13. *Levina A.B.* Modelirovanie kriptosistem [Modeling of cryptosystems]. Saint Petersburg: Intermediya, 2016, 144 p.
14. *Osipyan V.O.* Razrabotka matematicheskoy modeli disimmetrichnoy bigrammnoy kriptosistemy na osnove parametricheskogo resheniya mnogostepennoy sistemy diofantovykh uravneniy [Development of a mathematical model of a dissymmetric bigram cryptosystem based on a parametric solution of a multi-degree system of Diophantine equations], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2020, N. 6. Available at: ivdon.ru/ru/magazine/archive/n6y2020/6534.
15. *Bolibrukh A.A.* Problemy Gil'berta (100 let spustya) [Hilbert's problems (100 years later)]. Moscow: MTsNMOB, 1999, 24 p.
16. *Bolelov E.A.* Kriptograficheskie metody zashchity informatsii [Cryptographic methods of information protection]. Moscow: MGTU GA, 2011, 80 p.
17. *Salomaa A.* Kriptografiya s otkrytym klyuchom [Public-key cryptography]. Moscow: Mir, 1995, 318 p.
18. *Smart N.* Kriptografiya [Cryptography]. Moscow: Tekhnosfera, 2005, 528 p.
19. *Matiyasevich Yu.V.* Desyataya problema Gil'berta [Hilbert's tenth problem]. Moscow: Nauka, 1993, 12 p.
20. *Osipyan V.O., Osipyan K.V.* Kriptografiya v zadachakh i uprazhneniyakh [Cryptography in tasks and exercises]. Moscow: Gelios ARV, 2004, 144 p.
21. *Katts D., Lindel Y.* Vvedenie v sovremennuyu kriptografiyu [Introduction to modern cryptography]. Chepmen end Kholl: CRC, 2014, 336 p.

Осипян Валерий Осипович – Кубанский государственный университет; e-mail: v.osippyan@gmail.com; г. Краснодар, Россия; кафедра анализа данных и искусственного интеллекта; д.ф.-м.н.; доцент.

Фурсина Елизавета Сергеевна – ООО "БСР"; e-mail: lizafursina@gmail.com; г. Краснодар, Россия; программист 1С.

Альгариб Эман Талиб – Кубанский государственный университет; e-mail: emanalghareeb38@gmail.com; г. Краснодар, Россия; кафедра анализа данных и искусственного интеллекта; аспирант.

Osipyan Valeriy Osipovich – Kuban State University; e-mail: v.osippyan@gmail.com; Krasnodar, Russia; the Department of Data Analysis and Artificial Intelligence; dr. of phys. and math. sc.; associate professor.

Fursina Elizaveta Sergeevna – Limited Liability Partnerships "BSR"; e-mail: lizafursina@gmail.com; Krasnodar, Russia; 1C programmer.

Alghareeb Eman Talib – Kuban State University; e-mail: emanalghareeb38@gmail.com; Krasnodar, Russia; the Department of Data Analysis and Artificial Intelligence; graduate student.

УДК 004.056.55 DOI 10.18522/2311-3103-2025-3-99-110

К.С. Романенко, Е.А. Ищукова, Н.Б. Ельчанинова

ШИФРОВАНИЕ ДАННЫХ В СЭД НА ОСНОВЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ

Рассмотрены вопросы хранения конфиденциальных и персональных данных в системах электронного документооборота. Рассмотрена возможность хранения конфиденциальных и персональных данных в системах электронного документооборота на основе блокчейн технологий. Одной из ключевых характеристик блокчейна является открытость данных. Все транзакции, внесенные в блокчейн, видны всем участникам сети. Это может стать серьезной проблемой при хранении чувствительных данных, таких как личная информация, банковские реквизиты или медицинская история. В связи с этим возникает неизбежный вопрос о безопасном хранении личных данных, поскольку блокчейн-платформа является открытой. Для скрытия информации применяются различные методы, включая гомоморфное шифрование, ZK-SNARK (доказательства с нулевым разглашением), специализированные аппаратные дополнения и другие способы. Ранее авторами был представлен протокол для хранения конфиденциальных данных в блокчейн системах с использованием гибридного шифрования. В работе уделено внимание применению алгоритмов симметричной криптографии в связке с криптографией на эллиптических кривых, поскольку она широко используется в современных блокчейн-платформах, таких как Bitcoin и Ethereum. Причиной выбора эллиптических кривых являются их высокая криптографическая стойкость при относительно малой длине ключа, эффективность вычислений и низкие требования к ресурсам, что особенно важно для децентрализованных сетей с ограниченными вычислительными возможностями узлов. В статье представлены резуль-

таты по моделированию процесса формирования зашифрованных конфиденциальных данных с использованием различных алгоритмов шифрования – ECC ElGamal, ECDH-AES, ECDH-Магма (в режимах CTR и CBC). Эксперименты показали, что наиболее эффективным решением является использование гибридного алгоритма ECDH-AES с поддержкой AES-NI, обеспечивающего высокую скорость обработки данных при сохранении высокого уровня безопасности. Проведённый анализ позволяет утверждать, что применение гибридного шифрования в блокчейн-системах обеспечивает баланс между необходимостью обеспечения конфиденциальности и сохранения ключевых преимуществ технологии – децентрализации, неизменности и прозрачности для авторизованных участников. Рассмотрены возможные форматы представления данных, проведено экспериментальное сравнение различных алгоритмов шифрования, которые могут быть использованы в системах электронного документооборота на основе блокчейн технологий.

Система электронного документооборота (СЭД); конфиденциальные данные; блокчейн; шифрование; формат данных; ключ; эллиптические кривые.

