# Раздел I. Алгоритмы обработки информации

УДК 004.056.55 DOI 10.18522/2311-3103-2023-4-6-13

**Л.К. Бабенко, А.С. Шумилин**

## ИСПОЛЬЗОВАНИЕ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ ДЛЯ РЕАЛИЗАЦИИ МЕТОДА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НА ОСНОВЕ СХЕМЫ ШАМИРА В МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ*

*В современном мире медицинские информационные системы становятся наиболее популярными инструментами для обработки, хранения, систематизации и передачи медицинских данных пациентов. Медицинские обследования могут быть представлены в виде файлов различных форматов и сильно варьироваться по размеру (от нескольких байт до сотен гигабайт). Например, некоторые двоичные файлы имеют малый размер поскольку содержат лишь заключения врачей в виде текстового описания, а файлы, записи ночного видеомониторинга пациента или DICOM-файлы компьютерной томограммы органов человека, содержащие несколько сотен слайсов могут достигать размера в сотни гигабайт. Соответственно, большие файлы требуют значительных вычислительных ресурсов при передаче с сервера на сервер. Кроме того, при использовании метода обеспечения безопасности, который представляет собой алгоритм разделения секрета (файла с обследованием) по схеме Шамира операции, операции по разделению секрета на части и слиянию частей воедино могут занимать больше времени при последовательном режиме работы, чем при параллельном. Поэтому, видится возможность ускорить процесс обработки больших данных без снижения уровня безопасности. Целью работы является подтверждение гипотезы уменьшения времени на выполнения операцией разделения и слияния частей секрета с использованием средств параллельных вычислений при реализации метода обеспечения безопасности по схеме разделения секрета Шамира в медицинской информационной системе. Объектом исследования является метод обеспечения безопасности, который разработан авторами для внедрения в подсистемы защиты информации медицинской информационной системы. В рамках исследования проведен анализ наиболее эффективных средств для распараллеливания процессов (MPI и OpenMP) и выбран инструмент, подходящий под решение поставленной цели. Также проведены эксперименты (анализ времени в зависимости от количества параллельных потоков и количества символов, содержащихся в DICOM файле), которые подтвердили концепцию возможности распараллелить алгоритм обмена секретом на основе схемы Шамира, добившись почти линейного ускорения с помощью библиотеки MPI.*

*Безопасность данных; параллельные вычисления; медицинская информационная система; MPI; большие данные.*

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90138.

**L.K. Babenko, A.S. Shumilin**

## USE OF PARALLEL COMPUTING FOR SECURITY METHOD IMPLEMENTATION BASED ON THE SHAMIR SCHEME IN A MEDICAL INFORMATION SYSTEM

*Medical information systems currently are becoming the most popular tools for processing, storing, organizing, and transmitting patient medical data. Medical examinations can be presented in the form of files in various formats and vary greatly in terms of size (from a few bytes to hundreds of gigabytes). For example, some binary files are small and lightweight because they contain only doctors' conclusions in the form of a text description. However, records of night video monitoring of a patient or DICOM files of human organs CT scans containing several hundred slices, can reach hundreds of gigabytes in size. Accordingly, large files require significant computing resources when transferred from server to server. In addition, when using the security method, which is an algorithm of a secret sharing (medical output file) according to the Shamir sharing scheme, operations to split the secret into parts and merge the parts together may take longer in serial operation than in parallel way. Therefore, it seems possible to speed up the processing of big data without reducing the level of security. The main purpose of the work is to confirm the hypothesis of reducing time to perform the operation of splitting and merging parts of a secret based on parallel computing tools withing implementing the security method according to the Shamir secret sharing scheme in a medical information system. The object of the study is a security method developed by the author for implementation in the information security subsystems of a medical information system. As part of the study, author analyzed the most effective tools for parallelizing processes (like MPI and OpenMP). MPI has been used as a tool as much more suitable for the current purpose. Moreover, several waves of experiments have been run (analysis of time depending on the number of parallel streams and the number of characters contained in the DICOM file) and allowed us to prove a concept of parallelizing the secret exchange algorithm based on the Shamir scheme, achieving almost linear acceleration using the MPI library.*

*Data security; parallel computing; medical information system; MPI; big data.*

**Введение.** На сегодняшний день процессы накопления и обработки информации в сфере здравоохранения набирают свою актуальность из-за масштабной информатизации как в рамках Российской Федерации, так и в целом в мире [1]. Задачи, связанные с хранением, систематизацией и обработкой больших объемов данных делают актуальным процесс разработки медицинских информационных систем (МИС). Благодаря электронному документообороту у медицинского персонала появляется возможность оперативно принимать решения о постановке диагноза и оказывать необходимую помощь [2]. В нашей стране медицинские организации участвуют в сборе, накоплении, хранении, изменении, распространении и уничтожении конфиденциальной информации.

