Методология моделирования устойчивости цифровых данных*

А. В. Соловьев[I], Н. Б. Баканова[II]

[I] Федеральное государственное учреждение «Федеральный исследовательский центр "Информатика и управление" Российской академии наук», г. Москва, Россия
[II] Федеральный Исследовательский Центр Институт Прикладной Математики им. М. В. Келдыша Российской Академии Наук, г. Москва, Россия

Аннотация. В статье предложена методология моделирования устойчивости цифровых данных к дестабилизирующим воздействиям в процессе долговременного хранения. Приведена постановка проблемы, дан обзор проблем обеспечения устойчивости к дестабилизирующим воздействиям, показана связь выявленных проблем между собой. Сделан вывод о необходимости комплексного решения выявленных проблем с помощью предложенной методологии. Приведены основные положения методологии, ограничения и допущения при ее реализации и возможные области ее применения. Определены сферы дальнейших исследований по разработке методологического и алгоритмического аппарата моделирования устойчивости цифровых данных.

Ключевые слова: цифровые данные, долговременное хранение, устойчивость, дестабилизирующие воздействия, цифровизация.

DOI 10.14357/20718632210207

Введение

При долговременном хранении цифровых данных необходимо принимать дополнительные технические и организационные меры для решения проблем сохранности, аутентичности и интерпретируемости данных и носителей информации [1]. Это приводит к необходимости создания технологии долговременного хранения цифровых данных в условиях параметрических возмущений среды хранения [2]. При этом информационная избыточность цифровых данных возрастает пропорционально их важности и величине сроков хранения [3].

Если важность (ценность) цифровых данных оценивается как достаточно высокая (сама оценка ценности выходит за рамки данного исследования), то при долговременном хранении таких данных необходимо продумывать решения, позволяющие не только обеспечить безопасность хранения, в смысле защиты от несанкционированного доступа, надежность хранения, в смысле обеспечения бесперебойности работы программных и технических средств [4], но и обеспечивать сохранность цифровых данных при возможном дестабилизирующем воздействии, в том числе и катастрофического характера. То есть, возникает

* Работа выполнена при частичной финансовой поддержке РФФИ в рамках научных проектов № 18-29-03070 и № 18-29-03085.

необходимость обеспечения сохранности важных цифровых данных при природных, техногенных, антропогенных или иных воздействиях, которые приводят:

- к массовому выходу из строя программно-технических средств (ПТС),
- невозможности использовать запасные части, инструменты и приспособления (ЗИП),
- к полной потере информации.

В данной статье приведены разработанные авторами рекомендации по созданию методологического и алгоритмического аппарата моделирования и оценки устойчивости цифровых данных к дестабилизирующим воздействиям, а также по повышению уровня защиты данных от дестабилизирующих воздействий. Выделены проблемы и возможные пути их решения, которые могут помочь разработчикам программно-технического обеспечения для долговременной сохранности цифровых данных.

1. Краткий обзор проблем обеспечения устойчивости к дестабилизирующим воздействиям

Приведем основные понятия и определения, используемые в данной статье.

Под устойчивостью цифровых данных к дестабилизирующим воздействиям будем понимать способность к восстановлению за минимальный период времени как самих данных, так и работоспособности приложений, ответственных за интерпретацию этих данных, а также работоспособности иных программных сред (например, операционных систем) и технических средств, без которых использование цифровых данных не представляется возможным.

Технические и программные средства включены в понятие устойчивости не случайно, а в связи с тем, что без необходимых средств интерпретации данных, программных сред функционирования этих средств, а также соответствующих технических средств, невозможно воспользоваться самими цифровыми данными.

Под дестабилизирующими подразумевается не только воздействиями катастрофического характера (пожар, наводнение и т.п.) но и возможные непредвиденные сбои в работе служб, разрушение данных или повреждение всего центра обработки в результате разных причин (повреждение телекоммуникационных линий, несанкционированный доступ к данным, диверсия, саботаж, халатность, другие проявления человеческого фактора – ЧФ).