K.S. Romanenko, E.A. Ishchukova, N.B. Elchaninova

DATA ENCRYPTION IN EDMS BASED ON BLOCKCHAIN TECHNOLOGIES

The article discusses the issues of storing confidential and personal data in electronic document management systems. The possibility of storing confidential and personal data in electronic document management systems based on blockchain technologies is considered. One of the key characteristics of blockchain is the openness of data. All transactions entered into the blockchain are visible to all network participants. This can become a serious problem when storing sensitive data, such as personal information, bank details or medical history. storage of personal data, since the blockchain platform is open. Various methods are used to hide information, including homomorphic encryption, ZK-SNARKs (zero-knowledge proofs), specialized hardware add-ons, and other methods. Previously, the authors presented a protocol for storing confidential data in blockchain systems using hybrid encryption. The paper focuses on the use of symmetric cryptography algorithms in conjunction with elliptic curve cryptography, as it is widely used in modern blockchain platforms such as Bitcoin and Ethereum. The reason for choosing elliptic curves is their high cryptographic strength with a relatively short key length, computational efficiency, and low resource requirements, which is especially important for decentralized networks with limited node computing capabilities. The article presents the results of modeling the process of generating encrypted confidential data using various encryption algorithms: ECC ElGamal, ECDH-AES, ECDH-Magma (in CTR and CBC modes). Experiments have shown that the most effective solution is to use the hybrid ECDH-AES algorithm with AES-NI support, which provides high data processing speed while maintaining a high level of security. The analysis suggests that the use of hybrid encryption in blockchain systems strikes a balance between the need to ensure privacy and preserve the key benefits of the technology – decentralization, immutability, and transparency for authorized participants. Possible formats of data presentation are considered, an experimental comparison of various encryption algorithms that can be used in electronic document management systems based on blockchain technologies is carried out.

Electronic document management system (EDMS); confidential data; blockchain; encryption; data format; key; elliptical curves.

Введение. Хранение личной информации в системах блокчейна сопряжено с рядом технических проблем. Системы блокчейна, особенно публичные, сталкиваются с ограничениями масштабируемости. Хранение большого количества личных данных в реестре может привести к перегрузке сети и замедлению транзакций. Решение этой проблемы требует улучшения протоколов консенсуса и архитектурных изменений.

Блокчейн изначально спроектирован для обеспечения прозрачности и целостности данных. Это может привести к проблемам с сохранением конфиденциальности личной информации. Решения по обеспечению конфиденциальности, такие как zk -SNARKs [1] и кольцевые подписи [2], могут быть сложными в реализации и требовать вычислительных ресурсов.

Известно, что данные в блокчейне неизменяемы. Это означает, что, если персональные данные были размещены в блокчейне по ошибке или с нарушением законодательства, то они не могут быть удалены или изменены без ущерба для целостности всего блокчейна. Это создает серьезные проблемы с правом на забвение и другими законными требованиями.

Управление доступом к личным данным в блокчейне может оказаться сложной задачей. Должны быть обеспечены безопасность и контроль данных для предотвращения несанкционированного доступа. В зависимости от платформы блокчейна скорость обработки транзакций может быть ограничена. Хранение больших объемов персональных данных может увеличить время и затраты на обработку транзакций [3]. Блокчейны могут подвергаться атакам, а потеря приватных ключей или атака в сети могут привести к утечке персональных данных [4].

В статье [5] обсуждается проблема хранения персональных данных на платформе блокчейна и предлагается хранить данные в форме ключ-значение, но этот подход применяется только в публичной платформе Ethereum и не рассматриваются приватные платформы, которые могут применятся в СЭД. Авторы отмечают, что предлагаемый ими подход имеет ряд ограничений, связанных с ограничением сложной обработки данных в целях экономии средств и обеспечения информационной безопасности.

В работах [5, 6] обсуждаются проблемы хранения персональных данных на платформе Ethereum. Авторы предлагают управляемую пользователем и проверяемую структуру контроля доступа для Decentralized Online Social Network (DOSN) с использованием технологии блокчейн. В предложенном авторами подходе блокчейн используется для определения политики конфиденциальности. Владелец ресурса использует открытый ключ для определения гибких политик контроля доступа на основе ролей, в то время как закрытый ключ, связанный с учетной записью Ethereum субъекта, используется для расшифровки личных данных после проверки разрешения доступа в блокчейне.

В работе [7] рассматривается проблема хранения данных и предлагается хранить данные в базе данных, развернутой на клиенте. Используемые персональные данные хранятся в автономной базе данных и при необходимости извлекаются безопасным способом и передаются пользователю или веб-сервису, имеющему право доступа к этим файлам.

На сегодняшний день одной из острых проблем в области блокчейн-технологий является обеспечение конфиденциальности данных. Поскольку большинство существующих блокчейн-систем по своей природе предполагают прозрачность и доступность информации для всех участников сети, хранение конфиденциальных данных в открытом виде в таких системах является неприемлемым. Это ограничивает возможность использования блокчейна для реализации надежных и безопасных систем электронного документооборота, где защита персональных и коммерческих данных играет ключевую роль.

В этой связи возникает необходимость разработки механизмов, которые бы позволили эффективно шифровать данные перед их записью в блокчейн, обеспечивая тем самым их конфиденциальность. При этом важно сохранить основные преимущества блокчейн-технологий – децентрализацию, неизменность и прозрачность операций для авторизованных участников. Такой механизм может стать основой для создания защищённых систем электронного документооборота, сочетающих высокий уровень безопасности с функциональностью распределённого реестра.

Ранее авторами был представлен протокол хранения персональных данных на основе использования гибридного шифрования [8]. Хранение и обмен такими данными предполагается осуществлять в зашифрованном виде. Известно, что в основе любой блокчейн-платформы лежит асимметричная криптография. Как правило, это криптография, основанная на использовании эллиптических кривых [9]. Так, например, платформы Bitcoin и Ethereum используют алгоритм ECDSA, основанный на кривой secp256k1. При этом сами блокчейн-системы никаким образом не регулируют процесс пользовательского обмена ключами или другими данными для совершения транзакций. Для оптимизации работы ранее разработанного протокола и выбора правильных параметров шифрования требуется провести эксперимент по эффективности применения различных подходов шифрования.

Авторы видят два возможных пути применения шифрования для разработанного протокола. Первый вариант заключается в использовании асимметричной криптографии на эллиптической кривой (например, алгоритма Эль-Гамаля ECC ElGamal) для шифрова-

ния небольшой порции информации, которую требуется сохранить в блокчейне. Известно, что асимметричные шифры работают медленнее симметричных и не предназначены для шифрования больших объемов данных. Но в случае, если сохраняемый в блокчейне объем данных небольшой и занимает всего 1-2 блока, такой вариант облегчает работу протокола, так как не требуется производить дополнительную выработку ключа между разными абонентами блокчейн-системы. Вторым вариантом сохранения данных в блокчейне является использование симметричного шифрования в связке с протоколом Elliptic Curve Diffie-Hellman (ECDH), т.к. данный протокол может использовать кривую secp256k1, уже используемую в блокчейн-системах. В этом случае абоненты блокчейн-сети могут использовать свои открытые и закрытые ключи для выработки общего секрета, которые впоследствии будет использоваться как ключ симметричного шифрования. Для того, чтобы сделать правильный выбор, необходимо определить потенциальный объем хранения конфиденциальных данных, а также экспериментально оценить скорость обработки этих данных с использованием различных алгоритмов.

