (*Db*) = 128 бит

Степень изменения:

$$Pr = \frac{128}{256} \times 100 = 50\%$$

Экспериментальные данные показали, что в SHA-3 изменяются около 50% битов; в SHA-256 – отличаются примерно 48% битов, а в SHA-1 - около 35% битов.

Это наглядно показывает, что SHA-3 наиболее ярко выражает лавинообразный эффект, максимально реагируя на мельчайшие модификации данных значительным изменением битовой массы, - такое свойство придает SHA-3 дополнительную устойчивость и гарантирует защиту от потенциальных атак, основанных на частичных видоизменениях входных данных. Проведенные тесты наглядно продемонстрировали, что хеш-функция SHA-3 обладает высочайшей чувствительностью даже к самым незначительным корректировкам во входных данных. Это качество, называемое лавинообразным эффектом (avalanche effect), заключается в том, что малейшее изменение исходного набора данных - например, смена одного бита - вызывает радикальное преобразование хеш-значения. Способность алгоритма SHA-3 молниеносно откликаться на такие изменения обусловлена особенностями его внутреннего устройства, базирующегося на методе губчатой конструкции (sponge construction).

Этот метод позволяет генерировать хеши, исчерпывающе зависящие от каждого отдельного элемента входных данных, что делает невозможным предугадать или восстановить исходные данные, зная лишь конечное значение хеша. Тесты выявили, что при минимальных изменения исходных данных SHA-3 моментально отражает это перестановкой или сменой порядка половины или более битов в результирующем хеш-значении. Так, для длины хеша в 256 бит в случае изменения единственного бита во входных данных изменится половина или большая часть битов результата.

Этими свойствами SHA-3 становится незаменимым механизмом для применения там, где требуется безусловная гарантия целостности информации, он используется там, где требуется ещё более высокая безопасность, например, в системах с критически важной конфиденциальностью или долговечностью данных.

Заключение

Проведенное исследование однозначно подтвердило лидирующие позиции алгоритма SHA-3 по трем основным параметрам оценки: производительности, стойкости к коллизиям и чувствительности к незначительным изменениям данных. Также в проведенном эксперименте было продемонстрировано, что алгоритм SHA-3 имеет высокую эффективность при обработке данных большого размера, а среднее время вычисления хеш-значения в сравнении с другими алгоритмами заметно короче.

Стойкость к коллизиям является главной угрозой для безопасности данных, это свойство выражается в повторных хеш-значениях, полученных после обработки функциями хеширования. В свою очередь SHA-3 показал наибольшую устойчивость к таким угрозам, вероятность того, что после обработки алгоритмом, встретятся повторные значения незначительно мала и в реальном использовании практически не встречается, поэтому данный алгоритм является оптимальным в системах, где необходима повышенная безопасность и надежность.

Что касаемо чувствительности к незначительным изменениям данных, то и здесь данный алгоритм хеширования SHA-3 показывает превосходящие другие алгоритмы результаты, при изменении даже незначительных изменений, например, одного бита входных данных, будут следовать существенные изменения результата хеширования. Это свойство известно под названием «лавинообразный эффект» и является одним из самых значимых для угроз, связанных с подбором данных.

Таким образом, на основе достигнутых результатов в проведенном исследовании были составлены рекомендации по выбору хеш-функций с учетом особенностей и требований информационных систем: были предложены решения для серверных систем, которые в процессе использования подвергаются большим вычислительным нагрузкам, где наиболее оптимальным вариантов будет использование алгоритма SHA-3 для обеспечения высокой скорости работы в сочетании с повышенным уровнем безопасности и надежности от угроз коллизий.

В результате исследования мы получили комплексную систему оценки хеш-функций, которая позволяет выбрать наиболее подходящий вариант хеширования в зависимости от специфики информационной системы. Эти рекомендации помогут специалистам в области информационной безопасности принимать осознанные решения при проектировании систем защиты данных.

Библиография

1. Аблаев Ф. М., Зиятдинов М. Т. Универсальное семейство хеш-функций на основе квантовых процедур. Ученые записки Казанского университета. Серия физико-математические науки. 2020. № 3. С. 10-25.
2. Бахарев А. О. Новая модель квантового оракула для гибридной квантово-классической атаки на постквантовые криптосистемы, основанные на решетках. Дискретный анализ и исследование операций. 2024. Том 31, № 3. С. 22-51.
3. Бархатов Н. А., Ревунов С. Е. Гелиогеофизические приложения современных методов обработки цифровых данных : монография. Мининский университет. Москва : ФЛИНТА, 2017. 316 с. ISBN 978-5-9765-3011-9.
4. Заболотникова М. А., Картечина О. С., Пчелинцева Н. В. Сравнительный анализ алгоритмов хеш-функций. Материалы всероссийской научно-технической конференции молодых ученых. Нижний Новгород, 2020. С. 124-130.
5. Ким А. С., Симаков Е. Е., Симакова М. Н. Роль хэширования в работе «белого хакера». Юный ученый. 2023. № 8 (71). С. 54-60.
6. Поначугин А. В., Степанов В. Д., Базуева А. С. Перспективы использования искусственного интеллекта в информационно-телекоммуникационных сетях. Доклады Томского государственного университета систем управления и радиоэлектроники. 2025. Т. 28, № 1. С. 119-123.
7. Торгашов К. В., Шевцов Н. И., Зубарев Я. И., Голояд М. В., Сопин К. Ю., Самойленко Д. В. Методика криптографического контроля целостности данных на основе геометрических фракталов. Известия ТулГУ. Технические науки. 2022. № 5. С. 34-48.
8. Хорошев М. А., Бурова А. Д., Помелова Д. В., Старушенкова Е. Е. Методы модификации RSA-шифрования для обеспечения безопасности автоматизированных информационных систем SCADA. E-Scio. 2023. № 6 (81). С. 110-123.