Если отказоустойчивая (надежная) программно-техническая система долговременного хранения должна быть способной сохранять работоспособность в случае выхода из строя отдельных узлов и компонентов системы, то устойчивая к дестабилизирующим воздействиям должна оставаться работоспособной в случае одновременного множественного выхода из строя ее составных частей или узлов в результате действий непредвиденного характера.

В настоящее время проблема обеспечения устойчивости цифровых данных осложняется стремительной цифровизацией экономики, т.е. возникновения огромных объемов цифровых данных, предназначенных для долговременного хранения, за относительно короткий промежуток времени. Безусловная ценность таких данных определяет необходимость создания механизмов, позволяющих оперативно моделировать и проводить оценку устойчивости таких данных при воздействии различных дестабилизирующих факторов и меры противодействия им.

Данная проблема порождает следующую проблему, а именно, отсутствие общепринятого математического и алгоритмического аппарата, позволяющего выполнить оценку устойчивости системы к дестабилизирующим воздействиям. Обычно при ее оценке применяют стандартные механизмы резервирования, основанные на оценке степени или коэффициента доступности [5-7], рассчитываемого по вероятностной модели.

Однако вероятность реализации дестабилизирующего воздействия, особенно катастрофического характера, оценить бывает крайне трудно, а иногда и бессмысленно, т.к. вероятность наступления события может быть сколь угодно малой. Такая вероятность незначительно скажется на общем показателе устойчивости и может привести к неверной оценке.

Следующей проблемой является возможность уничтожения цифровых данных при исправности технических и программных средств

вследствие умышленного действия, ошибки или халатности. При хранении «нецифровых» данных обычно применяются меры, способные противодействовать дестабилизирующим воздействиям (противопожарные, охранные и т.д.). В каком-то смысле бумажный документ сложнее уничтожить, в отличие от цифровых данных, которые можно просто «стереть». Однако у цифровых данных может быть реализовано преимущество географически разделенных мест хранения, что снижает риск полного уничтожения данных. Кроме того, цифровые данные могут быть защищены сложной системой прав доступа, протоколов действий пользователей и других организационных мероприятий. Все эти меры реализуемы в современных программно-технических системах. Однако они порождают следующую проблему: возникновение неконтролируемой избыточности данных при долговременном хранении.

Как было показано в предыдущих статьях автора (например, [2; 3]), избыточность данных при долговременном хранении, например, для обеспечения интерпретируемости (читаемости), аутентичности (неизменности), надежности хранения неизбежна. Важно, чтобы избыточность была контролируемой, и, что немаловажно, чтобы накопленные избыточные данные также позволили гарантировать их аутентичность и интерпретируемость через годы и десятилетия [1].

В свою очередь, неконтролируемая избыточность данных может породить следующую проблему: появление измененных данных в одной из копий при отсутствии «мастер»-копии данных. Действительно, допустим, мы храним цифровые данные в нескольких копиях, все они являются равноправными с точки зрения аутентичности и интерпретируемости. Если в какой-то момент времени окажется, что они различные, как восстановить оригинал и подтвердить его аутентичность? Наличие «мастер»-копии не всегда гарантирует долговременную сохранность, т.к. обслуживающий персонал имеет возможность подменить и ее, например, вследствие административного воздействия.

Тем самым, можно заключить, что общая проблема контроля избыточности данных заключается в том, что достаточно сложно продумать разумную избыточность при долговременном хранении данных. Таким образом, обеспечение долговременной сохранности и устойчивости к дестабилизирующим факторам сводится к необходимости постоянного оценивания рисков возникновения различных дестабилизирующих воздействий, в том числе и катастрофического характера. Т.е. необходимо своевременно выявлять изменение рисков и тем самым корректировать модели дестабилизирующих факторов, проводить оценку рисков в течение срока хранения цифровых данных, обеспечивать выбор и проведение контрмер для нейтрализации или минимизации последствий дестабилизирующих воздействий. Без продуманной избыточности при поддержании работоспособности процесс долговременного хранения, и без того дорогого, может быть крайне затратным из-за необходимого программно-аппаратного решения.

