Раздел II. Алгоритмы обработки информации

УДК 004.056.55 DOI 10.18522/2311-3103-2021-5-120-134

Л.К. Бабенко, А.С. Шумилин, Д.М. Алексеев

АЛГОРИТМ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ОБЛАЧНОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Целью работы является разработка и реализация архитектуры облачной системы хранения, систематизации и обработки результатов обследований (на примере ЭЭГ) и алгоритма обеспечения защиты конфиденциальных данных на основе полностью гомоморфной криптосистемы. Объектом исследования являются технологии хранения, передачи, обработки и защиты конфиденциальной информации в распределенных медицинских информационных системах. Разработана архитектура облачной платформы распределенного хранения, обработки, систематизации и защиты конфиденциальных данных (результатов медицинских обследований), позволяющая взаимодействовать с различными медицинскими информационными системами и аппаратными средствами диагностики с целью формирования больших данных. Разработан алгоритм обеспечения безопасности медицинских данных, хранимых в облачной платформе в электронном виде, регистрируемых при проведении обследований пациентов с целью расчета среднего значения для каждого из ритмов мозговой активности (по результатам серии обследований за длительный период времени) с использованием алгоритма полностью гомоморфного шифрования. На основе результатов тестирования (анализ времени выполнения таких операций, как: шифрование, дешифрование, сложение, умножение, отношение сигнал шум зашифрованного текста к открытому тексту) из двух потенциальных претендентов на использование в качестве алгоритмов полностью гомоморфного шифрования (схемы BFV и CKKS) выбран оптимальный алгоритм. В результате показано, что схема полностью гомоморфного шифрования CKKS наиболее эффективна, особенно в условиях критичности требований к высокому уровню безопасности конфиденциальных данных, чем обусловлен выбор данной схемы для реализации предложенного в настоящей работе алгоритма.

Защита информации; медицинская информационная система; конфиденциальность; облачные вычисления; информационная безопасность; обработка данных; систематизация данных; большие данные; шифрование.

L.K. Babenko, A.S. Shumilin, D.M. Alekseev

ALGORITHM OF PROTECTING CONFIDENTIAL DATA IN THE CLOUD MEDICAL INFORMATION SYSTEM

The aim of the work is the development and implementation of the architecture of a cloud storage system, systematization and processing of survey results (for example, EEG) and an algorithm for ensuring the protection of confidential data based on a completely homomorphic cryptosystem. The object of the research is the technologies of storage, transmission, processing and protection of confidential information in distributed medical information systems. The architecture of a cloud platform for distributed storage, processing, systematization and protection of confidential data (results of medical examinations) has been developed, which makes it possible to interact with various medical information systems and diagnostic hardware in order to generate big data. An algorithm has been developed to ensure the safety of medical data stored in a cloud platform in

electronic form, recorded during patient examinations in order to calculate the average value for each of the brain activity rhythms (based on the results of a series of examinations over a long period of time) using a fully homomorphic encryption algorithm. Based on the test results (analysis of the execution time of such operations as: encryption, decryption, addition, multiplication, signal-to-noise ratio of ciphertext to plaintext), the optimal algorithm. According to the results of the work, it is shown that the fully homomorphic encryption scheme CKKS is the most effective, especially in the context of the criticality of the requirements for a high level of security of confidential data, which determines the choice of this scheme for the implementation of the algorithm proposed in this work.

Information security; medical information system; privacy; cloud computing; information security; data processing; data systematization; big data, encryption.

Введение. Век всеобщей информатизации и развития информационных технологий оказал значительное влияние на все сферы человеческой жизнедеятельности. Ежедневно каждый из нас использует компьютерные технологии для достижения определенных целей: общение в социальных сетях, поиск нужной информации в сети Интернет, чтение книг, сложные математические расчеты, просмотр видеофильмов, создание программного обеспечения, телемедицина. Ситуацию с актуальностью и быстрыми темпами развития информационных технологий обострила, в том числе, пандемия.

В связи с этим, в настоящее время процессы создания, накопления и обработки информации в сфере здравоохранения становятся все более актуальными, что обусловлено масштабной информатизацией отрасли по всему миру.

В век всеобщей информатизации и активного развития информационных технологий медицинские учреждения в ходе выполнения диагностических исследований обрабатывают и систематизируют значительные объемы данных для последующей реабилитации и лечения пациентов [1].

Эффективность оказываемой медицинской помощи прямо пропорциональна оперативности и удобству использования данной информации специалистами медицинских организаций. Наличие задач, связанных с хранением, систематизацией и обработкой увеличивающихся объемов данных обуславливает актуальность разработки и интеграции в медицинские учреждения медицинских информационных систем (МИС). Возможность оперирования данными в электронном виде обеспечивает оперативность получения врачом необходимой информации о пациенте, что увеличивает скорость принятия решения о постановке диагноза и методах лечения [2, 4].

Анализ проблемы. Медицинские организации в силу законодательства являются операторами персональных данных своих пациентов. Они принимают непосредственное участие в сборе, систематизации, накоплении, хранении, уточнении, обновлении, изменении, распространении и уничтожении такой информации.

Одной из проблем при проектировании медицинских информационных систем является необходимость интеграции механизмов защиты конфиденциальной информации [3].

К категории конфиденциальной информации относят: фамилия, имя, отчество пациента, месяц, дата и место рождения, серия и номер паспорта, адрес регистрации и фактического проживания, идентификационный номер налогоплательщика (ИНН), страховое свидетельство государственного пенсионного страхования (СНИЛС), семейное, социальное положение, образование, профессия, должность, специальность, серия и номер страхового медицинского полиса и его действительность и др.

В связи с тем, что данная категория информации представляет собой, как правило, текстовую форму и ее содержание статично (информация не меняется в режиме реального времени в ходе проведения обследований), ее защита обеспечи-

вается стандартными методами и средствами шифрования. К категории персональных медицинских данных, требующих нетрадиционных подходов к их защите, относят динамически изменяющиеся показатели результатов медицинских обследований пациентов (например, показателей электроэнцефалограммы).

Например, каждый пациент регистрирует в процессе проведения ЭЭГ-обследований (сеансов) показатели биоритмов головного мозга (альфа, бета и тета ритмы). Изменение волновой активности (по каждому из видов ритмов) представляет собой изменяющийся ряд числовых данных (обновление один раз за одну секунду). Для правильной постановки диагноза и выбора тактики лечения пациентов важна динамика изменения показателей и их средние значения за длительный период времени (например, суточное ежедневное мониторирование мозговой активности в течение одного месяца реабилитации пациента).