Study of the Effectiveness of Hash Functions for Ensuring Data Integrity

Aleksandr V. Ponachugin

PhD in Economic Sciences, Associate Professor,
Head of the Department of Applied Informatics
and Information Technologies in Education,
Nizhny Novgorod State Pedagogical University named after K. Minin,
603005, 1, Ulyanova str., Nizhny Novgorod, Russian Federation;
e-mail: Ponachygin_AV@mininuniver.ru

Aleksandra S. Bazueva

Student,
Department of Applied Informatics
and Information Technologies in Education,
Nizhny Novgorod State Pedagogical University named after K. Minin,
603005, 1, Ulyanova str., Nizhny Novgorod, Russian Federation;
e-mail: bazueva_sasha@mail.ru

Nikita A. Batyaev

Student,
Department of Applied Informatics
and Information Technologies in Education,
Nizhny Novgorod State Pedagogical University named after K. Minin,
603005, 1, Ulyanova str., Nizhny Novgorod, Russian Federation;
e-mail: neket.1992@mail.ru

Abstract

Modern digital technologies impose high demands on data protection, a key element of which is integrity control. The article presents a comprehensive analysis of popular hash functions, revealing their strengths and weaknesses in the context of ensuring data security. A methodology is proposed that allows for a comparable analysis of performance, collision resistance, and sensitivity to data changes. The obtained results serve as a basis for developing practical recommendations on choosing a suitable hash function for various classes of information systems.

For citation

Ponachugin A.V., Bazueva A.S., Batyaev N.A. (2025) Issledovaniye effektivnosti khesh-funktsiy dlya obespecheniya tselostnosti dannykh [Study of the Effectiveness of Hash Functions for Ensuring Data Integrity]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (10A), pp. 150-160. DOI: 10.34670/AR.2025.16.59.013

Keywords

Hash functions, data integrity, cryptography, information security, collision resistance, information security, encryption algorithms, comparative analysis.

References

1. Ablaev, F. M., & Ziyatdinov, M. T. (2020). Universalnoe semeistvo khesh-funktsii na osnove kvantovykh protsedur [Universal family of hash functions based on quantum procedures]. *Uchenye zapiski Kazanskogo universiteta. Seriia fiziko-matematicheskie nauki,* (3), 10–25.
2. Bakharev, A. O. (2024). Novaia model kvantovogo orakula dlia gibridnoi kvantovo-klassicheskoi ataki na postkvantovye kriptosistemy, osnovannye na reshetkakh [A new model of a quantum oracle for a hybrid quantum-classical attack on lattice-based post-quantum cryptosystems]. *Diskretnyi analiz i issledovanie operatsii*, 31(3), 22–51.
3. Barkhatov, N. A., & Revunov, S. E. (2017). *Geliogeofizicheskie prilozheniia sovremennykh metodov obrabotki tsifrovykh dannykh: monografiia* [Heliogeophysical applications of modern digital data processing methods: A monograph]. Mininsky University, FLINTA. ISBN 978-5-9765-3011-9.
4. Kartechina, O. S., Pchelintseva, N. V., & Zabolotnikova, M. A. (2020). Sravnitelnyi analiz algoritmov khesh-funktsii [Comparative analysis of hash function algorithms]. In *Materialy vserossiiskoi nauchno-tekhnicheskoi konferentsii molodykh uchenykh* (pp. 124–130). Nizhny Novgorod.
5. Kim, A. S., Simakov, E. E., & Simakova, M. N. (2023). Rol kheshirovaniia v rabote "belogo khakera" [The role of hashing in the work of a "white hacker"]. *Yunyi uchenyi*, (8(71)), 54–60.
6. Ponachugin, A. V., Stepanov, V. D., & Bazueva, A. S. (2025). Perspektivy ispolzovaniia iskusstvennogo intellekta v informatsionno-telekommunikatsionnykh setiakh [Prospects for the use of artificial intelligence in information and telecommunication networks]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki*, 28(1), 119–123.
7. Torgashov, K. V., Shevtsov, N. I., Zubarev, Ya. I., Goloyad, M. V., Sopin, K. Yu., & Samoilenko, D. V. (2022). Metodika kriptograficheskogo kontrollia tselostnosti dannykh na osnove geometricheskikh fraktalov [Methodology for cryptographic data integrity control based on geometric fractals]. *Izvestiia TulGU. Tekhnicheskie nauki*, (5), 34–48.
8. Khoroshev, M. A., Burova, A. D., Pomelova, D. V., & Starushenkova, E. E. (2023). Metody modifikatsii RSA-shifrovaniia dlia obespecheniia bezopasnosti avtomatizirovannykh informatsionnykh sistem SCADA [Methods for modifying RSA encryption to ensure the security of automated SCADA information systems]. *E-Scio*, (6(81)), 110–123.