Одной из проблем при проектировании медицинских информационных систем является **потребность в интеграции систем защиты** конфиденциальной информации, которая является основным объектом защиты внутри МИС. Соответственно, в медицинской информационной системе видится необходимость внедрения подсистемы **механизмов защиты**, который представляет собой метод обеспечения защиты конфиденциальных данных на основе схемы разделения секрета Шамира, предложенный, реализованный и исследованный авторами [3, 4].

Идея схемы Шамира заключается в том, что двух точек достаточно для задания прямой, трех точек – для задания параболы, четырёх точек – для кубической параболы, и так далее. Чтобы задать многочлен степени k, требуется k+1 точек [5].

Для того, чтобы после разделения секрет *M* могли восстановить только *k* участников, его скрывают в формулу многочлена степени *(k-1)* над конечным полем *G(k).* Для однозначного восстановления этого многочлена необходимо знать его значения в *k* точках, причем, используя меньшее число точек, однозначно восста-

новить исходный многочлен не получится. Количество же различных точек многочлена не ограничено (на практике оно ограничивается размером числового поля, в котором ведутся расчёты) [6, 7].

Алгоритм можно описать следующим образом: пусть дано конечное числовое поле, в котором зафиксировано n различных ненулевых несекретных элементов. Каждый из этих элементов приписывается определённому члену группы. Чтобы восстановить секрет, можно воспользоваться интерполяционной формулой, например формулой Лагранжа [8, 9].

Многочлен *L(x)* минимальной степени, принимающий значения в заданном наборе точек, то есть решающий задачу интерполяции.

$$L(x) = \sum_{i=0}^{n} y_i l_i(x), \quad (1)$$

где $y_i$ и $l_i$ – *базисные полиномы*

Важным достоинством схемы Шамира является то, что она легко масштабируема. Чтобы увеличить число пользователей, необходимо лишь добавить соответствующее число несекретных элементов к существующим. В то же время компрометация одной части секрета переводит схему из (n,t) пороговой в (n-1, t-1)-пороговую [10].

**Анализ проблемы.** Схема разделения секрета Шамира представляет собой метод разделения секрета между группами, где для воспроизведения секрета необходимо объединить определенный порог ключей. С большими секретами, такими как целый текстовый документ, этот процесс может быть медленным и дорогим, особенно если число участников и порог высоки. Возникает необходимость к использованию параллельных вычислительных систем для повышения безопасности и ускорения. Существующие в современном мире программные решения актуальны в сфере здравоохранения, в первую очередь для обеспечения безопасности конфиденциальных данных [11, 12].

В качестве примера можно выделить отчеты, изображения, DICOM и Nifti – файлы, как наиболее часто используемые артефакты из области медицины.

**Основная часть.** В данной работе приведены результаты исследования распараллеливания алгоритма Шамира с целью сокращения времени, затрачиваемого как на создание, так и на объединение общих ресурсов в масштабируемом виде.

Масштабирование в анализе высокопроизводительных программ делится на две категории: «сильное» и «слабое» масштабирование.

- сильное масштабирование описывает, как производительность изменяется по мере увеличения количества процессов или потоков при фиксированном размере задачи;
- слабое масштабирование исследует, как изменяется производительность по мере увеличения количества процессоров/потоков и размера задачи.

Как ранее упоминалось, алгоритм совместного использования секрета по схеме Шамира требует наличия двух параметров:

- желаемого количества общих ресурсов (n);
- порогового значения, необходимого для «разблокировки» секрета (t).

Алгоритм вычисляет доли, генерируя случайное полиномиальное уравнение степени *t-1*. Секрет становится постоянной величиной в полиномиальном уравнении.

$$Пример: 9x^3 + 2x^2 + 3x + секрет. \quad (2)$$

Требуемый порог для воспроизведения секрета функции, указанной в формуле 3, будет равен 4 долям, потому что t = 4 дает полином степени 3 (t-1). После генерации случайного полинома алгоритм вычисляет пары координат X и Y, генерируя случайное значение X и подставляя его в полиномиальную функцию для получения соответствующего значения Y.

$$Y = ax^3 + bx^2 + cx + секрет. \quad (3)$$

В представленной реализации делается дополнительный шаг, и весь полином вычисляется по модулю простого большого числа, например, 257. Это решает проблему получения злоумышленником информации о секрете с помощью каждого найденного ключа, используя арифметику конечных полей вместо целочисленной арифметики.