Объем персональных данных в популярных системах электронного документооборота. Объем персональных данных, которые хранятся в системах электронного документооборота (СЭД) для одного человека, может существенно различаться в зависимости от ряда факторов. К ним относятся тип информации, которая сохраняется, структура данных, используемая в системе, а также внутренние требования и политики организации, которая управляет этими данными. В среднем, объем персональных данных на одного человека может составлять от нескольких килобайт до нескольких мегабайт.

Для более глубокого понимания того, как формируется объем персональных данных, важно детально разобрать его основные составляющие. Прежде всего, ключевым фактором является тип хранимой информации. Это могут быть как простые данные, например, фамилия, имя, отчество, дата рождения, номера телефонов или адреса электронной почты, так и более сложные материалы, такие как отсканированные копии документов, фотографии, электронные подписи, история переписки, письма и другие файлы.

Персональные данные могут включать различные типы информации, каждый из которых занимает определенный объем. Идентификационные данные, такие как ФИО, дата рождения, паспортные данные, ИНН, СНИЛС и другие, обычно хранятся в текстовых полях (VARCHAR или STRING) и занимают от 100 до 500 байт. Контактная информация, включая адрес, телефон и email, также хранится в текстовых полях и требует от 100 до 300 байт. Рабочая информация, такая как должность, отдел и история работы, занимает больше места – от 1 до 5 КБ в текстовом формате.

Биометрические данные, например фотографии или сканы документов, могут занимать от 100 КБ до 5 МБ в зависимости от качества изображения. Электронные документы, такие как трудовой договор, приказы или сканы паспорта, сохраняются в форматах PDF или других форматах и могут занимать от 100 КБ до 10 МБ, в зависимости от количества страниц и разрешения сканирования. История действий, включая логи изменений, подписей и согласований, обычно хранится в текстовом или JSON-формате и занимает от 1 до 10 КБ.

Примерный расчет объема данных для одного человека может варьироваться в зависимости от типа и количества хранимой информации. Если в системе сохраняются только основные данные, такие как ФИО, контактная информация и должность, то объем составит от 1 до 10 КБ. Это минимальный объем, который требуется для хранения базовых сведений.

Если к этим данным добавляются сканированные копии документов, например, паспорта, СНИЛС или трудового договора, то объем увеличивается до 1–10 МБ. Это средний уровень, который учитывает хранение как текстовой информации, так и файлов.

В случае, когда система хранит подробные данные, включая историю изменений, множество сканов документов и биометрические данные (например, фотографии или отпечатки пальцев), объем может достигать 10–50 МБ и более. Это максимальный объем, который требуется для хранения полного набора персональных данных с учетом всех возможных файлов и метаданных.

Системы электронного документооборота (СЭД) используют различные подходы к хранению данных, что влияет на объем информации и структуру хранения. Рассмотрим подробнее, как организовано хранение данных в популярных СЭД, включая размеры полей и особенности каждой системы.

1С:Документооборот использует реляционные базы данных, такие как PostgreSQL или Microsoft SQL Server, для хранения информации. Данные в системе делятся на текстовые поля и прикрепленные файлы. Основные поля, такие как ФИО, дата рождения, контактная информация, занимают от 100 до 500 байт каждое. Например, поле для ФИО (VARCHAR) обычно имеет ограничение в 255 символов, что соответствует 255 байтам. Дополнительные данные, такие как должность или история работы, могут занимать от 1 до 5 КБ в зависимости от объема текста. Сканы документов, фотографии и другие файлы хранятся отдельно. Размер таких файлов варьируется от 100 КБ до 10 МБ в зависимости от качества сканирования и количества страниц. Например, скан паспорта в высоком разрешении может занимать 2–3 МБ. Для одного пользователя с минимальным набором данных (текстовые поля и несколько файлов) объем может составлять 1–10 МБ. Если добавляются дополнительные документы и история изменений, объем может увеличиться до 50 МБ и более [10].

Система «ДЕЛО» от компании ЭОС (Электронные Офисные Системы) поддерживает хранение больших объемов данных, включая сканы документов и метаданные. Для оптимизации хранения система использует комбинацию реляционной базы данных и файлового хранилища. Основные поля, такие как ФИО, контактная информация и должность, занимают от 100 до 500 байт. Поля для хранения описаний документов или комментариев могут занимать до 5 КБ. Сканы документов хранятся в файловом хранилище, что позволяет экономить место в основной базе данных. Размер файлов зависит от качества сканирования: низкое разрешение занимает 100–500 КБ, а высокое разрешение – 1–5 МБ. Например, скан трудового договора в высоком разрешении может занимать 3–4 МБ. Для одного пользователя с минимальным набором данных объем составляет 1–10 МБ. Если добавляются сканы документов и история изменений, объем может достигать 10–50 МБ [11].

Диалог от компании СКБ Контур ориентирован на хранение электронных документов и их метаданных. Система активно используется для обмена юридически значимыми документами, что требует надежного хранения и быстрого доступа к информации. Основные поля, такие как ФИО, ИНН, контактная информация, занимают от 100 до 500 байт. Поля для хранения метаданных (например, дата создания документа или подпись) могут занимать до 1 КБ. Электронные документы, такие как счета-фактуры, договоры или акты, хранятся в формате PDF. Размер файлов зависит от количества страниц и разрешения: документ на 1–2 страницы занимает 100–500 КБ, а документ на 10 и более страниц – 1–5 МБ. Для одного пользователя с минимальным набором данных объем составляет 1–5 МБ. Если добавляются дополнительные документы и история изменений, объем может увеличиться до 10–20 МБ [12].

Docsvision – это гибкая система, которая поддерживает хранение данных как в реляционных базах данных, так и в файловых хранилищах. Это позволяет адаптировать систему под нужды конкретной организации. Основные поля, такие как ФИО, контактная информация и должность, занимают от 100 до 500 байт. Поля для хранения описаний документов или истории изменений могут занимать до 10 КБ. Сканы документов и другие файлы хранятся в файловом хранилище. Размер файлов зависит от их типа: сканы документов занимают 100 КБ – 5 МБ, а электронные документы (PDF) – 100 КБ – 10 МБ. Для одного пользователя с минимальным набором данных объем составляет 1–10 МБ. Если добавляются сканы документов, биометрические данные и история изменений, объем может достигать 10–50 МБ и более [13].