Можно утверждать, что решением перечисленных проблем должна быть методология, позволяющая разрабатывать математические модели устойчивости программно-технических решений обеспечения долговременной сохранности в течение всего срока их эксплуатации. Т.е. необходимо постоянное в течении всего срока хранения моделирование устойчивости, включая составление и корректировку моделей дестабилизирующих факторов и применяемых контрмер. Только так, по мнению авторов, может быть обеспечена устойчивость, а, следовательно, и сохранность цифровых данных. Ниже мы приводим основные положения разработанной методологии, а также допущения и ограничения при ее реализации для конкретных программно-технических решений.

2. Основные положения методологии моделирования устойчивости цифровых данных

Безусловно, основные положения данной методологии должны быть тесно связаны с общим подходом, на котором основано проектирование программно-технических решений по обеспечению долговременной сохранности цифровых данных. Создание и моделирование мер противодействия дестабилизирующим воз-

действиям должно выполняться вместе с проектированием программно-технических решений по обеспечению долговременной сохранности (ПТРОДС).

Ниже под элементами ПТРОДС будем понимать центры обработки данных (ЦОД), состоящие из различных ПТС, а также оборудование и каналы связи (ОКС). Под узлами ПТРОДС будем понимать конкретное оборудование, входящее в ЦОД и ОКС. Характеристики ПТС, ОКС, ЦОД, описания возможных дестабилизирующих воздействий должны храниться в отдельной базе данных (БД), которая является основой для моделирования дестабилизирующих воздействий и мер противодействия им (контрмер).

Положение № 1. В основе моделирования устойчивости к дестабилизирующим воздействиям должен лежать принцип моделирования основного технологического цикла работы ПТРОДС при воздействии на ПТРОДС дестабилизирующих факторов. Движение информационных потоков должно моделироваться с учетом этих факторов (разного рода отказы оборудования, в т.ч. элементов ЦОД, умышленный ущерб, человеческий фактора [10]). Характеристики дестабилизирующих факторов (ДФ), а также сценарии развития дестабилизирующих воздействий должны задаваться отдельными параметрическими моделями и храниться в отдельной БД.

Результатом моделирования должно быть вычисление показателей устойчивости к дестабилизирующим воздействиям, надежности и эффективности работы [4] ПТРОДС, а также качественные выводы о готовности ПТРОДС к выполнению своих функций при развитии заданных дестабилизирующих воздействий с анализом причин нарушения устойчивости системы на основе полученной информации.

В отдельной БД должна накапливаться и храниться «история» развития реальных проблем, возникавших при эксплуатации системы. Это необходимо для построения модели ретроспективного анализа развития дестабилизирующих воздействий и оценки эффективности контрмер [11]).

Положение № 2. При моделировании устойчивости к дестабилизирующим воздействиям должен применяться сценарный подход анализа («что, если...») и прогнозирования поведения ПТРОДС с учетом влияния дестабилизирующих факторов (ДФ).

Моделирование поведения ПТРОДС должно производиться, исходя из предположения, что дестабилизирующее воздействие состоялось. Необходимо смоделировать состояние ПТРОДС, движение информационных потоков, влияние отказа элемента на поведение ПТРОДС с учетом времени восстановления элемента. Сценарий развития дестабилизирующих воздействий, степень влияния ДФ на ПТРОДС должны задаваться отдельными параметрическими моделями, в которых параметрами выступают степень воздействия, вероятность возникновения, наличие средств противодействия дестабилизирующим воздействиям.

Как было сказано выше, вероятность возникновения наводнения или землетрясения оценить бывает крайне трудно, а иногда и бессмысленно. Вместо этого должны проводиться оценки вероятности выполнения мер по восстановлению работоспособности ПТРОДС после того, как произошло предполагаемое воздействие на ПТРОДС.