Проблема с таким подходом (при последовательном вычислении) заключается в том, что для каждого символа входных данных должна итерация должна выполняться n раз. Этот процесс медленный, а значит может быть представлена возможность реализовать параллельные вычисления.

Реализация алгоритма разделения секрета Шамира [13] с открытым исходным кодом на языке С позволила исследовать преимущества распараллеливания алгоритма. Общая цель заключалась в том, чтобы ускорить процесс разделения и слияния долей секрета для больших файлов с учетом большого количества взаимодействующих сторон без проигрыша в безопасности.

Был проведен анализ основных стандартов для распараллеливания программ, среди которых номинальными кандидатами оказались OpenMP и MPI [14].

OpenMP – представляет собой способ программирования на вычислительных мощностях с общей оперативной памятью [15]. Это означает, что параллелизм существует в том случае, когда каждый параллельный поток имеет доступ ко всем имеющимся данным - то есть в процессе выполнения определенного цикла «for» разделяя этот цикл между всеми потоками [16].

MPI – это библиотека для разработки и ускореня программного кода на устройствах с распределенной памятью. Параллелизм существуем, в том случае если каждый процесс работает **в своем собственном пространстве памяти** изолированно от других [17]. Иначе говоря, каждый бит программного кода, выполняется независимо отдельным процессом. Параллелизм происходит потому, что каждому процессу абсолютно точно указывается, над какой частью конкретной задачи он должен работать, основываясь исключительно на идентификаторе процесса [18].

Таким образом для решения задачи в рамках распределенной медицинской системы наиболее оптимальным с точки зрения эффективного потребления ресурсов вариантом является способ на основе библиотеки MPI. Для подтверждения теории были проведены экспериментальные расчеты. Все эксперименты проводились на локальной рабочей станции: процессор Intel Core i7 – 11800H (8-ядер по 2,3 ГГц с гиперпоточностью), 16 ГБ ОЗУ с использованием максимального количества долей и порогового значения, которое исходная программа могла сгенерировать (255 долей ключа). В качестве тестовых наборов данных использовались DICOM-файлы, содержащие 500, 1000, 2000, 4000 и 8000 символов в случайных полях.

Эксперименты «слабого масштабирования» заключались в удвоении количества символов во входном файле при одновременном удвоении количества потоков. Были определены 2 функции в реализации, которые позволили существенно сократить время вычисления долей.

*Во-первых,* удалось распараллелить процесс генерации случайных коэффициентов, используемых в полиномиальной функции.

*Во-вторых,* удалось распараллелить генерацию общих долей ключей. Оставив функцию слияния долей нетронутой, реализована проверка корректности процесса распараллеливания, поскольку функция могла повторно собрать общие ресурсы в исходный файл. После реализации параллелизма на этапе генерации доли схемы разделения секрета Шамира и проверки корректности этого преобразования принято решение реализовать параллелизм и в функции слияния долей.

Проблема с распараллеливанием этапа соединения общих ресурсов в процессе совместного использования секрета Шамиром заключается в правильном определении области действия переменных MPI (т. е. выборе переменных, которые должны быть видны всем потокам), а также в определении и выделении критических областей. Наиболее важная область – это место, где каждый поток обновляет секрет после вычисления интерполяционных полиномов Лагранжа [19, 20]. Для этого пришлось синхронизировать доступ к такой области с помощью функционала библиотеки MPI, что позволило распараллелить цикл, вычисляющий интерполирующий полином Лагранжа функции, используемой при соединении долей обратно воедино.

Предлагаемый способ демонстрирует значительное ускорение при разделении и объединение долей секрета в схеме Шамира с помощью библиотеки MPI. Ниже приведены результаты.

В табл. 1 показано для «сильного масштабирования», что время создания общих ключей уменьшается почти вдвое каждый раз, когда мы удваиваем количество потоков, что означает, что такая реализация обеспечивает близкое к линейному ускорение.