Формат персональных данных для использования в блокчейн. Анализ существующих систем электронного документооборота показывает, что в среднем хранение основной информации о пользователе занимает от 100 до 500 байт. В связи с тем, что мы рассматриваем хранение данных не просто в базе данных, а именно в блокчейн системе, то в рамках данного исследования мы не будем останавливаться на вопросах хранения

«тяжелых» документов, таких как сканы в виде изображений или пдф-файлов, также не будем рассматривать хранение каких-либо других форматов файлов. Остановимся только на хранении основной информации о пользователе.

На первом шаге рассмотрим какие данные мы можем собирать в блоки с учетом предполагаемого к использованию алгоритма шифрования. Особенно это важно для первого исследуемого алгоритма ECC ElGamal, для которого в рамках протокола мы хотим ограничить шифрование одним блоком данных. Для шифров AES и Магма такое распределение не является критичным, так как используемые режимы обеспечивают шифрование любых объемов данных. В отведенную размерность 512 бит или 64 байта мы можем упаковать, например, ФИО пользователя. Согласно данным переписи населения в России самая длинная фамилия содержит 20 букв, самое длинное мужское имя содержит 15 букв (Абдурахмангаджи), женское – 12 букв (Вильгельмина), а самое длинное отчество содержит 19 букв (Абдурахмангаджиевич или Абдурахмангаджиевна). Отведем под эти поля символы с запасом так, как показано на рис. 1.

Также в один блок размерности 512 бит или 64 байта можно упаковать такую информацию как СНИЛС, ИНН, паспортные данные, дату рождения и телефон. Останется еще 4 байта для хранения служебной информации. Например, для связи данной записи с другими записями пользователя.

Таким образом мы определили минимальный объем персональных данных. Который в зашифрованном виде может быть помещен в блокчейн-систему.

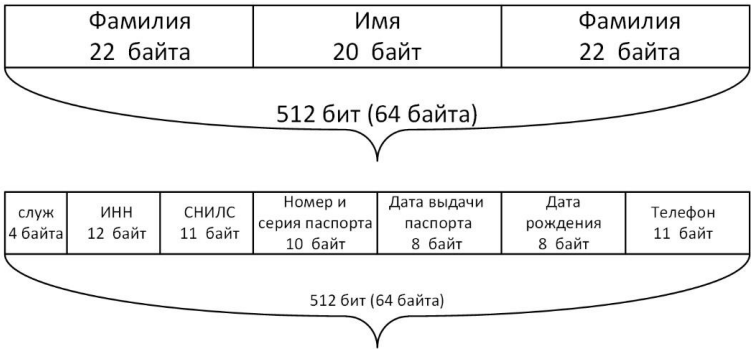

Рис. 1. Формат представления блока данных для алгоритма ECC ElGamal

Шифрование данных в блокчейн. Эллиптические кривые и асимметричная криптография на их основе играют важную роль в современных блокчейн-системах. Они обеспечивают безопасность и целостность данных, а также используются для создания цифровых подписей, аутентификации и защиты транзакций.

Эллиптическая кривая – это математический объект, который задается уравнением специального вида. В криптографии используются кривые над конечными полями, например, где значения координат точек кривой ограничены простым числом. Основное свойство эллиптических кривых, которое делает их полезными для криптографии, – это сложность задачи дискретного логарифмирования. Нахождение числа, которое связывает две точки на кривой, является вычислительно сложной задачей, что обеспечивает высокий уровень безопасности.

В блокчейн-системах, таких как Bitcoin и Ethereum, для подписи транзакций используется алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm). Этот алгоритм позволяет подтвердить, что транзакция была отправлена владельцем приватного ключа, не раскрывая сам ключ. Приватный ключ – это случайное число, выбранное из определенного диапазона, а публичный ключ – это точка на эллиптической кривой, которая вычисляется с использованием приватного ключа и базовой точки кривой. Подпись создается с использованием приватного ключа и хэша транзакции, а затем проверяется с помощью публичного ключа.

Важно отметить, что так как алгоритм ECDSA является основой публичных блокчейн систем, таких как Bitcoin и Ethereum, то все пользователи системы уже имеют пару назначенных им ключей вида открытый – закрытый ключ. Размерность ключа определяется параметрами используемой эллиптической кривой. В данном случае используется кривая вида secp256k1 и открытый ключ содержит две координаты эллиптической кривой общим объемом 512 бит. Ассиметричная криптография не предназначена для шифрования больших объемов данных. Однако мы можем попробовать рассмотреть вариант использования ассиметричных ключей алгоритма ECDSA для шифрования одного блока данных, если хранимые данные умещаются в 512 бит. Для этих целей подойдет использование алгоритма Эль-Гамаля на эллиптических кривых (ECC ElGamal). Алгоритм ECC ElGamal – это асимметричный алгоритм шифрования, адаптированный для работы с эллиптическими кривыми. В отличие от гибридных схем, он шифрует данные напрямую, используя математические операции на кривой. Для шифрования сообщение преобразуется в точку на кривой, что требует дополнительных вычислительных ресурсов.

Во всех остальных случаях, когда объем данных, предназначенных для хранения, превышает размерность ключа алгоритма ECDSA, целесообразнее использовать симметричное шифрование. При этом у пользователей должна быть возможность сформировать общий секретный ключ. Например, с использованием протокола Диффи-Хеллмана, адаптированного под использование на эллиптических кривых (ECDH, Elliptic Curve Diffie-Hellman).

Рассмотрим в качестве шифрования два основных стандарта: стандарт AES (Advanced Encryption Standard) и стандарт ГОСТ Р 34.12-2015 (Магма).

Стандарт AES представляет собой симметричный блочный шифр, основанный на алгоритме Rijndael. Будем рассматривать вариант стандарта, в котором блок данных и секретный ключ шифрования имеют длину 128 бит. Будем рассматривать применение стандарта AES в режиме CBC (Cipher Block Chaining).

