УДК 004.056.5 Вестник УрФО № 1(51) / 2024, с. 14–21

Кротова Е.Л., Субботина Ю.В., Ермаков Д.Г., Тишин К.Л.

DOI: 10.14529/secur240102

ОСОБЕННОСТИ РАЗРАБОТКИ И ВНЕДРЕНИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Работа посвящена сравнительному анализу традиционного и электронного голосования. Определены основные проблемы, возникающие при внедрении электронного формата голосования, определенные Федеральным законом от 12.06.2002 N 67-ФЗ (ред. От 31.-7.2020) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации». На базе сформулированных критериев, следование которым свидетельствовало бы об улучшении решений и несоблюдение которых, на данный момент, является их слабой стороной. Сформулированы требования, которые предъявляются к любой системе голосования. Предложен вариант обхода существующих недостатков разрабатываемых и внедряемых систем электронного голосования.

Ключевые слова: *протокол электронного голосования, криптография, блокчейн.*

Krotova E.L., Subbotina Yu.V., Ermakov D.G., Tishin K.L.

PECULIARITIES OF DEVELOPMENT AND IMPLEMENTATION OF THE ELECTRONIC VOTING SYSTEM

The work is devoted to a comparative analysis of traditional and electronic voting. The main problems arising from the implementation of the electronic voting format, defined by the Federal Law of June 12, 2002 N 67-FZ (as amended on July 31, 2020) "On the basic guarantees of electoral rights and the right to participate in a referendum of citizens of the Russian Federation," are identified. Based on the formulated criteria, adherence to which would indicate an improvement in decisions and non-compliance with which, at the moment, is their weakness, the requirements that apply to any voting system are formulated. An option is proposed to bypass the existing shortcomings of electronic voting systems being developed and implemented.

Keywords: *electronic voting protocol, cryptography, blockchain.*

Голосование – это форма принятия решения, при которой общее мнение голосующей группы формулируется путем подсчета голосов ее членов.

Рассмотрим традиционную систему голосования (бумажную) и электронную систему голосования.

Традиционная аналоговая система голосования подразумевает под собой голосование с урной и бумажными бюллетенями на традиционном участке, где избиратель приходит на участок, предъявляет документ, который удостоверяет личность избирателя. Далее член избирательной комиссии при наличии избирателя в списке выдает ему бюллетень под роспись. Затем, избиратель проходит в индивидуальную кабину для голосования, где заполняет бюллетень и после опускает его в урну.

Электронная голосование – форма принятия решения, с помощью традиционного голосования, но с применением специальных электронных средств голосования и технических электронных средств, с помощью которых подсчитываются голоса и оглашаются результаты [1-3]. Стоит понимать, что, говоря о технических электронных средствах, мы в том числе подразумеваем под этим и сканеры избирательных бюллетеней. В менее обширном понимании электронным голосованием считается голосование с использованием машин прямой записи результатов без использования бумажных бюллетеней. Это новая концепция основана на криптографии. Система поддерживает полнофункциональное голосование онлайн на любых устройствах. Результаты опроса рассчитываются автоматически и анонимно.

Сравним традиционное голосование с электронным, используя наиболее важные требования, которые предъявляются к любой системе голосования.

Таблица 1

Сравнение видов голосования по заданным критериям

	Скорость обработки голосов	Экономия времени заполнения бюллетеней	Ход голосования в реальном времени	Эффективная масштабируемость
Бумажное голосование	ниже	ниже	Не доступно	ниже
Электронное голосование	выше	выше	доступно	выше

Выводы, которые мы можем сделать исходя из таблицы сравнения видов голосования по заданным критериям:

– электронное голосование более экономичная система;

– электронное голосование более прозрачная система;

– электронное голосование более объективная система.

Также важно отметить, что традиционная (бумажная) форма требует личного присутствия при процедуре голосования и больших финансовых затрат, если речь идет о выборах государственного масштаба. Электронное голосование, в свою очередь, позволяет сократить время избирателей на посещение избирательного участка и время подсчета голосов.

Не смотря на положительные стороны электронного голосования, система имеет большой риск фальсификации и компрометации результатов подсчета, так как может быть взломана третьими лицами, или администратором, который имеет доступ к машине, производящей подсчет голосов, с целью их изменения.