Как правило, показатели мозговой активности (альфа, бета и тета ритмы) определяют и регистрируют носимые беспроводные устройства для мониторинга состояния здоровья. Зарегистрированные результаты медицинских исследований могут передаваться в медицинские организации (учреждения здравоохранения) в автоматическом режиме по сети или посредством беспроводных каналов связи. Доступ со стороны потенциального злоумышленника к передаваемым данным с целью их изменения может оказаться критичным для пациента. Это обусловлено не только вероятной дискредитацией данных с точки зрения доступа к ним со стороны третьих лиц (например, с целью оповещения страховых компаний), но и потенциальной опасностью изменения результатов медицинских обследований. Например, в случае, если доктор не уведомлен о том, что статистика показателей и их результаты искажены, возникает риск установить некорректный диагноз, что впоследствии может привести к тому, что устройства персонализированной медицины подадут медикаменты в неправильной дозировке. Это, в свою очередь, может нанести непоправимый вред состоянию здоровья и даже поставить под угрозу саму жизнь пациента [5, 6].

В связи с тем, что требованиями законодательства установлена необходимость защиты персональных данных, ключевой задачей при реализации облачной системы хранения, систематизации и обработки медицинских данных является обеспечение безопасности хранимой информации.

Научная новизна работы заключается в разработке медицинской информационной системы на базе облачных технологий для сбора, систематизации и обработки результатов обследований и разработке эффективного алгоритма защиты конфиденциальных данных с использованием систем полностью гомоморфного шифрования.

Данный подход отличается от известных использованием механизмов защиты медицинских данных, позволяющих выполнять облачные вычисления над зашифрованными результатами обследований (без предварительной расшифровки) в недоверенной среде, а также возможностью интеграции с большинством существующих программно-аппаратных комплексов и средств диагностики. Ключевой особенностью медицинской информационной системы является подсистема механизмов защиты, которая представляет собой алгоритм обеспечения защиты конфиденциальных данных на основе полностью гомоморфной криптосистемы, предложенный, реализованный и исследованный автором.

Новизна разработанного алгоритма заключается в возможности его использования для различных типов данных (результатов различных видов медицинских обследований), одновременном снижении времени работы в медицинской информационной системе (за счет отсутствия необходимости расшифровки данных для подсчета средних значений параметров за длительный период времени) и повышении эффективности систем обеспечения защиты информации.

Постановка задачи. Целью работы является разработка и реализация архитектуры облачной системы хранения, систематизации и обработки результатов обследований (на примере ЭЭГ) и алгоритма обеспечения защиты конфиденциальных данных на основе полностью гомоморфной криптосистемы.

Достижение поставленной цели предполагает необходимость решения следующих **задач**:

- ♦ изучение существующих архитектурных решений при проектировании информационных процессов в области здравоохранения и медицины;
- ♦ анализ ключевых особенностей технологий хранения и систематизации данных медицинских обследований, аккумулирующихся в цифровых системах электронной регистратуры;
- ♦ выполнить проектирование архитектуры распределенной облачной платформы хранения, систематизации и обработки конфиденциальных данных медицинских обследований, позволяющую регистрировать и получать данные с использованием различных аппаратных средств диагностики;
- ♦ разработать алгоритм обеспечения безопасности медицинских данных, хранимых в облачной платформе в электронном виде, регистрируемых при проведении обследований пациентов с целью расчета среднего значения для каждого из ритмов мозговой активности (по результатам серии обследований, например, в ходе курса реабилитации методом биологической обратной связи);
- ♦ выбрать эффективный алгоритм полностью гомоморфного шифрования для использования в рамках разработанного алгоритма;
- ♦ создать интегрируемую облачную платформу распределенного хранения, анализа и систематизации медицинских данных и систему обеспечения безопасности с использованием разработанного алгоритма защиты;
- ♦ провести анализ эффективности предложенного алгоритма защиты конфиденциальной медицинской информации в условиях интеграции в разработанную облачную платформу.

Анализ современного состояния исследований. В работе [11] Котяшичев И.А. и Бырылова Е.А. рассматривают возможность использования облачных технологий с целью повышения эффективности внедрения информационных систем в различные отрасли медицины. Среди наиболее распространённых способов обеспечения безопасности данных авторы выделяют шифрование. Однако в ходе работы отмечается неотъемлемая проблема симметричных систем шифрования – проблема распределения ключей, что осложняет процесс работы с такими системами. Проблема заключается в том, что хранение ключей на облачном сервере нецелесообразно, поскольку пользователь, имеющий доступ к облачным серверам, получает доступ к ключу, а следовательно, и к расшифрованным данным [7, 8].

Керейтова М.Р. и Малыш В.Н. в работе [12] отмечают проблему обеспечения информационной безопасности конфиденциальных данных пациентов как одну из наиболее важных при создании и проектировании медицинских информационных систем. Вопрос защиты информации рассматривается на примере распределенной информационной системы Департамента охраны здоровья населения Кемеровской области, охватывающей все лечебно-профилактические учреждения (ЛПУ) Кемеровской области. Авторы предлагают комплексный подход к решению проблемы: ввести контроль за рабочими станциями на предмет необычно высокой активности, в полной мере использовать антивирусную защиту, следить за всеми обновлениями для имеющихся операционных систем, использовать многоуровневую аутентификацию пользователей, предполагающую использование USB-ключей, смарт-карт, паролей, файловых ключей. Однако предлагаемый авторами подход не учитывает механизмов обеспечения защиты данных в аспекте предотвращения их

утечки и/или несанкционированного доступа при передаче и хранении информации в системах с архитектурой клиент-сервер. Таким образом, в рамках данной работы рассмотрены способы и средства, обеспечивающие защиту на уровне доступа к рабочим станциям пользователям системы [9, 10].

Бойченко И.В. в работе [13] отмечает важность проблемы реализации прав граждан в области защиты персональных данных пациентов. Автор рассматривает возможность использования медицинских информационно-аналитических центров в структуре здравоохранения, акцентируя внимание лишь на правовом и юридическом аспектах проблемы. Предварительный анализ, проведенный автором, позволяет сделать вывод о большом потенциале использования облачных технологий в решении задач современного здравоохранения. Однако для их повсеместного внедрения требуется грамотное техническое решение, направленное на разработку методов обеспечения безопасности передаваемой информации и конфиденциальности персональных данных пациентов.