Шифр Магма представляет собой симметричный блочный шифр с длиной ключа 256 бит и объемом одного шифруемого блока 64 бита. Для шифра ГОСТ Р 34.12-2015 (Магма) есть два режима, предназначенных для шифрования файлов: режим CTR (Counter) и режим CBC. Режим CTR (Counter) превращает блочный шифр в потоковый, позволяя выполнять параллельную обработку данных. Режим CBC требует, чтобы каждый блок данных зависел от предыдущего, что исключает параллельную обработку. Рассмотрим в эксперименте оба режима.

Таким образом, в настоящей работе будет проведен эксперимент для определения эффективности использования того или иного метода шифрования с использованием четырех разных подходов: ECC ElGamal, ECDH-AES, ECDH-Магма- CTR и ECDH-Магма- CBC.

Результаты экспериментов. При проведении сравнительного анализа алгоритмов шифрования для систем электронного документооборота (СЭД) на основе блокчейна важно учитывать не только криптографическую стойкость, но и скорость обработки данных различных размеров. Рассмотрим четыре алгоритма: Эль-Гамаль на эллиптических кривых ECC ElGamal, ECDH-AES, ECDH-Магма-CTR и ECDH-Магма-CBC. Три последних из них сочетают в себе асимметричные и симметричные методы, но с разными подходами к шифрованию, что влияет на производительность.

Экспериментальное сравнение алгоритмов проводилось с использованием библиотеки OpenSSL и с использованием компилятора g++ для языка программирования C++ в операционной системе Ubuntu 24.04.2 LTS (WSL). Процессор QuadCore Intel Core i5-4460, 3233 MHz (34 x 95). Оперативная память 16 ГБ (DDR3-1600 DDR3 SDRAM).

OpenSSL – это одна из наиболее известных и широко используемых библиотек с открытым исходным кодом, предназначенная для реализации криптографических функций, протоколов безопасности и работы с SSL/TLS. Она предоставляет разработчикам инструменты для защиты данных, аутентификации, шифрования и создания защищенных сетевых соединений. Библиотека написана на языках C и ассемблере, что обеспечивает высокую производительность и кроссплатформенность. OpenSSL активно применяется в веб-серверах (например, Apache, Nginx), блокчейн-системах, мобильных приложениях и IoT-устройствах [14-16].

OpenSSL включает реализацию симметричных шифров (AES, DES), асимметричных алгоритмов (RSA, ECDSA, EdDSA), хэш-функций (SHA-256, SHA-3, MD5) и алгоритмов обмена ключами (Diffie-Hellman, ECDH). Это позволяет выбирать оптимальные методы для конкретных задач, будь то шифрование данных, цифровые подписи или аутентификация [17, 18].

Распространенной практикой оценки скорости шифрования одного блока данных является многократное повторение действий по шифрованию (например, шифрование 1000 блоков) и потом получение усредненного значения. Так как разные шифры шифруют разные объемы данных, то итоговое сравнение будем делать не по скорости обработки одного блока, а по скорости обработки 64 байт информации. Для алгоритма ECC ElGamal такое преобразование займет всего один блок данных, для алгоритма ECDH-AES – 4 блока данных, а для алгоритмов ECDH-Магма-CTR и ECDH-Магма-CBC – по 8 блоков данных соответственно. Для алгоритмов, использующих протокол ECDH, выработка ключа производится однократно. После чего весь объем данных шифруется на одном и том же ключе.

В результате проведенного эксперимента, были получены временные замеры обработки информации, которые сведены в табл. 1

Таблица 1

Скорость шифрования данных

Алгоритм / Время обработки, сек	ECC+ Эль-Гамаля	ECDH-AES	ECDH-AES (AES-NI)	ECDH-Магма (CTR)	ECDH-Магма (CBC)
1024 байт	0,0370294 секунд	0,00002684 секунд	0.000002651 секунд	0,001 секунд	0,001 секунд
10240 байт	0,340882 секунд	0,000277854 секунд	0,000021231 секунд	0,001 секунд	0,001 секунд
Среднее время для обработки 1 блока	0,00116406 секунд	0,000001631 секунд	0,000000715 секунд	0,001 секунд	0,001 секунд
Среднее время для 64 байт	0,00225913 секунд	0,000003103 секунд	0,000000919 секунд	0,001 секунд	0,001 секунд

При шифровании небольших объемов данных (до 1 КБ) ECC ElGamal демонстрирует приемлемую скорость, так как операции на кривой выполняются быстро. Однако преобразование данных в точки может добавлять задержки. Для файлов размером от 1 МБ и выше производительность резко падает. Асимметричное шифрование требует значительных вычислений для каждого блока данных, что делает алгоритм непрактичным для больших объемов данных, как и предполагалось изначально. Таким образом, как и ожидалось, экспериментально подтверждено, что применение алгоритма ECC ElGamal для шифрования одного блока данных может быть использовано в блокчейн-системах без использования дополнительных надстроек криптографии.

Настройка ECDH добавляет задержку (генерация ключей и обмен), но сам AES крайне эффективен. Для документов до 1 КБ общее время шифрования сопоставимо с ECC ElGamal. AES оптимизирован для быстрой обработки крупных объемов, особенно при использовании аппаратного ускорения (например, инструкций AES-NI). Для файлов от 1 МБ ECDH-AES значительно превосходит ECC ElGamal.

Магма в режиме CTR работает быстро даже на небольших файлах, но уступает AES из-за менее оптимизированных реализаций. Для документов до 1 МБ разница между CBC и CTR не критична, но CBC всё же медленнее из-за последовательной природы.

В результате проведенного анализа можно сделать вывод, что гибридный алгоритм ECDH-AES оказался быстрее. Современные процессоры Intel (и AMD) имеют встроенные инструкции для ускорения AES, известные как AES-NI (Advanced Encryption Standard New Instructions) [19–22]. Эти инструкции позволяют выполнять операции шифрования и расшифрования AES на аппаратном уровне, что значительно ускоряет процесс по сравнению с программной реализацией.

OpenSSL активно использует аппаратные возможности процессоров, включая AES-NI. Если процессор поддерживает AES-NI, OpenSSL автоматически задействует эти инструкции для выполнения операций шифрования и дешифрования.