В связи с этим, стоит обратить внимание на основные требования, которые предъявляются к любой системе голосования, как для традиционного, так и для электронного формата голосования, определенные Федеральным законом от 12.06.2002 N 67-ФЗ (ред. От 31.-7.2020) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» и включают в себя [4, 5]:

1. Голосование на выборах должно быть тайным и исключать возможность контроля за волеизъявлением в любом виде.

2. Иметь возможность голосования могут только те лица, которые обладают активным избирательным правом на этом голосовании.

3. Не мало важно соблюдать принцип «один избиратель – один голос». Иными словами, «двойное» голосование не допускается.

4. Для тех, кто голосует, т.е. для избирате-

лей, а также для наблюдателей процесс голосования должен быть открытым и гласным.

5. Важно обозначить, что возможность неизменности поданного голоса также должна обеспечиваться.

6. Также возможность подсчитать промежуточные итоги голосования до его завершения должна гарантировано отсутствовать.

Для того, чтобы снизить риски нарушения требований к системам электронного голосования, было разработано большое множество протоколов связанных с конфиденциальностью бюллетеней, индивидуальной проверкой, надежностью, доступностью и т.д., где реализованы различные технологии, в том числе технологии «слепая подпись», «гомоморфное шифрование», «кольцевая подпись», «Mix networks», «доказательство с нулевым разглашением» и т.п. [6-10].

Анализируя практику применения сканеров избирательных бюллетеней (СИБ), констатируем два основных недостатка:

– отсутствует решение по защите от одновременного принятия более одного бюллетеня (голоса);

– нестабильность работы оптической схемы, которая распознает информацию о голосовании.

Существование этих недостатков потребовало разработки новой модели электронного голосования.

Поэтому, в 2001 году был разработан первый комплекс обработки избирательных бюллетеней (КОИБ), куда был встроен компьютер, который обеспечивал работу устройства и сохранял итоги голосования на дискету. Именно тогда, распечатываемые КОИБ итоги голосования стали иметь юридическую силу. Помимо того, что был исключен ручной подсчет бюллетеней, что существенно увеличило скорость получения результатов голосования, к тому же повысилось доверие избирателей к результатам. Эта модель просуществовала в период с 2004 по 2011 гг., а затем усовершенствовалась и служила эффективным инструментом для голосования вплоть до 2020 года [11-15]. Также, при анализе практики применения КОИБ, констатируем два основных недостатка:

– сложность в обслуживании и высокая стоимость машин;

– невозможность проверки корректности работы оборудования для голосования независимыми экспертами.

Попытки исследователей достигнуть поставленных целей при поиске наиболее эффективного способа голосования и подсчета голосов привели их к использованию технологии blockchain. С 2015 года исследователи США были заинтересованы в разработке и апробации блокчейн-голосования на платформе с приложением Web 3.0. Такое голосование предусматривало интернет-регистрацию избирателя и голосование с помощью ID-голосования и избирательного бюллетеня с QR-кодами. В том же году, исследователи З. Жао и Т. Чан представили способ голосования с использованием технологии blockchain и zk-SNARK, которые обеспечивали соблюдения свойств конфиденциальности, своевременной проверяемости и неизменяемости. В 2016 году П. С. Джейсон, и К. Ючи предложили протокол с использованием карт Bitcoin и слепой подписи. Но, система голосования, основанная на платформе Bitcoin, имела недостаточную пропускную способность сети, а сама криптовалюта имела большую популярность, что приводило к низкой скорости обработки транзакций и повышению стоимости комиссий [16-18].

Анализ мирового опыта автоматизации голосования вместе с существующими решениями и их недостатками, позволяют нам выявить схожие и особенные характеристики/критерии, следование которым свидетельствовало бы об улучшении решений и несоблюдение которых, на данный момент, является их слабой стороной:

– критерий достаточной прозрачности процесса голосования. Подсчет голосов должен осуществляться корректным образом без возможности его фальсификации.

– критерий достаточной отказоустойчивости системы голосования. Недостаточность отказоустойчивости системы, может привести к тому, что если машина, занимающаяся обработкой голосов, выйдет из строя, то это приведет к нарушению всего процесса голосования.

– критерий надежности системы голосования. Принцип построения архитектуры системы голосования должен обеспечивать отсутствие единой «точки отказа» этой системы.