Таблица 1

**Время необходимое для генерации 255 долей секрета с порогом 255**

| Количество потоков | 1000 – символьный файл |
|---|---|
| 1 | 8.42 сек |
| 2 | 4.24 сек |
| 4 | 2.35 сек |
| 8 | 1.3 сек |
| 16 | 0.7 сек |

Были получены аналогичные результаты масштабирования при повторном объединении общих ресурсов для восстановления исходного секрета, как показано в табл. 2. Здесь важно отметить, что происходит увеличение времени при 16 потоках при обратном объединении общих ресурсов. Это соответствует количеству физических ядер тестовой машины (восемь с шестнадцатью гиперпотоками). На этом этапе увеличение количества потоков становится контрпродуктивным, поскольку они не могут выполняться параллельно на таком оборудовании.

Таблица 2

**Время необходимое на восстановление 255 долей секрета**

| Количество потоков | 1000 – символьный файл |
|---|---|
| 1 | 1.48 сек |
| 2 | 0.75 сек |
| 4 | 0.4 сек |
| 8 | 0.29 сек |
| 16 | 0.33 сек |

Табл. 3 показывает результаты для «слабого масштабирования», а именно, что время не увеличивается пропорционально, поскольку были удвоены как размер входных данных, так и количество потоков.

Таблица 3

**Изменение времени при генерации долей секрета с одновременным удвоением количества символов и потоков**

| Количество потоков | Количество символов | Время |
|---|---|---|
| 1 | 500 | 4,53 сек |
| 2 | 1000 | 4.65 сек |
| 4 | 2000 | 5.07 сек |
| 8 | 4000 | 5.66 сек |
| 16 | 8000 | 7.13 сек |

**Заключение:** в рамках исследования произведен процесс распараллеливания алгоритма обмена секретом на основе схемы Шамира, в предложенном авторами методе обеспечения безопасности в рамках медицинской информационной системы. Подход на основе подключения библиотеки MPI позволил добиться почти линейного ускорения и сократить время генерации долей секрета в 1,87 раза и в 1,74 раза для задачи восстановления долей – при увеличении вдвое количества потоков. Подход демонстрирует ускорение на локальной машине (Intel Core i7 – 11800H: 8-ядер по 2,3 ГГц с гиперпоточностью до 16, 16 ГБ ОЗУ). Можно сделать предположение, что в распределенной облачной системе удастся добиться большего ускорения поскольку будет использоваться значительное количество вычислительных ресурсов – количество ядер процессоров на распределенных серверах. Кроме того, использованная библиотека MPI для распараллеливания имеет большой функционал и поддержку облачных вычислений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. *Карнаухов Н.С., Ильюхин Р.Г.* Возможности технологий "Big Data" в медицине // Врач и информационные технологии. – 2019. – № 1.
2. *Калугина Е.А.* Система электронного документооборота, ее преимущества и переход на электронный документооборот // Вестник НИБ. – 2019. – № 37.
3. *Алексеев Д.М., Бабенко Л.К., Шумилин А.С.* Алгоритм обеспечения защиты конфиденциальных данных облачной медицинской информационной системы // Известия ЮФУ. Технические науки. – 2021. – № 5 (222). – С. 120-134.
4. *Shumilin A., Babenko L., Alekseev D.* Development of the algorithm to ensure the protection of confidential data in cloud medical information system // 2021 14th International Conference on Security of Information and Networks (SIN).
5. *Сундуков Р.Ш., Королева В.В.* Программное средство разделения секрета с использованием схемы Шамира // Безопасность информационного пространства: Сб. трудов XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых, Магнитогорск, 28–29 ноября 2019 года. – Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова, 2019. – С. 263-267. – EDN MGJHFO.
6. Схема разделения секрета Шамира. Хабр журнал. – Режим доступа: https://habr.com/ru/post/431392/ (дата обращения: 22.08.2023).
7. Cryptographic algorithms – Shamir Secret Sharing. – Режим доступа: https://cryptography.fandom.com/wiki/Shamir%27s_Secret_Sharing (дата обращения: 22.08.2023).
8. *Парватов Н.Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. – 2008. – № 2 (2). – С. 41-47.
9. *Червяков Н.И., Дерябин М.А.* Новый метод порогового разделения секрета, основанный на системе остаточных классов // Информационные технологии. – 2016. – Т. 22, № 3. – С. 211-219.
10. *Шенец Н.Н.* Об идеальных модулярных схемах разделения секрета в кольцах многочленов от нескольких переменных. – 2019.