Заключение. В данной работе был проведен анализ возможного объема хранимой информации в системах электронного документооборота, а также проведен сравнительный анализ алгоритмов шифрования, которые могут использоваться для шифрования данных в системах электронного документооборота на основе блокчейн технологий. Следующим шагом станет детальная проработка протоколов для хранения персональных данных в системе электронного документооборота на основе блокчейн-технологий. Эта работа будет учитывать выбранную блокчейн-платформу, специфику решаемой задачи, а также предполагает использование оптимального алгоритма шифрования – в данном случае ECDH-AES-NI с поддержкой аппаратного ускорения, реализованного в библиотеке OpenSSL.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Кондырев Дмитрий*. Метод обеспечения конфиденциальности данных на основе ЗК-СНАРК // Прикладная дискретная математика. Приложение. – 2021. – 14. – С. 132-134.
2. *Бендер А., Кац Дж., Морселли Р.* Кольцевые сигнатуры: более строгие опреде-ления и конструкции без случайных оракулов / Халеви С., Рабин Т. (ред.) // Теория криптографии. TCC 2006. Конспекты лекций по информатике. Т. 3876. – Springer, Берлин, Гейдельберг, 2006. – https://doi.org/10.1007/11681878_4.
3. *Зискинд Г., Натан О. и Пентланд А.* Децентрализация конфиденциальности: ис-пользование блокчейна для защиты персональных данных // Семинары IEEE по безопасности и конфиденциальности, 2015 г. Сан-Хосе, Калифорния, США, 2015 г. – С. 180-184. Номер документа: 10.1109/ SPW.2015.27.
4. *Гуггенбергер Тобиас, Шлатт Винсент, Шмид Джонатан, Нильс Урбах.* Структурированный обзор атак на системы блокчейн. – 2021. – URL: https://www.researchgate.net/publication/352960457_A_Structured_Overview_of_Attacks_on_Blockchain_Systems (дата обращения: 22.03.2025).
5. *Алдиафла И. и др.* Проектирование и реализация безопасного хранилища данных на основе смарт-контракта Ethereum // Applied Sciences. – 2023. – Vol. 13, No. 9.
6. *Рахман М., Баярди Ф., Гуиди Б., Риччи Л.* Защита персональных данных с помощью смарт-контрактов // Матер. IEEE Int. Conf. Blockchain. – 2019. – URL: https://ieeexplore.ieee.org/document/8971241 (дата обращения: 22.03.2025).
7. *Киран А., Дхараникота С. и Басава А*. Контроль доступа к данным на основе блокчейна с использованием смарт-контрактов // TENCON, конференция IEEE Region 10 (TENCON), 2019–2019 гг., Кочи, Индия, 2019 г. – С. 2335-2339. – DOI: 10.1109/TENCON.2019.8929451.
8. *Романенко К.С., Ищукова Е.А.* Алгоритм хранения приватных данных в блокчейн системах // Современные методы, средства и технологии защиты информации: Сб. трудов XV Международной научно-практической конференции имени Олега Борисовича Макаревича (Таганрог, 11–15 сентября 2024 г.). – Ростов-на-Дону; Таганрог: Изд-во ЮФУ, 2024.
9. *Ищукова Е.А., Панасенко С.П., Романенко К.С., Салманов В.Д.* Криптографические основы блокчейн-технологий. – М.: ООО "ДМК Пресс. Электронные книги", 2022. – 301 с. – ISBN 978-5-9706-0865-4.
10. 1С:Документооборот 8. – URL: https://v8.1c.ru/doc8/ (дата обращения: 22.03.2025).
11. СЭД «Дело». – URL: https://eos.ru/eos_products/eos_delo/sed-delo/ (дата обращения: 22.03.2025).
12. Контур Диадок. – URL: https://www.diadoc.ru/ (дата обращения: 22.03.2025).
13. Платформа Docsvision. – URL: https://docsvision.com/ (дата обращения: 22.03.2025).
14. *Ситников Д.С., Гайрбеков С.М.К.* Анализ возможного использования библиотеки криптографических процедур OpenSSL // Информационные технологии в науке, бизнесе и образовании. Проблемы обеспечения цифрового суверенитета государства: Матер. XIII Международной на-

учно-практической конференции студентов, аспирантов и молодых ученых, Москва, 26 ноября 2021 г. / под общ. ред. А.М. Прохорова, А.В. Царегородцева. – М.: Московский государственный лингвистический университет, 2022. – С. 85-91.
15. *Белявский Д.* Российская криптография в свободном ПО // Пятнадцатая конференция разработчиков свободных программ: Тезисы докладов. Калуга, 28–30 сентября 2018 г. / отв. ред. В.Л. Черный. – Калуга: ООО "МАКС Пресс", 2018. – С. 38-39.
16. *Никифоров А.Н., Матвеева Н.Н.* Исследование методов защиты информации с помощью криптографии // Современные информационные технологии, инновации и молодежь - «СИТИМ-2024»: Матер. Всероссийской студенческой научно-практической конференции с международным участием, Якутск, 22-23 марта 2024 г. – Ульяновск: ИП Кеньшенская Виктория Валерьевна (Изд-во "Зебра"), 2024. – С. 151-155.
17. OpenSSL. – URL: https://openssl-library.org/ (дата обращения: 22.03.2025).
18. *Гафуров И.Р.* Методы оптимизации программной реализации блочного шифра "Магма" // Ученые записки УлГУ. Серия: Математика и информационные технологии. – 2022. – № 1. – С. 8-16.
19. *Tezcan C.* Optimization of Advanced Encryption Standard on Graphics Processing Units // IEEE Access. – 2021. – Vol. 9. – P. 67315-67326. – DOI: 10.1109/ACCESS.2021.3077551.
20. *Valamehr J., Tiwari M., Sherwood T. [et al.].* Hardware assistance for trustworthy systems through 3-D integration // Proceedings - Annual Computer Security Applications Conference, ACSAC: 26th Annual Computer Security Applications Conference, ACSAC 2010, December 6–10, 2010 / sponsors: Applied Computer Security Associates (ACSA). – Austin, TX: [s.n.], 2010. – P. 199-210. – DOI: 10.1145/1920261.1920292.
21. *Лебедев Р.К.* Применение расширений процессорной архитектуры x86 для затруднения анализа программного кода // МНСК-2021: Матер. 59-й Международной научной студенческой конференции. Новосибирск, 12–23 апреля 2021 г. Новосиб. нац. исслед. гос. ун-т. – Новосибирск: Изд-во НГУ, 2021. – С. 12.
22. *Пристанскоов Е.И., Кудрявцев О.А., Андреев Д.Е. [и др.].* Анализ аппаратной поддержки криптографии при построении информационной безопасности вуза // Управление образованием: теория и практика. – 2022. – № 6 (52). – С. 126-132. – DOI: 10.25726/h2048-6130-4735-p.