На основе критериев, которые мы сформулировали и требований, которые предъявляются к любой системе голосования, определенные Федеральным законом от 12.06.2002 N 67-ФЗ (ред. От 31.07.2020) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан

Российской Федерации» все чаще к рассмотрению предлагается протокол на основе технологии blockchain, который должен их удовлетворить [5].

Технология блокчейн основной базовый компонент большинства криптовалютных сетей, так как при записи и передачи данных использует прозрачный, надежный и доказуемый метод. Являясь децентрализованной, распределённой и общедоступной цифровой бухгалтерской книгой (DLT), технология отвечает за ведение постоянной записи цепочки блоков ранее всех подтвержденных транзакций. То есть, обобщая сказанное выше, мы можем сказать, что блокчейн – цепочка блоков, каждый из которых содержит в себе информацию о серии транзакций, которые были проведены в течении определенного промежутка времени. Термин «транзакция» представляет собой вычислительный процесс, который происходит в цепочке блокчейна или, иными словами, единицы данных, которые содержат сведения о транзакции и отметке времени [6-8]. Транзакции блокчейна происходят в одноранговой сети глобально распределённых компьютеров (рис. 1) peer-to-peer (P2P), где было введено свойство отсутствие доверия, которое позволяет проверять и хранить все транзакционные данные в общедоступном блокчейне. Система без доверия означает, что пользователям не нужно знать или доверять друг другу или третьей стороне, чтобы система функционировала, так как нет единого субъекта, имеющего контроль над всей системой. То есть, каждый компьютер (узел) сети поддерживает копию блокчейна, тем самым обеспечивает ей безопасность и функционирование.

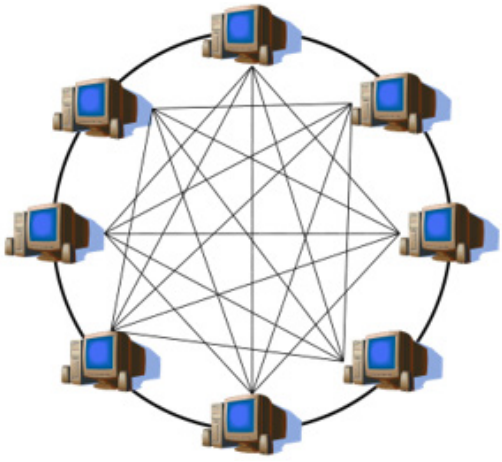

Рис. 1. Схематичное представление одноранговой сети P2P

Структура блока технологии состоит из четырех строк:

– первая строка адрес, который является публичным ключом. Он генерируется ассиметричным алгоритмом шифрования с помощью приватного ключа, который придумывает пользователь;

– вторая строка включает в себя дату и время того момента, когда был создан блок.

– третья строка содержит в себе хэш, который вычисляется с помощью хэш-функции (например, SHA256) от адреса предыдущего и суммы всех транзакций текущего блоков. Так как при вычислении хэш использует адреса предыдущего и текущего блока, его называют связующим. Именно он объединяет блоки в одну цепь;

– четвертая строка содержит само сообщение, т.е. информацию (сведения) о транзакциях. Эту строку также называют телом блока (рис. 2).

Рис. 2. Структура блока технологии blockchain

Предыдущий и последующий блоки связываются с помощью идентификатора блока (рис. 3), что позволяет сохранить надежность этой системы.

То есть, если мы не верим, что система надежна и решили внести изменения в данные одного из блоков в целях ее компрометации, то мы заметим, что идентификатор всех последующих блоков также изменится (рис. 4) и наша корректировка данных будет обнаружена и признана невалидной.

При анализе существующих систем электронного голосования в РФ с помощью применения СИБ были выявлены следующие недостатки:

– отсутствует решение по защите от одно-

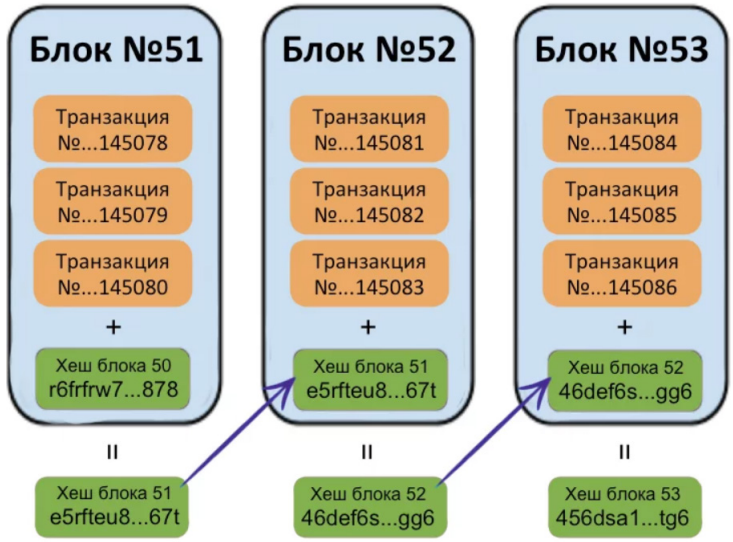

Рис. 3. Связь блоков между собой в технологии blockchain

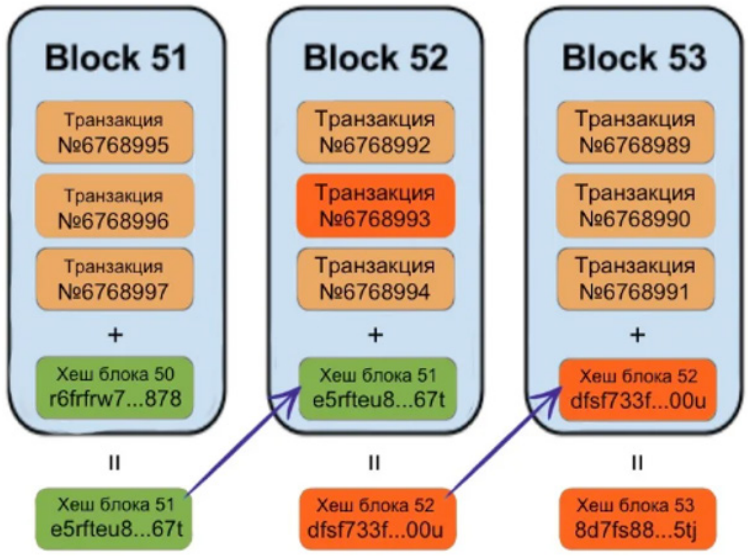

Рис. 4. Иллюстрация попытки изменения данных в блоке

временного принятия более одного бюллетеня (голоса);

– нестабильность работы оптической схемы, которая распознает информацию о голосовании.

Также, при анализе СЭГ в РФ с помощью применения КОИБ в качестве недостатков мы сформулировали следующее:

– сложность в обслуживании и высокая стоимость машин;

– невозможность проверки корректности работы оборудования для голосования независимыми экспертами.

В ходе аналитической работы был выявлен ряд целей, к которым стремиться любая система электронного голосования:

– повышение скорости подсчета голосов;

– сокращение роли человека в подсчете голосов;

– повышение доверия к результатам голосования.

Исходя из этого, была сформулирована следующая проблема: принимая во внимание обстоятельства последних двух лет и несоответствие им существующих решений избирательной системы, возникает необходимость создания безопасного и защищенного от фальсификаций метода электронного голосования на основе прогрессивных технологий.

Литература

1. Российский центр обучения избирательным технологиям при ЦИК.

2. России [Электронный ресурс]. URL: http://www.rcoit.ru/main/tech/tech/17065/.

3. Cyberleninka.ru / Электронное голосование: «За» и «Против» [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/elektronnoe-golosovanie-za-i-protiv.

4. Сапожников Д.В., Полякова Е.Н. Правовое обеспечение информационной безопасности российских телематических сетей на примере ГАС «Выборы» // Безопасность информационного пространства: сб. материалов XV Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых. Курган: Курган. гос. ун-т. 2016. С. 62–65.

5. Худолей Д. М., Худолей К. М. Электронное голосование в России и за рубежом // Вестник Пермского университета. Юридические науки. 2022. Вып. 57. С. 476–503. DOI: 10.17072/1995-4190-2022-57-476-503.

6. Lilleker D.G. Koc-Michalska K. What Drives Political Participation? Motivations and Mobilization in a Digital Age // Political Communication. 2016. Vol. 33. P. 1–23. DOI: 10.1080/10584609.2016.1225235.

7. Володенков С.В., Артамонова Ю.Д. Информационные капсулы как структурный компонент современной политической интернет-коммуникации // Вестник Томского государственного университета. Философия. Социология. Политология. 2020. № 53. С. 188–196. DOI: 10.17223/1998863X/53/20.