Положение № 3. При оценке состояния и степени готовности ПТРОДС к выполнению своих функций должно применяться ретроспективное моделирование поведения ПТРОДС. При оценке состояния ПТРОДС, а также оценке риска возникновения аварийной или критической ситуации должен использоваться анализ истории отказов ее элементов и вариантов разрешения проблем (восстановления) с оценкой эффективности примененных контрмер. Моделирование отказов элементов ПТРОДС должно производиться также и по случайному закону распределения отказов в ее элементах, как это делается при оценке надежности системы [4]).

Хранение «истории отказов» безусловно вносит существенную избыточность в ПТРОДС, однако это единственный способ знать, что происходило с системой много лет назад, особенно в условиях, когда обслуживающий персонал ПТРОДС за это время сменился и имеет навык применения контрмер, осуществленных в прошлом.

Положение № 4. Модель устойчивости ПТРОДС к дестабилизирующим воздействиям должна быть расширяемой и предусматривать:

• ввод новых моделей ДФ, их характеристик и функций воздействия на ПТРОДС,

• обработку новых статистических данных по «истории» отказов и изменению конфигурации ЦОД, ОКС, отдельных ПТС. Это важно, т.к. технические и программные средства могут модернизироваться или меняться в процессе долговременного хранения.

Положение № 5. Модель устойчивости ПТРОДС к дестабилизирующим воздействиям должна обладать свойством непротиворечивости, т.е. должна соблюдаться непротиворечивость принципам функционирования ПТРОДС и проводимым контрмерам.

3. Ограничения и допущения методологии моделирования устойчивости

При реализации методологии оценки и моделирования устойчивости цифровых данных к дестабилизирующим воздействиям в конкретных разрабатываемых или эксплуатируемых ПТРОДС могут быть приняты следующие допущения:

• все последствия дестабилизирующих воздействий на ПТРОДС по причинению ущерба адекватны первопричине (например, пожар, вызванный землетрясением или ураганом и т. п.), поэтому при моделировании устойчивости принимается во внимание только первопричина;

• система обеспечения устойчивости ПТРОДС проектируется таким образом, что резервные объекты (если таковые имеются), которым переданы функции ЦОД или иных элементов ПТРОДС, попавших под дестабилизирующее воздействие, выполнят поставленную перед ними задачу;

• риски возникновения и развития дестабилизирующих воздействий могут быть по последствиям оценены так, что передача функций резервным объектам обязательна, независимо от того, что ущерб от дестабилизирующих воздействий может быть меньше, чем спрогнозирован;

• восстановление функционирования элементов ПТРОДС с заданным уровнем доверительной вероятности (обеспечение достоверности, полноты и своевременности выполнения функций ПТРОДС) проводится за время, не превышающее заданное.

Заключение

Общая тенденция стремительной цифровизации в мире говорит о том, что в ближайшее время объем цифровых данных, в том числе предназначенных для долговременного хранения, станет стремительно возрастить. Тем самым подходы к их безопасному хранению должны быть выработаны уже сейчас. При длительных сроках хранения тем более должна быть обеспечена устойчивость цифровых данных к дестабилизирующим воздействиям, т. к. в условиях цифровизации цифровые данные становятся ключевым фактором цифрового производства и тем самым представляют большую ценность.

Для создания программно-технических решений обеспечения долговременной сохранности, функционирование которых связано с хранением ценных и особо ценных цифровых данных, необходимо уделять большое внимание степени защищенности от дестабилизирующих воздействий не только природного, но и техногенного, и антропогенного характера.