REFERENCES

1. *Kondyrev Dmitriy.* Metod obespecheniya konfidentsial'nosti dannykh na osnove ZK-SNARK [A method for ensuring data confidentiality based on the ZK-SNARK], *Prikladnaya diskretnaya matematika. Prilozhenie* [Applied discrete mathematics. Appendix], 2021, 14, pp. 132-134.
2. *Bender A., Kats Dzh., Morselli R.* Kol'tsevye signatury: bolee strogie opredeleniya i konstruktsii bez sluchaynykh orakulov [Ring signatures: stricter definitions and constructions without random oracles], Khalevi S., Rabin T. (ed.), *Teoriya kriptografii. TCC 2006. Konspekty lektsiy po informatike* [Theory of cryptography. TCC 2006. Lecture Notes on Computer Science]. Vol. 3876. Springer, Berlin, Geydel'berg, 2006. Available at: https://doi.org/10.1007/11681878_4.
3. *Ziskind G., Natan O. and Pentland A.* Detsentralizatsiya konfidentsial'nosti: ispol'zovanie blokcheyna dlya zashchity personal'nykh dannykh [Decentralizing Privacy: Using Blockchain to Protect Personal Data], *Seminary IEEE po bezopasnosti i konfidentsial'nosti, 2015 g. San-Khose, Kaliforniya, SShA, 2015 g.* [IEEE Seminars on Security and Privacy, 2015, San Jose, California, USA, 2015], pp. 180-184. Document number: 10.1109/ SPW.2015.27.
4. *Guggenberger Tobias, Shlatt Vinsent, Shmid Dzhonatan, Nil's Urbakh*. Strukturirovannyy obzor atak na sistemy blokcheyn [Structured overview of attacks on blockchain systems], 2021. Available at: https://www.researchgate.net/publication/352960457_A_Structured_Overview_of_Attacks_on_Blockchain_Systems (accessed 22 March 2025).
5. *Aldiafla I., et al.* Proektirovanie i realizatsiya bezopasnogo khranilishcha dannykh na osnove smart-kontrakta Ethereum [Designing and implementing a secure data warehouse based on the Ethereum smart contract], *Applied Sciences,* 2023, Vol. 13, No. 9.
6. *Rakhman M., Bayardi F., Guidi B., Richchi L.* Zashchita personal'nykh dannykh s pomoshch'yu smart-kontraktov [Protection of personal data using smart contracts], *Mater. IEEE Int. Conf. Blockchain* [Proceedings of the IEEE Int. Conf. Blockchain], 2019. Available at: https://ieeexplore.ieee.org/document/8971241 (accessed 22 March 2025).
7. *Kiran A., Dkharanikota S. and Basava A*. Kontrol' dostupa k dannym na osnove blokcheyna s ispol'zovaniem smart-kontraktov [Blockchain-based data access control using smart contracts], *TENCON, konferentsiya IEEE Region 10 (TENCON), 2019–2019 gg., Kochi, Indiya, 2019 g*. [TENCON, IEEE Region 10 Conference (TENCON), 2019-2019, Kochi, India, 2019], pp. 2335-2339. DOI: 10.1109/TENKON.2019.8929451.

8. *Romanenko K.S., Ishchukova E.A.* Algoritm khraneniya privatnykh dannykh v blokcheyn sistemakh [Algorithm for storing private data in blockchain systems], *Sovremennye metody, sredstva i tekhnologii zashchity informatsii: Sb. trudov XV Mezhdunarodnoy nauchno-prakticheskoy konferentsii imeni Olega Borisovicha Makarevicha (Taganrog, 11–15 sentyabrya 2024 g.)* [Proceedings of the XV International Scientific and Practical Conference Named After Oleg Borisovich Makarevich (Taganrog, September 11–15, 2024)]. Rostov-on-Don; Taganrog: Izd-vo YuFU, 2024.
9. *Ishchukova E.A., Panasenko S.P., Romanenko K.S., Salmanov V.D.* Kriptograficheskie osnovy blokcheyn-tekhnologiy [Cryptographic foundations of blockchain technologies]. Moscow: OOO "DMK Press. Elektronnye knigi", 2022, 301 p. ISBN 978-5-9706-0865-4.
10. 1S:Dokumentooborot 8 [1C:Document management 8]. Available at: https://v8.1c.ru/doc8/ (accessed 22 March 2025).
11. SED «Delo» [SED "Delo"]. Available at: https://eos.ru/eos_products/eos_delo/sed-delo/ (accessed 22 March 2025).
12. Kontur Diadok [Contour of Diadems]. Available at: https://www.diadoc.ru/ (accessed 22 March 2025).
13. Platforma Docsvision [Docsvision platform]. Available at: https://docsvision.com/ (accessed 22 March 2025).
14. *Sitnikov D.S., Gayrbekov S.M.K.* Analiz vozmozhnogo ispol'zovaniya biblioteki kriptograficheskikh protsedur OpenSSL [Analysis of the possible use of the OpenSSL cryptographic procedure library], *Informatsionnye tekhnologii v nauke, biznese i obrazovanii. Problemy obespecheniya tsifrovogo suvereniteta gosudarstva: Mater. XIII Mezhdunarodnoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh, Moskva, 26 noyabrya 2021 g.* [Information technologies in science, business and education. Problems of ensuring the digital sovereignty of the state: Proceedings of the XIII International Scientific and Practical Conference of Students, Postgraduates and Young Scientists, Moscow, November 26, 2021], under the general ed. A.M. Prokhorova, A.V. Tsaregorodtseva. Moscow: Moskovskiy gosudarstvennyy lingvisticheskiy universitet, 2022, pp. 85-91.
15. *Belyavskiy D.* Rossiyskaya kriptografiya v svobodnom PO [Russian cryptography in free software], *Pyatnadtsataya konferentsiya razrabotchikov svobodnykh programm: Tezisy dokladov. Kaluga, 28–30 sentyabrya 2018 g*. [The Fifteenth Conference of Free Software Developers : abstracts. Kaluga, September 28-30, 2018], ed. by V.L. Chernyy. Kaluga: OOO "MAKS Press", 2018. – S. 38-39.
16. *Nikiforov A.N., Matveeva N.N.* Issledovanie metodov zashchity informatsii s pomoshch'yu kriptografii [Investigation of information security methods using cryptography], *Sovremennye informatsionnye tekhnologii, innovatsii i molodezh' - «SITIM-2024»: Mater. Vserossiyskoy studencheskoy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem, Yakutsk, 22-23 marta 2024 g.* [Modern information technologies, innovations and youth - SITIM-2024 : proceedings of the All-Russian Student Scientific and Practical Conference with international participation, Yakutsk, March 22-23, 2024]. Ul'yanovsk: IP Ken'shenskaya Viktoriya Valer'evna (Izd-vo "Zebra"), 2024, pp. 151-155.
17. OpenSSL. Available at: https://openssl-library.org/ (accessed 22 March 2025).
18. *Gafurov I.R.* Metody optimizatsii programmnoy realizatsii blochnogo shifra "Magma" [Methods of optimizing the software implementation of the block cipher "Magma"], *Uchenye zapiski UlGU. Seriya: Matematika i informatsionnye tekhnologii* [Scientific notes of the USU. Series: Mathematics and Information Technology], 2022, No. 1, pp. 8-16.
19. *Tezcan C.* Optimization of Advanced Encryption Standard on Graphics Processing Units, *IEEE Access,* 2021, Vol. 9, pp. 67315-67326. DOI: 10.1109/ACCESS.2021.3077551.
20. *Valamehr J., Tiwari M., Sherwood T. [et al.].* Hardware assistance for trustworthy systems through 3-D integration, *Proceedings - Annual Computer Security Applications Conference, ACSAC: 26th Annual Computer Security Applications Conference, ACSAC 2010, December 6–10, 2010 / sponsors: Applied Computer Security Associates (ACSA)*. Austin, TX: [s.n.], 2010, pp. 199-210. DOI: 10.1145/1920261.1920292.
21. *Lebedev R.K.* Primenenie rasshireniy protsessornoy arkhitektury x86 dlya zatrudneniya analiza programmnogo koda [The use of extensions of the x86 processor architecture to complicate the analysis of program code], *MNSK-2021: Mater. 59-y Mezhdunarodnoy nauchnoy studencheskoy konferentsii. Novosibirsk, 12–23 aprelya 2021 g.* [MNSK-2021: Proceedings of the 59th International Scientific Student Conference. Novosibirsk, April 12-23, 2021]. *Novosib. nats. issled. gos. un-t*. Novosibirsk: Izd-vo NGU, 2021, pp. 12.
22. *Pristanskov E.I., Kudryavtsev O.A., Andreev D.E. [et al.].* Analiz apparatnoy podderzhki kriptografii pri postroenii informatsionnoy bezopasnosti vuza [Analysis of hardware support for cryptography in building information security of a university], *Upravlenie obrazovaniem: teoriya i praktika* [Education Management: Theory and Practice], 2022, No. 6 (52), pp. 126-132. DOI: 10.25726/h2048-6130-4735-p.