11. *Мартишин С.А., Храпченко М.В., Шокуров А.В.* Исследование задачи обеспечения безопасности при хранении и обработке конфиденциальных данных // Тр. ИСП РАН. – 2021. – № 2.
12. *Минаков В.Ф., Шепелёва О.Ю., Лобанов О.С.* Многофакторная модель обеспечения безопасности конфиденциальных данных // Правовая информатика. – 2020. – № 1.
13. *Basavegowda R., Seenapp S.* Electronic Medical Report Security Using Visual Secret Sharing Scheme // 2013 UKSim 15th International Conference on Computer Modelling and Simulation.
14. *Титов К.Е.* Исследование поведения фреймворка openmp в программах с параллельными вычислениями // E-Scio. – 2021. – № 4 (55).
15. *Мартыненко С.И., Бахтин В.А., Румянцев Е.В., Тарасов Г.А., Середкин Н.Н., Боярских К.А.* Параллельное решение краевых задач с помощью технологии openmp // Вестник МГТУ им. Н.Э. Баумана. Сер. Естественные науки. – 2022. – № 2 (101).
16. *Аксенов С.В., Мальчуков А.Н., Мыцко Е.А.* Применение технологии параллельных вычислений OpenMP для поиска образующих полиномов // Вестник евразийской науки. – 2013. – № 6 (19).
17. MPI. – Режим доступа: https://ru.wikipedia.org/wiki/MPI (дата обращения: 22.08.2023).
18. *Тузко Я.Н., Соколова О.О., Акишин Б.А.* Организация параллельных вычислений в многоядерных процессорах // Молодой исследователь Дона. – 2018. – № 5 (14).
19. *Гервич Л.Р., Штейнберг Б.Я.* Об автоматизации применения размещения данных с перекрытиями в распределенной памяти // Вестник ЮУрГУ. Серия: Математическое моделирование и программирование. – 2023. – № 1.
20. *Листунов С.Б.* Исследование метода решения задач интерполяции функции методом полинома Лагранжа // Научные междисциплинарные исследования. – 2021. – № 2.

REFERENC

1. *Karnaukhov N.S., Il'yukhin R.G.* Vozmozhnosti tekhnologiy "Big Data" v meditsine [Possibilities of "Big Data" technologies in medicine], *Vrach i informatsionnye tekhnologii* [Doctor and information technologies], 2019, No. 1.
2. *Kalugina E.A.* Cistema elektronnogo dokumentooborota, ee preimushchestva i perekhod na elektronnyy dokumentooborot [Electronic document management system, its advantages and the transition to electronic document management], *Vestnik NIB* [Bulletin of the National Institute of Business], 2019, No. 37.
3. *Alekseev D.M., Babenko L.K., Shumilin A.S.* Algoritm obespecheniya zashchity konfidentsial'nykh dannykh oblachnoy meditsinskoy informatsionnoy sistemy [Algorithm for ensuring the protection of confidential data of a cloud medical information system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2021, No. 5 (222), pp. 120-134.
4. *Shumilin A., Babenko L., Alekseev D.* Development of the algorithm to ensure the protection of confidential data in cloud medical information system, *2021 14th International Conference on Security of Information and Networks (SIN).*
5. *Sundukov R.Sh., Koroleva V.V.* Programmnoe sredstvo razdeleniya sekreta s ispol'zovaniem skhemy Shamira [A software tool for sharing a secret using the Shamir scheme], *Bezopasnost' informatsionnogo prostranstva: Sb. trudov XVIII Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh, Magnitogorsk, 28–29 noyabrya 2019 goda* [Security of the information space: Collection of proceedings of the XVIII All-Russian scientific and practical conference of students, graduate students and young scientists, Magnitogorsk, November 28–29, 2019]. Magnitogorsk: Magnitogorskiy gosudarstvennyy tekhnicheskiy universitet im. G.I. Nosova, 2019, pp. 263-267. EDN MGJHFO.
6. Skhema razdeleniya sekreta Shamira. Khabr zhurnal [Shamir's secret sharing scheme. Habr magazine. – Access mode]. Available at: https://habr.com/ru/post/431392/ (accesse 22 August 2023).
7. Cryptographic algorithms – Shamir Secret Sharing. Available at: https://cryptography.fandom.com/wiki/Shamir%27s_Secret_Sharing (accesse: 22 August 2023).
8. *Parvatov N.G.* Sovershennye skhemy razdeleniya sekreta [Perfect secret sharing schemes], *Prikladnaya diskretnaya matematika* [Applied discrete mathematics], 2008, No. 2 (2), pp. 41-47.
9. *Chervyakov N.I., Deryabin M.A.* Novyy metod porogovogo razdeleniya sekreta, osnovannyy na sisteme ostatochnykh klassov [A new threshold secret sharing method based on a system of residual classes], *Informatsionnye tekhnologii* [Information technologies], 2016,Vol.. 22, No. 3, pp. 211-219.