В работе [14] Rohan Jathanna отмечает уязвимость облачных систем к атакам со стороны злоумышленников (DDoS-атаки, атаки с целью проникновения на сервер, несанкционированный доступ к базам данных). Для предотвращения потери доступа к конфиденциальным данным автор предлагает использовать возможности средств резервного копирования. Противодействие несанкционированному доступу достигается путём использования алгоритмов шифрования. Предлагаемые автором подходы имеют существенные недостатки. Система резервного копирования требует большого количества дополнительных вычислительных ресурсов и ресурсов памяти, а также обеспечения нового объекта защиты (ресурса с резервной копией). Эффективность используемых алгоритмов шифрования снижается в связи с наличием проблемы распределения ключей: необходимо предусмотреть возможность передачи ключа от клиента на сервер по защищенному каналу связи. Последствием компрометации ключа шифрования является потеря доступа к конфиденциальным данным [17].

В работе [15] Кривошеева Д.А. выделяет основные недостатки использование ассиметричных систем шифрования в медицинских облачных платформах: большие затраты вычислительных ресурсов, а также времени, которое требуется для реализации вычислительных процессов. Автор предлагает альтернативный подход к созданию симметричного ключа шифрования, основанный на использовании физиологического сигнала пациента в качестве «физиологической» подписи. Существенным недостатком предлагаемого метода является тот факт, что физиологические сигналы (электрокардиограмма, фотоплетизмограмма, электроэнцефалограмма и др.) могут изменяться в течение жизни человека. Соответственно, ключ шифрования, сформированный ранее, спустя определённое время может стать недействительным и, как следствие, доступ к персональным данным станет невозможен [16, 18].

Не менее важной проблемой предлагаемого метода видится возможность доступа к данным только со стороны их обладателя (пациента, который предоставил физиологический сигнал для формирования ключа шифрования). Таким образом, возможность получения доступа к результатам обследования другими лицами (например, лечащим доктором, родственниками пациента, аналитиком системы здравоохранения и др.) затрудняется или вовсе исключается.

Подводя итоги, стоит отметить, что в работах, доступных в открытом доступе в научной литературе и электронных библиотеках, имеются различные недостатки, основными из которых являются: проблема распределения ключей, высокие требования к вычислительным ресурсам, ресурсам времени и памяти. Предлагаемый в рамках работы подход направлен на исключение указанных выше недостат-

ков за счет применения систем полностью гомоморфного шифрования, ключевой особенностью которых является возможность реализации обработки зашифрованной информации без её расшифровки [20].

Гомоморфное шифрование: определение, виды и библиотеки. Гомоморфное шифрование – форма шифрования, позволяющая производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполненных с открытым текстом. Например, один человек мог бы сложить два зашифрованных числа, не зная расшифрованных чисел, а затем другой человек мог бы расшифровать зашифрованную сумму – получить расшифрованную сумму, не имея расшифрованных чисел. Гомоморфное шифрование позволяет предоставлять различные услуги, не предоставляя открытые пользовательские данные для каждой услуги.

Гомоморфное шифрование является формой шифрования, позволяющей осуществить определённую алгебраическую операцию над открытым текстом посредством выполнения алгебраической операции над зашифрованным текстом.

Пусть k – ключ для шифрования, t – подлежащий шифрованию открытый текст (сообщение), $\mathrm{E}(\mathrm{k}, \mathrm{t})$ – выполняющая шифрование функция.

Функция E называется гомоморфной относительно операции * (сложения или умножения) над открытыми текстами (сообщениями) t1 и t2, если существует эффективный алгоритм M (требующий полиномиального числа ресурсов и работающий за полиномиальное время), который, получив на вход любую пару шифрованных текстов вида $\mathrm{E}(\mathrm{k}, t_1)$ и $\mathrm{E}(\mathrm{k}, t_2)$, выдаёт зашифрованный текст (шифротекст) $\mathrm{c} = \mathrm{M}(\mathrm{E}(\mathrm{k}, t_1), \mathrm{E}(\mathrm{k}, t_2))$ такой, что при расшифровании c будет получен открытый текст t1 * t2.

Система шифрования является гомоморфной относительно операции умножения (обладает мультипликативными гомоморфными свойствами), если выполняется равенство: $D\big(\mathrm{E}(t_1) \times \mathrm{E}(t_2)\big) = t_1 \times t_2$.

Система шифрования является гомоморфной относительно операции сложения (обладает аддитивными гомоморфными свойствами), если выполняется равенство: $D\big(\mathrm{E}(t_1) + \mathrm{E}(t_2)\big) = t_1 + t_2$.

Система шифрования является гомоморфной относительно операций умножения и сложения, то есть, полностью гомоморфной (обладает и мультипликативными, и аддитивными гомоморфными свойствами), если выполняются равенства:

$$D\big(\mathrm{E}(t_1) \times \mathrm{E}(t_2)\big) = t_1 \times t_2;$$
$$D\big(\mathrm{E}(t_1) + \mathrm{E}(t_2)\big) = t_1 + t_2.$$

В настоящее время доступно множество программных реализаций систем полностью гомоморфного шифрования [20]. Некоторые из них носят экспериментальный характер и разработаны в академических целях, другие нацелены на использование широким кругом разработчиков. В рамках настоящей работы рассмотрены популярные библиотеки, предоставляющие возможности полностью гомоморфного шифрования и обладающие открытым исходным кодом:

♦ HELib – одна из наиболее популярных библиотек, разработана Халеви и Шупом, предоставляет возможность тонкой настройки режимов работы схем гомоморфного шифрования.

♦ Библиотека гомоморфного шифрования SEAL разработана исследователями Microsoft Research, поддерживает операции сложения и умножения над целыми и вещественными числами.

♦ Библиотека криптографических механизмов PALISADE, основанных на целочисленных решетках, в том числе систем полностью гомоморфного шифрования.

♦ Библиотека разработана авторами одноименной системы полностью гомоморфного шифрования TFHE. В отличие от HELib и SEAL, не поддерживает работу с вещественными числами.

♦ Библиотека HEAAN разработана авторами системы CKKS, предоставляет возможность выполнения гомоморфных приближенных вычислений над вещественными числами.

♦ Λ ○ λ – Haskell-библиотека общего назначения, предоставляющая интерфейс для многих математических операций, используемых в криптографических механизмах, основанных на целочисленных решетках. В том числе в библиотеке реализован модифицированный вариант системы BGV.