8. Прасти Н. Блокчейн. Разработка приложений, // Н. Прасти, В.С. Яценков. — СПб.: БХВ-Петербург, 2018. – 256 с.

9. Равал С. Децентрализованные приложения. Технология Blockchain в действии, // С. Равал. — СПб.: Питер, - 2017. - 192 с.

10. Тапскотт Д., Тапскотт А. Технология блокчейн - то, что движет финансовой революцией сегодня, // Д. Тапскотт, А. Тапскотт. — М.: Эксмо, 2017. – 448 с.

11. Насколько надежно электронное голосование [Электронный ресурс]. – Режим доступа: https://www.svoboda.org/a/269300.html, свободный.

12. Норвегия официально отказалась от электронного голосования на выборах: оно контрпродуктивно [Электронный ресурс]. – Режим доступа: http://www.mk.ru/politics/world/2014/06/30/norvegiya-otkazalasv-politike-ot-elektronnogo-golosovaniya.html, свободный.

13. Block The Vote: Could Blockchain Technology Cybersecure Elections? [Электронный ресурс]. – Режим доступа: http://www.forbes.com/sites/realspin/2016/08/30/block-the-votecouldblockchain-technology-cybersecure-elections, свободный.

14. California: The Top to Bottom Review [Электронный ресурс]. – Режим доступа: http://www.votetrustusa.org/index.php?option=com_content&task=view&id =2554&Itemid=113, свободный.

15. IGS Votomatic Prototype Goes to the Smithsonian [Электронный ресурс]. – Режим доступа: https://web.archive.org/web/20070713201451/http://www.igs.berkeley.edu/publications/par/winter2001/votomatic.htm, свободный.

16. Kiwi. Bitcoin testnet sandbox. [Электронный ресурс]. – Режим доступа: https://testnet.manu.backend.hamburg/faucet, свободный.

17. NSW election result could be challenged over iVote security flaw [Электронный ресурс]. – Режим доступа: https://www.theguardian.com/australia-news/2015/mar/23/nsw-electionresult-could-be-challenged-over-ivote-security-flaw, свободный.

18. Peer-to-peer [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf, свободный.

References

1. Rossiyskiy tsentr obucheniya izbiratel'nym tekhnologiyam pri TSIK.

2. Rossii [Elektronnyy resurs]. URL: http://www.rcoit.ru/main/tech/tech/17065/.

3. Cyberleninka.ru / Elektronnoye golosovaniye: «Za» i «Protiv» [Elektronnyy resurs]. URL: https://cyberleninka.ru/article/v/elektronnoe-golosovanie-za-i-protiv.

4. Sapozhnikov D.V., Polyakova Ye.N. Pravovoye obespecheniye informatsionnoy bezopasnosti rossiyskikh telematicheskikh setey na primere GAS «Vybory» // Bezopasnost' informatsionnogo prostranstva: sb. materialov XV Vseros. nauch.-prakt. konf. studentov, aspirantov i molodykh uchenykh. Kurgan: Kurgan. gos. un-t. 2016. S. 62–65.

5. Khudoley D. M., Khudoley K. M. Elektronnoye golosovaniye v Rossii i za rubezhom // Vestnik Permskogo universiteta. Yuridicheskiye nauki. 2022. Vyp. 57. C. 476–503. DOI: 10.17072/1995-4190-2022-57-476-503.

6. Lilleker D.G. Koc-Michalska K. What Drives Political Participation? Motivations and Mobilization in a Digital Age // Political Communication. 2016. Vol. 33. P. 1-23. DOI: 10.1080/10584609.2016.1225235.

7. Volodenkov S.V., Artamonova YU.D. Informatsionnyye kapsuly kak strukturnyy komponent sovremennoy politicheskoy internet-kommunikatsii // Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya. 2020. № 53. S. 188–196. DOI: 10.17223/1998863X/53/20.

8. Prasti N. Blokcheyn. Razrabotka prilozheniy, // N. Prasti, V.S. Yatsenkov. — SPb.: BKHV-Peterburg, 2018. – 256 s.

9. Raval S. Detsentralizovannyye prilozheniya. Tekhnologiya Blockchain v deystvii, // S. Raval. — SPb.: Piter, - 2017. - 192 s.