10. *Shenets N.N.* Ob ideal'nykh modulyarnykh skhemakh razdeleniya sekreta v kol'tsakh mnogochlenov ot neskol'kikh peremennykh [On ideal modular secret sharing schemes in polynomial rings of several variables], 2019.
11. *Martishin S.A., Khrapchenko M.V., Shokurov A.V.* Issledovanie zadachi obespecheniya bezopasnosti pri khranenii i obrabotke konfidentsial'nykh dannykh [Study of the problem of ensuring security during the storage and processing of confidential data], *Tr. ISP RAN* [Proceedings of ISP RAS], 2021, No. 2.
12. *Minakov V.F., SHepeleva O.Yu., Lobanov O.S.* Mnogofaktornaya model' obespecheniya bezopasnosti konfidentsial'nykh dannykh [Multifactor model for ensuring the security of confidential data], *Pravovaya informatika* [Legal informatics], 2020, No. 1.
13. *Basavegowda R., Seenapp S.* Electronic Medical Report Security Using Visual Secret Sharing Scheme, *2013 UKSim 15th International Conference on Computer Modelling and Simulation*.
14. *Titov K.E.* Issledovanie povedeniya freymvorka openmp v programmakh s parallel'nymi vychisleniyami [Study of the behavior of the openmp framework in programs with parallel computing], *E-Scio*, 2021, No. 4 (55).
15. *Martynenko S.I., Bakhtin V.A., Rumyantsev E.V., Tarasov G.A., Seredkin N.N., Boyarskikh K.A.* Parallel'noe reshenie kraevykh zadach s pomoshch'yu tekhnologii openmp [Parallel solution of boundary value problems using openmp technology], *Vestnik MGTU im. N.E. Baumana. Ser. Estestvennye nauki* [Bulletin of MSTU im. N.E. Bauman. Series Natural Sciences], 2022, No. 2 (101).
16. *Aksenov S.V., Mal'chukov A.N., Mytsko E.A.* Primenenie tekhnologii parallel'nykh vychisleniy OpenMP dlya poiska obrazuyushchikh polinomov [Application of OpenMP parallel computing technology to search for generating polynomials], *Vestnik evraziyskoy nauki* [Bulletin of Eurasian Science], 2013, No. 6 (19).
17. MPI. Available at:https://ru.wikipedia.org/wiki/MPI (accessed 22 August.2023).
18. *Tuzko Ya.N., Sokolova O.O., Akishin B.A.* Organizatsiya parallel'nykh vychisleniy v mnogoyadernykh protsessorakh [Organization of parallel computing in multi-core processors], *Molodoy issledovatel' Dona* [Young researcher of the Don], 2018, No. 5 (14).
19. *Gervich L.R., Shteynberg B.Ya.* Ob avtomatizatsii primeneniya razmeshcheniya dannykh s perekrytiyami v raspredelennoy pamyati [On automation of the application of data placement with overlaps in distributed memory], *Vestnik YuUrGU. Seriya: Matematicheskoe modelirovanie i programmirovanie* [Bulletin of the South Ural State University. Series: Mathematical modeling and programming], 2023, No. 1.
20. *Listunov S.B.* Issledovanie metoda resheniya zadach interpolyatsii funktsii metodom polinoma Lagranzha [Research of a method for solving problems of interpolation of a function using the Lagrange polynomial method], *Nauchnye mezhdistsiplinarnye issledovaniya* [Scientific interdisciplinary research], 2021, No. 2.

Статью рекомендовал к опубликованию д.т.н. Г.Е. Веселов.

**Бабенко Людмила Климентьевна** – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; г. Таганрог, Роччия; тел.: +79054530191; кафедра безопасности информационных технологий; д.т.н.; профессор.

**Шумилин Александр Сергеевич –** e-mail: ashumilin@sfedu.ru; тел.: +79081773495; кафедра безопасности информационных технологий; программист.

**Babenko Ludmila Klimentyevna –** Southern Federal University; e-mail: lkbabenko@sfedu.ru; Taganrog, Russia; phone: +79054530191; the department of information technologies security; dr. of eng. sc.; professor.

**Shumilin Alexander Sergeevich –** e-mail: ashumilin@sfedu.ru; phone: +79081773495; the department of information technologies security; programmer.