♦ lattigo – реализация на языке Go криптографических механизмов, основанных на целочисленных решетках. Включает набор функций для программной реализации систем BFV и CKKS.

Разработка платформы медицинской информационной системы. Для решения задачи хранения, систематизации и обработки медицинских данных авторами разработана облачная платформа, общая схема которой представлена на рис. 1.

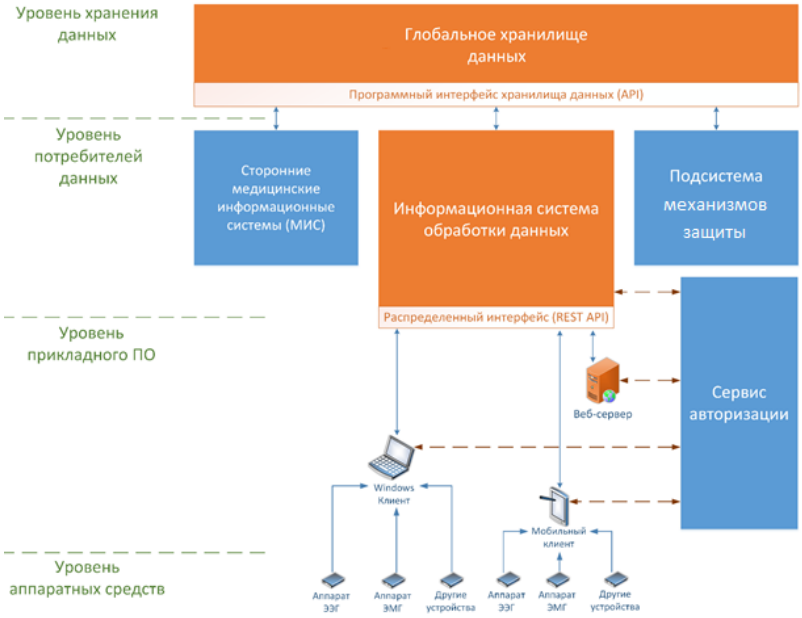

Рис. 1. Общая схема облачной платформы хранения, систематизации и обработки медицинских данных

Разработанная облачная система включает 4 основных уровня:

Уровень хранения данных: глобальное хранилище данных, которое включает в себя базу данных для хранения исходных данных обследований и отчетов, а также антропометрическая, диагностическая, демографическая информация о пациентах. Хранилище содержит полный объем информации для исследований и обучения машинных алгоритмов, но идентификация пациента возможна только по защищенному идентификатору.

Уровень потребителей данных – слой, включающий системы, которые принимают и обрабатывают данные из Глобального хранилища или передают в него новые данные. Этот уровень связан с уровнем хранения данных через стандартизированный программный интерфейс (Storage API). Потребителями данных могут

быть: сторонние медицинские информационные системы; исследовательские системы; информационная система обработки данных – содержит базу персональных данных пациентов, соответствует требованиям безопасности и защиты персональных данных и медицинских данных (Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»; Федеральный закон от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; Health Insurance Portability and Accountability Act of 1996, HIPAA) [2]. Данный модуль обеспечивает взаимодействие с конечными клиентскими приложениями по средствам распределенного интерфейса (REST API).

Уровень прикладного ПО – уровень, содержащий программные средства конечных клиентов, где формируются и/или отображаются медицинские данные (обследования в виде сигналов, отчетные и персональные данные пациента): Windows клиенты – программное обеспечение для ОС семейства Windows; Вебсервер – предоставляет пользователю возможность доступа через web browser, в соответствии с назначенными этому пользователю ролями; Мобильный клиент – предоставляет доступ в информационную систему обработки данных используя мобильные устройства (Android, iOS).

Уровень аппаратных средств – физические устройства для проведения обследований. В общем случае могут быть различных видов: электроэнцефалографы, кардиографы, системы биологической обратной связи, носимые фитнес трекеры и т.д.

Экспериментальная часть. Алгоритм обеспечения защиты конфиденциальных данных на основе полностью гомоморфной криптосистемы. В результате исследований разработан следующий алгоритм обеспечения защиты конфиденциальных данных (результатов медицинских обследований на примере ЭЭГ) на основе полностью гомоморфной криптосистемы:

Предусловия алгоритма:

1. Пользователями медицинской информационной системы являются доктора и пациенты. Каждый пользователь системы зарегистрирован в ней с использованием уникального идентификатора (логин) и пароля.

2. При посещении лечебного учреждения доктор сообщает пациентам о необходимости проведения серии мониторинговых обследований (например, суточное ежедневное мониторирование мозговой активности в течение одного месяца реабилитации пациента). Для правильной постановки диагноза и выбора тактики лечения пациентов важна динамика изменения показателей и их средние значения за длительный период времени. При этом доктор предоставляет свой уникальный идентификатор пациенту, необходимый для его первичной регистрации в медицинской информационной системе.

3. При регистрации в системе пациент указывает собственные персональные данные и уникальный идентификатор доктора, назначившего серию обследований.

4. В дальнейшем в личном кабинете пользователя (на мобильном телефоне или в программе на ПК) отображается перечень докторов, работающих с данным пациентом. В личном кабинете доступна функция добавления новых докторов (для потенциального масштабирования системы и добавления новых специалистов аналогичного или другого профиля).

5. При попытке привязки уникального идентификатора доктора к личному кабинету пациента доктор получает уведомление с запросом на подтверждение данного действия. После подтверждения запроса у доктора появляются права доступа на просмотр результатов медицинских обследований конкретного пациента.

6. Сервер S, предназначенный для хранения и систематизации всех данных, содержит базу данных с правами доступа для каждого зарегистрированного доктора системы к результатам пациентов.

Шаги алгоритма:

Шаг 1. На стороне каждого доктора медицинской информационной системы для каждого из его пациентов генерируется и хранится пара ключей (открытый и секретный ключ). Генерация ключей осуществляется сразу после подтверждения запроса на привязку доктора к личному кабинету определенного пациента.

Шаг 2. После подтверждения привязки доктора к личному кабинету пациента открытый ключ доктора для конкретного пациента отправляется данному пациенту.

Шаг 3. Каждый пациент регистрирует в процессе проведения обследований (сеансов) показатели биоритмов головного мозга (альфа, бета и тета ритмы). Изменение волновой активности (по каждому из видов ритмов) представляет собой изменяющийся ряд числовых данных (обновление один раз за одну секунду).