10. Tapskott D., Tapskott A. Tekhnologiya blokcheyn - to, chto dvizhet finansovoy revolyutsiyey segodnya, // D. Tapskott, A. Tapskott. — M.: Eksmo, 2017. – 448 s.

11. Naskol'ko nadezhno elektronnoye golosovaniye [Elektronnyy resurs]. – Rezhim dostupa: https://www.svoboda.org/a/269300.html, svobodnyy.

12. Norvegiya ofitsial'no otkazalas' ot elektronnogo golosovaniya na vyborakh: ono kontrproduktivno [Elektronnyy resurs]. – Rezhim dostupa: http://www.mk.ru/politics/world/2014/06/30/norvegiya-otkazalasv-politike-ot-elektronnogo-golosovaniya.html, svobodnyy.

13. Block The Vote: Could Blockchain Technology Cybersecure Elections? [Electronic resource]. - Access mode: http://www.forbes.com/sites/realspin/2016/08/30/block-the-votecouldblockchain-technology-cybersecure-elections, free.

14. California: The Top to Bottom Review [Electronic resource]. - Access mode: http://www.votetrustusa.org/index.php?option=com_content&task=view&id =2554&Itemid=113, free.

15. IGS Votomatic Prototype Goes to the Smithsonian [Electronic resource]. - Access mode: https://web.archive.org/web/20070713201451/http://www.igs.berkeley.edu/publications/par/winter2001/votomatic.htm, free.

16. Kiwi. Bitcoin testnet sandbox. [Electronic resource]. - Access mode: https://testnet.manu.backend.hamburg/faucet, free.

17. NSW election result could be challenged over iVote security flaw [Electronic resource]. - Access mode: https://www.theguardian.com/australia-news/2015/mar/23/nsw-electionresult-could-be-challenged-over-ivote-security-flaw, free.

18. Peer-to-peer [Electronic resource]. - Access mode: https://bitcoin.org/bitcoin.pdf, free.

КРОТОВА Елена Львовна, кандидат физико-математических наук, доцент кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

KROTOVA Elena Lvovna, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Territory, Perm, Komsomolsky prospect, 29. E-mail: lenkakrotova@yandex.ru

СУББОТИНА Юлия Владимировна, ведущий инженер кафедры «Высшая математика», аспирант кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: yulyia.urazbaeva@mail.ru

SUBBOTINA Yulia Vladimirovna, leading engineer of the Department of Higher Mathematics, postgraduate student of the Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Territory, Perm, Komsomolsky prospect, 29. E-mail: yulyia.urazbaeva@mail.ru

ЕРМАКОВ Дмитрий Германович, кандидат физико-математических наук, старший научный сотрудник отдела дифференциальных уравнений Лаборатории научно-информационных ресурсов, Федеральное государственное бюджетное учреждение науки Институт математики и механики им. Н. Н. Красовского Уральского отделения Российской академии наук (ИММ УрО РАН). 620108, г. Екатеринбург, ул. Софьи Ковалевской, д. 16.; кандидат физико-математических

наук, доцент, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. 620002, Екатеринбург, ул. Мира, 19. E-mail: Dmitry.Ermakov@mail.ru

YERMAKOV Dmitry Germanovich, PhD in Physics and Mathematics, Senior Researcher, Differential Equations Department, Laboratory of Scientific and Information Resources, Federal State Budgetary Institution of Science Institute of Mathematics and Mechanics named after N. N. Krasovsky Ural Branch of the Russian Academy of Sciences (Institute of Mathematics and Mechanics of the Ural Academy of Sciences). N. N. Krasovsky Institute of Mathematics and Mechanics of the Ural Branch of the Russian Academy of Sciences (IMM Ural Branch of the Russian Academy of Sciences), 620108, Ekaterinburg, Sofya Kovalevskaya St., 16.; candidate of Physical and Mathematical Sciences, Associate Professor, Ural Federal University named after the first President of Russia B.N.Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: Dmitry.Ermakov@mail.ru

ТИШИН Константин Львович, аспирант кафедры «Высшая математика», Пермский национальный исследовательский политехнический университет. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: konstantinlvovich777@gmail.com

TISHIN Konstantin Lvovich, postgraduate student, Department of Higher Mathematics, Perm National Research Polytechnic University. 614990, Perm Territory, Perm, Komsomolsky prospect, 29. E-mail: konstantinlvovich777@gmail.com