Романенко Кирилл Сергеевич – Южный федеральный университет; e-mail: kirromanenko@sfedu.ru; г. Таганрог, Россия; тел.: +79885190125; кафедра безопасности информационных технологий им. Макаревича О.Б.; ассистент.

Ищукова Евгения Александровна – Южный федеральный университет; e-mail: uaishukova@sfedu.ru; г. Таганрог, Россия; тел.: +79281435898; кафедра безопасности информационных технологий им. Макаревича О.Б.; к.т.н.; доцент.

Ельчанинова Наталья Борисовна – Южный федеральный университет; e-mail: inf_2012@mail.ru; г. Таганрог, Россия; тел.: +79185000495; кафедра безопасности информационных технологий им. Макаревича О.Б.; к.т.н.; доцент.

Romanenko Kirill Sergeevich – Southern Federal University; e-mail: kirromanenko@sfedu.ru; phone: +79885190125; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; assistant.

Ishchukova Evgeniya Aleksandrovna – Southern Federal University; e-mail: uaishukova@sfedu.ru; phone: +79281435898; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; cand. of eng. sc.; associate professor.

Elchaninova Nataliya Borisovna – Southern Federal University; e-mail: inf_2012@mail.ru; phone: +79185000495; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; cand. of eng. sc.; associate professor.

УДК 004.056.55 DOI 10.18522/2311-3103-2025-3-110-118

В.С. Стародубцев, Л.К. Бабенко, Н.Б. Ельчанинова

ОЦЕНКА ВРЕМЕНИ ВЫПОЛНЕНИЯ ПОИСКА СОСТАВЛЯЮЩИХ КЛЮЧА В АТАКЕ С ИЗВЕСТНЫМ ОТКРЫТЫМ ТЕКСТОМ НА КРИПТОСИСТЕМУ ДОМИНГО-ФЕРРЕРА

Представлено краткое описание полностью гомоморфной криптографической системы Доминго-Феррера, приводится характеристика этапов атаки с известным открытым текстом на данную криптосистему. Анализируется этап поиска составляющих ключа рассматриваемой атаки, для которого описываются существующие методы реализации, среди которых определяется метод, обладающий минимальной вычислительной сложностью. Обоснование вычислительной сложности и временных затрат рассматриваемого метода реализации этапа поиска составляющих ключа формируется на основе теоретических расчётов, а также экспериментальных исследований. Целью исследования является оценка сложности реализации этапа поиска составляющих ключа в атаке с известным открытым текстом на полностью гомоморфную криптографическую систему Доминго-Феррера с помощью метода Гаусса, разработанного для решения систем линейных алгебраических уравнений по модулю простого числа. Основным результатом настоящей работы является оценка вычислительной сложности этапа поиска составляющих ключа в атаке с известным открытым текстом на криптографическую систему Доминго-Феррера, реализованного с использованием метода Гаусса. Оценка сложности выражена в количестве базовых математических операций и подтверждена рядом экспериментальных исследований, что позволяет сделать обоснованные выводы о вычислительной сложности рассматриваемого метода. Проведенное исследование представляет собой значимый вклад в развитие полностью гомоморфной криптосистемы Доминго-Феррера, основанной на задаче факторизации целых чисел. Оно обладает практической значимостью, так как позволяет оценить критичность атаки с известным открытым текстом на данную криптосистему. Полученные результаты могут служить основой для исследователей и криптографов при разработке рекомендаций по выбору параметров криптосистемы Доминго-Феррера для обеспечения необходимого уровня безопасности в различных приложениях.

Информационная безопасность; гомоморфное шифрование; гомоморфная схема шифрования; полностью гомоморфное шифрование; криптосистема Доминго-Феррера; криптоанализ.