Шаг 4. Данные (показатели ритмов мозговой активности), зарегистрированные с использованием устройства (например, беспроводное ЭЭГ-устройство) на стороне пациента (мобильное приложение), шифруются на открытом ключе, полученным от доктора. Данные в зашифрованном виде передаются и хранятся на сервере.

Шаг 5. Данные, отправленные на сервер, хранятся на нем без последующего расшифрования. Данные о значениях ритмов мозговой активности статистически накапливается в течение определенного длительного периода времени (курса реабилитации). Параллельно осуществляется учет значения количества проведенных исследований для каждого пациента. Применение алгоритма гомоморфного шифрования позволяет проводить операцию сложения этих данных без предварительной расшифровки с целью расчета среднего значения для каждого из ритмов (по результатам серии обследований, например, в ходе курса реабилитации методом биологической обратной связи). Расчет среднего значения осуществляется в результате умножения суммарного значения каждого ритма (за серию обследований) на мультипликативное обратное для значения количества проведенных исследований.

Шаг 6. При необходимости получения расчетных данных каждого ритма (альфа, бета и тета) доктор отправляет на сервер запрос в виде идентификатора пациента на получение данных.

Шаг 7. После получения запроса на сервере проверяется наличие права доступа доктора на получение данных определенного пациента. Проверка осуществляется по идентификатору доктора.

Шаг 8. В случае наличия прав доступа сервер отправляет зашифрованные данные (средние значения ритмов мозговой активности) доктору, выполнившему запрос.

Шаг 9. Доктор расшифровывает полученные данные своим секретным ключом (сгенерированным для конкретного пациента).

Последовательность запросов и ответов (со стороны сервера, пациентов и докторов), необходимых для реализации алгоритма, схематично представлена на рис. 2.

В рамках работы реализован алгоритм обеспечения защиты конфиденциальных данных на основе полностью гомоморфной криптосистемы для данных мозговой активности. В качестве потенциальных претендентов на использование в качестве алгоритмов полностью гомоморфного шифрования выбраны схемы BFV и CKKS. Окончательный выбор схемы выполнен на основе результатов тестирования свойств заявленных кандидатов, полученных Бабенко М.Г., Голимблевской Е.И. и Ширяевым Е.М. и опубликованных в работе [1].

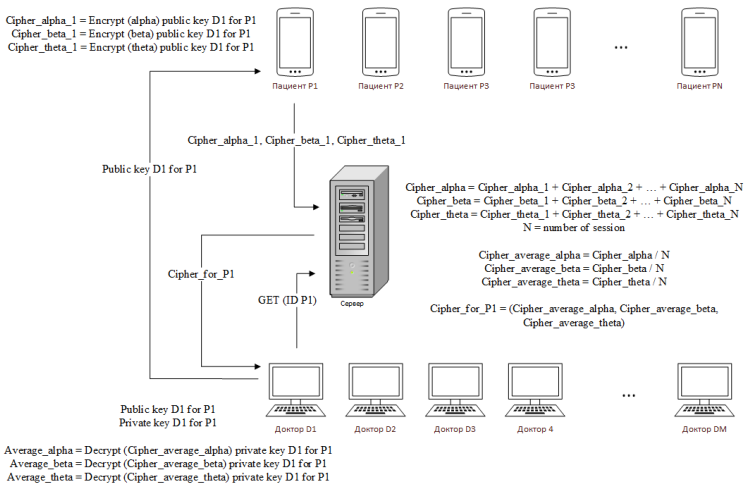

Рис. 2. Алгоритм обеспечения защиты конфиденциальных данных (результатов медицинских обследований на примере ЭЭГ) на основе полностью гомоморфной криптосистемы

Авторами работы [1] проведен обширных анализ криптографических свойств существующих гомоморфных шифров (CKKS, BFV) на основе обучения с ошибками, выполнено сравнение их технических характеристик: криптостойкости и избыточности данных, скорости кодирования и декодирования данных, скорости выполнения арифметических операций сложения и умножения данных, скорости выполнения операции KeySwitching.

Важно отметить высокий уровень теоретической и практической значимости результатов, полученных Бабенко М.Г., Голимблевской Е.И. и Ширяевым Е.М. Полученные авторами выводы могут служить основой для исследований в различных областях и направлениях информационной безопасности: анализ безопасности криптографических протоколов, криптографические средства защиты информации, защита информации и облачных вычислений. Научные результаты авторов позволяют разрабатывать эффективные алгоритмы обеспечения информационной безопасности, обеспечивать эффективную комплексную защиту информации, циркулирующей в распределенных медицинских системах, построенных на основе современных криптографических средств, что играет важную роль в обеспечении информационной безопасности в целом.

Для исследования схем гомоморфного шифрования авторами работы [1] выбрана криптографическая библиотека на основе решеток LattiGo, разработанная на языке GoLang. Эта библиотека содержит набор функций, реализующих гомоморфные схемы шифрования BFV и CKKS. Структура LattiGo позволяет проводить различные исследования схем, экспериментировать как с полными схемами, так и с отдельными операциями, выполняемыми в этих схемах. Все схемы соответствуют общепринятым стандартам безопасности.

Для анализа эффективности предложенного в настоящей работе алгоритма авторами выполнен анализ результатов, полученных в работе [1] с точки зрения времени выполнения таких операций, как: шифрование, дешифрование, сложение, умножение, отношение сигнал шум зашифрованного текста к открытому тексту. Измерения в работе [1] проводятся для разных размерностей вектора (от 128 до 2048 чисел) и для разных параметров шифрования (ID): чем выше уровень ID, тем выше уровень обеспечиваемой безопасности данных.

Сравнение времени выполнения функции шифрования для алгоритмов полностью гомоморфного шифрования (схем BFV и CKKS) в зависимости от рассмотренных наборов параметров безопасности (ID) и размерности вектора данных позволяет сделать следующие выводы: обе схемы шифрования имеют примерно одинаковую скорость по первым трем наборам параметров безопасности. При наивысших требованиях к уровню безопасности, схема BFV хуже масштабируется и имеет более низкую скорость, что говорит о том, что в целом BFV незначительно уступает по выполнению этой функции схеме CKKS. Данная ситуация объясняется особенностями арифметической реализации.

Сравнение времени выполнения функции расшифрования для алгоритмов полностью гомоморфного шифрования (схем BFV и CKKS) в зависимости от рассмотренных наборов параметров безопасности (ID) и размерности вектора данных позволяет сделать следующие выводы: обе схемы шифрования имеют сопоставимую скорость по первым двум наборам параметров безопасности. Однако при наивысших требованиях к уровню безопасности, схема BFV имеет более низкую производительность, что говорит о том, что BFV существенно уступает по выполнению этой функции схеме CKKS.

Сравнение времени выполнения функции сложения для алгоритмов полностью гомоморфного шифрования (схем BFV и CKKS) в зависимости от рассмотренных наборов параметров безопасности (ID) и размерности вектора данных позволяет сделать следующие выводы: изучение функции гомоморфного сложения также показывает преимущество схемы CKKS. Это связано с тем, что в схеме CKKS данные правильно масштабируются перед операцией.

Сравнение времени выполнения функции умножения для алгоритмов полностью гомоморфного шифрования (схем BFV и CKKS) в зависимости от рассмотренных наборов параметров безопасности (ID) и размерности вектора данных позволяет сделать следующие выводы: изучение функции гомоморфного умножения показывает преимущество схемы BFV. Это связано с тем, что схема BFV имеет скалярное умножение только для типа uint64, в то время как схема CKKS предоставляет решение для таких типов, как complex128, float64, uint64, int64 и int. При умножении зашифрованного текста на типы данных complex128, float64 (для CKKS) очевидно, требуется больше времени, чем при умножении на константу типа uint64 в схеме BFV, однако этот недостаток нивелируется возможностью работы с различными типами данных.

Известно, что полученный с помощью схем полностью гомоморфного шифрования зашифрованный текст имеет избыточность. Степень этой избыточности является важным параметром схем полностью гомоморфного шифрования. Эту избыточность можно определить, исследуя отношение сигнал шум.

Сравнение отношения сигнал шум для алгоритмов полностью гомоморфного шифрования (схем BFV и CKKS) в зависимости от рассмотренных наборов параметров безопасности (ID) и размерности вектора данных позволяет сделать следующие выводы: при шифровании открытого текста шум в схеме CKKS увеличивается намного больше, чем в схеме BFV. Но при более высоких настройках безопасности ее увеличение уменьшается. В целом можно отметить, что при более низких настройках безопасности и большей размерности зашифрованного текста схема BFV показывает меньшую избыточность данных, но в случае высоких настроек безопасности схема CKKS явно более эффективна.

Подводя итоги, стоит отметить, что схема полностью гомоморфного шифрования CKKS наиболее эффективна, особенно в условиях критичности требований к высокому уровню безопасности конфиденциальных данных, чем обусловлен выбор данной схемы для реализации предложенного в настоящей работе алгоритма.

Заключение. Оценка эффективности разработанной облачной платформы хранения, систематизации и обработки медицинских данных:

Иерархичное разделение потоков данных на уровни, стандартизация протоколов передачи данных и форматов их хранения обеспечивают создание универсальной, гибкой и надежной медицинской информационной системы. Разработанная архитектура позволяет быстро интегрироваться в существующие медицинские системы. Единое пространство для хранения данных дает возможность осуществлять исследование значительного массива классифицированной медицинской информации средствами машинного обучения.

Разработан алгоритм обеспечения безопасности медицинских данных, хранимых в облачной платформе в электронном виде, регистрируемых при проведении обследований пациентов с целью расчета среднего значения для каждого из ритмов мозговой активности (по результатам серии обследований за длительный период времени) с использованием алгоритма полностью гомоморфного шифрования. На основе результатов работы [1] в части тестирования (анализ времени выполнения таких операций, как: шифрование, дешифрование, сложение, умножение, отношение сигнал шум зашифрованного текста к открытому тексту) из двух потенциальных претендентов на использование в качестве алгоритмов полностью гомоморфного шифрования (схемы BFV и CKKS) выбран наиболее оптимальный алгоритм. В результате показано, что схема полностью гомоморфного шифрования CKKS наиболее эффективна, особенно в условиях критичности требований к высокому уровню безопасности конфиденциальных данных, чем обусловлен выбор данной схемы для реализации предложенного в настоящей работе алгоритма.

Работа выполнена при поддержке гранта РФФИ №20-37-90138 Аспиранты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бабенко М.Г., Голимблевская Е.И., Ширяев Е.М.* Сравнительный анализ алгоритмов гомоморфного шифрования на основе обучения с ошибками // Тр. ИСП РАН. – 2020. – № 2.
2. *Митькина П.А.* Особенности хранения медицинской информации // Современные научные исследования и инновации. – 2017. – № 5. – URL: http://web.snauka.ru/issues/2017/05/82546 (дата обращения: 07.10.2019).
3. Health Insurance Portability and Accountability Act. – URL: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act (дата обращения: 08.10.2019).
4. DICOM. – URL: https://ru.wikipedia.org/wiki/DICOM (дата обращения 08.10.2019).
5. *L.-Y. T. a. M.-S. H. Li-Chin Huangc.* A reversible data hiding method by histogram shifting in high quality medical images // The Journals of systems and software. – 2013. – Vol. 86. – P. 716-727.
6. *M.G. a. R.D. Jessica Fridrich.* Detecting LSB Steganography in Color and Gray-Scale Images. Binghamton.
7. *N.A.H.A.-C. Fatma E.-Z. A. Elgamal.* Secure Medical Images Sharing over Cloud Computing environment // International Journal of Advanced Computer Science and Applications. – 2013. – Vol. 4. – P. 130-138. A. B. K. R. G. a. J. P. S. Digvijay Singh Chauhan, "Double Secret Key Based Medical Image Watermarking for Secure Telemedicine in Cloud Environment // in 2017 40th International Conference on Telecommunications and Signal Processing (TSP), 2017.
8. Logistic map. – URL: https://en.wikipedia.org/wiki/Logistic_map (дата обращения 08.10.2019).
9. *Abdulrahman Alsalmany*. Cloud System for Encryption and Authentication Medical Images // IOSR Journal of Computer Engineering. e-ISSN: 2278-0661, p-ISSN: 2278-8727. – Vol. 20, Issue 1, Ver. II (Jan.-Feb. 2018). – P. 65-75. –https://www.researchgate.net/publication/332571801_Cloud_System_For_Encryption_And_Authentication_Medical_Images (дата обращения: 29.09.2019).
10. *Плотников А.В., Прилуцкий Д.А., Селищев С.В.* Стандарт DICOM в компьютерных медицинских технологиях. – https://mks.ru/library/article/1997/dicom.html (дата обращения 08.10.2019).

11. Визуальная криптография. – URL: http://cryptowiki.net/index.php?title=%D0%92%D0%B8%D0%B7%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F (дата обращения: 08.10.2019).
12. *Котяшичев И.А., Бырылова Е.А.* Защита информации в «Облачных технологиях» как предмет национальной безопасности. – Текст: непосредственный // Молодой ученый. – 2015. – № 6.4 (86.4). – С. 30-34. – URL: https://moluch.ru/archive/86/16357/ (дата обращения: 09.06.2020).
13. *Керейтова М.Р., Малыш В.Н.* Информационная безопасность в медицинских информационных системах // НиКа. – 2012. – URL: https://cyberleninka.ru/article/n/ informatsionnaya-bezopasnost-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 11.06.2020).
14. *Бойченко И.В.* Построение ИТ-инфраструктуры здравоохранения на основе парадигмы облачных вычислений // Врач и информационные технологии. – 2011. – № 3. – URL: https://cyberleninka.ru/article/n/postroenie-it-infrastruktury-zdravoohraneniya-na-osnove-paradigmy-oblachnyh-vychisleniy (дата обращения: 09.06.2020).
15. *Rohan Jathanna*. Int. Journal of Engineering Research and Application. – June 2017. – Vol. 7, Issue 6 (Part - 5). – P. 31-38. – ISSN: 2248-9622. – www.ijera.com. (дата обращения: 10.06.2020).
16. *Кривошеева Дарина*. Модель угроз безопасности в системах дистанционного мониторинга состояния человека // Правовая информатика. – 2016. – № 3. – URL: https://cyberleninka.ru/article/n/model-ugroz-bezopasnosti-v-sistemah-distantsionnogo-monitoringa-sostoyaniya-cheloveka (дата обращения: 11.06.2020).
17. *Назаренко Г.И., Михеев А.Е., Горбунов П.А., Гулиев Я.И., Фохт И.А., Фохт О.А.* Особенности решения проблем информационной безопасности в медицинских информационных системах // Врач и информационные технологии. – 2007. – № 4. – URL: https://cyberleninka.ru/article/n/osobennosti-resheniya-problem-informatsionnoy-bezopasnosti-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 16.10.2020).
18. *Горбунов П.А., Фохт И.А.* Проблемы информационной безопасности в медицинских информационных системах – теоретические решения и практические разработки // Программные системы: теория и приложения / под ред. С.М. Абра-мова. В 2- х т. Т. 1. – М.: Физматлит, 2006. – С. 107-112.
19. *Назаренко Г.И, Гулиев Я.И., Ермаков Д.Е.* Медицинские информационные системы: теория и практика / под ред. Г.И. Назаренко, Г.С. Осипова. – М.: Физматлит, 2005. – 320 с.
20. *Михеев В.А.* Основы построения подсистемы защиты информации многофункциональной информационной системы // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 165-167.
21. *Клепиков Е.А., Ясько А.О.* Вопросы защиты конфиденциальной медицинской информации о пациенте в медицинских информационных системах // Символ науки. – 2016. – № 9-1. – URL: https://cyberleninka.ru/article/n/voprosy-zaschity-konfidentsialnoy-meditsinskoy-informatsii-o-patsiente-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 16.10.2020).

REFERENCES

1. *Babenko M.G., Golimblevskaya E.I., SHiryaev E.M.* Sravnitel'nyy analiz algoritmov gomomorfnogo shifrovaniya na osnove obucheniya s oshibkami [Comparative analysis of homomorphic encryption algorithms based on learning with errors], *Tr. ISP RAN* [Proceedings of ISP RAS], 2020, No. 2.
2. *Mit'kina P.A.* Osobennosti khraneniya meditsinskoy informatsii [Features of storing medical information], *Sovremennye nauchnye issledovaniya i innovatsii* [Modern scientific research and innovations], 2017, No. 5. Available at: http://web.snauka.ru/issues/2017/05/82546 (accessed 07 October 2019).
3. Health Insurance Portability and Accountability Act. Available at: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act (accessed 08 October 2019).
4. DICOM. Available at: https://ru.wikipedia.org/wiki/DICOM (дата обращения 08.10.2019).
5. *L.-Y. T. a. M.-S. H. Li-Chin Huangc.* A reversible data hiding method by histogram shifting in high quality medical images, *The Journals of systems and software*, 2013, Vol. 86, pp. 716-727.

6. *M.G. a. R.D. Jessica Fridrich.* Detecting LSB Steganography in Color and Gray-Scale Images. Binghamton.
7. *N.A.H.A.-C. Fatma E.-Z. A. Elgamal.* Secure Medical Images Sharing over Cloud Computing environment, *International Journal of Advanced Computer Science and Applications*, 2013, Vol. 4, pp. 130-138. A. B. K. R. G. a. J. P. S. Digvijay Singh Chauhan, "Double Secret Key Based Medical Image Watermarking for Secure Telemedicine in Cloud Environment, *in 2017 40th International Conference on Telecommunications and Signal Processing (TSP), 2017.*
8. Logistic map. Available at: https://en.wikipedia.org/wiki/Logistic_map (accessed 08 October 2019).
9. *Abdulrahman Alsalmany.* Cloud System for Encryption and Authentication Medical Images, *IOSR Journal of Computer Engineering.* e-ISSN: 2278-0661, p-ISSN: 2278-8727, Vol. 20, Issue 1, Ver. II (Jan.-Feb. 2018), pp. 65-75. Available at: https://www.researchgate.net/ publication/332571801_Cloud_System_For_Encryption_And_Authentication_Medical_Images (accessed 29 September 2019).
10. *Plotnikov A.V., Prilutskiy D.A., Selishchev S.V.* Standart DICOM v komp'yuternykh meditsinskikh tekhnologiyakh [DICOM standard in computer medical technologies]. Available at: https://mks.ru/library/article/1997/dicom.html (data obrashcheniya 08 October 2019).
11. Vizual'naya kriptografiya [Visual cryptography]. Available at: http://cryptowiki.net/ index.php?title=%D0%92%D0%B8%D0%B7%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F (accessed 08 October 2019).
12. *Kotyashichev I.A., Byrylova E.A.* Zashchita informatsii v «Oblachnykh tekhnologiyakh» kak predmet natsional'noy bezopasnosti [Information protection in "Cloud technologies" as a subject of national security], *Molodoy uchenyy* [Young scientist], 2015, No. 6.4 (86.4), pp. 30-34. Available at: https://moluch.ru/archive/86/16357/ (accessed 09 June 2020).
13. *Kereytova M.R., Malysh V.N.* Informatsionnaya bezopasnost' v meditsinskikh informatsionnykh sistemakh [Information security in medical information systems], *NiKa* [NIK], 2012. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-meditsinskih-informatsionnyh-*sistemah* (accessed 11 June 2020).
14. *Boychenko I.V.* Postroenie IT-infrastruktury zdravookhraneniya na osnove paradigmy oblachnykh vychisleniy [Building IT infrastructure for healthcare based on the paradigm of cloud computing], *Vrach i informatsionnye tekhnologii* [Doctor and information technologies], 2011, No. 3. Available at: https://cyberleninka.ru/article/n/postroenie-it-infrastruktury-zdravoohraneniya-na-osnove-paradigmy-oblachnyh-vychisleniy (accessed 09 June 2020).
15. *Rohan Jathanna*. Int. Journal of Engineering Research and Application, June 2017, Vol. 7, Issue 6 (Part - 5), pp. 31-38. ISSN: 2248-9622. Available at: www.ijera.com (accessed 10 June 2020).
16. *Krivosheeva Darina.* Model' ugroz bezopasnosti v sistemakh distantsionnogo monitoringa sostoyaniya cheloveka [Model of security threats in systems of remote monitoring of human condition], *Pravovaya informatika* [Legal informatics], 2016, No. 3. Available at: https://cyberleninka.ru/article/n/model-ugroz-bezopasnosti-v-sistemah-distantsionnogo-monitoringa-sostoyaniya-cheloveka (accessed 11 June 2020).
17. *Nazarenko G.I., Mikheev A.E., Gorbunov P.A., Guliev Ya.I., Fokht I.A., Fokht O.A.* Osobennosti resheniya problem informatsionnoy bezopasnosti v meditsinskikh informatsionnykh sistemakh [Features of solving information security problems in medical information systems], *Vrach i informatsionnye tekhnologii* [Doctor and information Technology], 2007, No. 4. Available at: https://cyberleninka.ru/article/n/osobennosti-resheniya-problem-informatsionnoy-bezopasnosti-v-meditsinskih-informatsionnyh-sistemah (accessed 16 October 2020).
18. *Gorbunov P.A., Fokht I.A.* Problemy informatsionnoy bezopasnosti v meditsinskikh informatsionnykh sistemakh – teoreticheskie resheniya i prakticheskie razrabotki [Information security problems in medical information systems - theoretical solutions and practical developments], *Programmnye sistemy: teoriya i prilozheniya* [Software systems: theory and applications], ed. by S.M. Abramova. In 2 vol. Vol. 1. Moscow: Fizmatlit, 2006, pp. 107-112.
19. *Nazarenko G.I, Guliev Ya.I., Ermakov D.E.* Meditsinskie informatsionnye sistemy: teoriya i praktika [Medical information systems: theory and practice], ed. by G.I. Nazarenko, G.S. Osipova. Moscow: Fizmatlit, 2005, 320 p.

20. *Mikheev V.A.* Osnovy postroeniya podsistemy zashchity informatsii mnogofunktsional'noy informatsionnoy sistemy [Fundamentals of building a subsystem of information security for a multifunctional information system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2008, No. 8 (85), pp. 165-167.
21. *Klepikov E.A., YAs'ko A.O.* Voprosy zashchity konfidentsial'noy meditsinskoy informatsii o patsiente v meditsinskikh informatsionnykh sistemakh [Issues of protecting confidential medical information about a patient in medical information systems], *Simvol nauki* [Symbol of Science], 2016, No. 9-1. Available at: https://cyberleninka.ru/article/n/voprosy-zaschity-konfidentsialnoy-meditsinskoy-informatsii-o-patsiente-v-meditsinskih-informatsionnyh-sistemah (accessed 16 October 2020).

Статью рекомендовал к опубликованию д.э.н., профессор Е.Н. Тищенко.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; г. Таганрог, Россия; тел.: +79054530191; д.т.н.; профессор.

Шумилин Александр Сергеевич – e-mail: ashumilin@sfedu.ru; тел.: +79081773495; м.н.с.

Алексеев Дмитрий Михайлович – e-mail: dalekseev@sfedu.ru; тел.: +7951 5069532; ассистент.

Babenko Lyudmila Klimentievna – Southern Federal University; e-mail: lkbabenko@sfedu.ru; Taganrog, Russia; phone: +79054530191; dr. of eng. sc.; professor.

Shumilin Alexander Sergeevich – e-mail: ashumilin@sfedu.ru; phone: +79081773495; junior researcher.

Alekseev Dmitry Mikhailovich – e-mail: dalekseev@sfedu.ru; phone: +79515069532; assistant.

УДК 004.032 DOI 10.18522/2311-3103-2021-5-134-145

С.М. Гушанский, В.Н. Пуховский, В.С. Потапов

РЕАЛИЗАЦИЯ ВЕРОЯТНОСТНОГО ДЕКОДЕРА ГЛУБОКОЙ НЕЙРОННОЙ СЕТИ ДЛЯ КОДОВ СТАБИЛИЗАТОРА

В последнее время наблюдается стремительный рост интереса к квантовым компьютерам. Их работа основана на использовании для вычислений таких квантово-механических явлений, как суперпозиция и запутывание для преобразования входных данных в выходные, которые реально смогут обеспечить эффективную производительность на 3–4 порядка выше, чем любые современные вычислительные устройства, что позволит решать перечисленные выше и другие задачи в натуральном и ускоренном масштабе времени. Данная работа является исследованием влияния среды на квантовую систему кубитов и результаты ее выполнения. Разработан вероятностный декодер глубокой нейронной сети для кодов стабилизатора. Проанализированы и рассмотрены вопросы исправления ошибок для трехбитового кода без декодирования состояния. Актуальность данных исследований заключается в математическом и программном моделировании и реализации корректирующих кодов для исправления нескольких видов квантовых ошибок в рамках разработки и выполнения квантовых алгоритмов для решения классов задач классического характера. Научная новизна данного направления выражается в исключении одного из недостатков квантового вычислительного процесса. Научная новизна данного направления в первую очередь выражается в постоянном обновлении и дополнении поля квантовых исследований по ряду направлений.

Моделирование; квантовый алгоритм; кубит; модель квантового вычислителя; запутывание; суперпозиция; квантовый оператор.