Многими современными исследователями признано, что основные проблемы создания, эксплуатации и внедрения информационных технологий в организациях сопряжены с влиянием человеческого фактора [10; 12]. Более того, можно утверждать, что отсутствие оценки влияния этого фактора при проведении работ по анализу надежности, эффективности, безопасности и устойчивости информационных систем, снижает точность получаемого результата. Это означает, что система обеспечения устойчивости цифровых данных должна быть всесторонне продумана, чтобы избежать неучтенных рисков с одной стороны и неоправданных затрат с другой.

Как результат проведенных авторами исследований, в статье предложена методология моделирования устойчивости цифровых данных. Показана необходимость разработки моделей устойчивости цифровых данных, проверки и совершенствования моделей, тщательного исследования результатов моделирования, постоянного мониторинга устойчивости цифровых данных на основе созданных моделей.

Предлагаемая в статье методология может применяться не только к решениям по долго-

временному хранению цифровых данных, но и к решению проблем устойчивости широкого класса информационных систем. Предложенный подход предполагает избыточность цифровых данных и дополнительные временные затраты, однако, по мнению авторов, это необходимо и оправдано для обеспечения сохранности ценных цифровых данных.

В дальнейших исследованиях авторы планируют разработать алгоритмический аппарат решения проблемы устойчивости цифровых данных, а также методологию разработки математических моделей устойчивости.

Литература

1. Баканова, Н. Б., Соловьев, А. В. Проблемы долговременной сохранности больших данных // Информационные технологии и вычислительные системы. 2019. № 2. С. 44–53. doi: 10.14357/2071863219020.
2. Solovyev, A. V. Long-Term Digital Documents Storage Technology // Lecture Notes in Electrical Engineering. 2020. Vol. 641, pp. 901–911. ISSN 1876-1100. doi: 10.1007/978-3-030-39225-3_97.
3. Соловьев, А. В. Электронные архивы: разработка математической модели электронного документа при долговременном хранении // Информационные технологии и вычислительные системы. 2017. № 1. С. 46–61.
4. Акимова, Г. П., Соловьев, А. В., Тарханов, И. А. Моделирование надежности распределённых информационных систем // Информационные технологии и вычислительные системы. 2019. № 3. С. 79–86. doi: 10.14357/20718632190307.
5. Taylor, Z. and Ranganathan, S. Designing High Availability Systems: DFSS and Classical Reliability Techniques with Practical Real Life Examples. — Wiley, 2013. — 480 p. — ISBN: 9781118739839.
6. Schmidt, K. High Availability and Disaster Recovery: Concepts, Design, Implementation. — Springer, 2006. — 422 p. — ISBN: 9783540345824.
7. Будзко, В. И., Мельников, Д. А., Фомичев, В. М. Основы организации обеспечения информационной безопасности и киберустойчивости в централизованных информационно-телекоммуникационных системах высокой доступности // Системы высокой доступности. 2019. Том 15. № 1. С. 70–77.
8. Casti, J. 1979. Connectivity, complexity, and catastrophe in large-scale systems. Chichester etc. International Institute for Applied Systems Analysis. 220 p. ISBN 0 471 27661.
9. Poston, T., Stewart I. 1978. Catastrophe theory and its applications. Surveys and Reference Works in Mathematics, Pitman, London. 491 p.
10. Solovyev, A. V. Human Reliability Assessment in Control Systems // Lecture Notes in Electrical Engineering. 2021. Vol. 729, pp. 1–10. doi: 10.1007/978-3-030-71119-1_62.
11. Акимова, Г. П., Пашкина, Е. В., Соловьев, А. В. Ситуационно-аналитические центры, как способ снижения влияния человеческого фактора на принятие управленческих решений при эксплуатации больших информационных систем // Труды ИСА РАН. 2007. Т. 29. С.113–122.
12. Devyatkin D. A., Grigoriev O. G., Sochenkov I. V., Tikhomirov I. A., Zubarev D. V. Expert Assignment Method Based on Similar Document Retrieval // Data Analytics and Management in Data Intensive Domains: XXI In-ternational Conference DAMDID/RCDL'2019 (October 15–18, 2019, Kazan, Russia). Conference Proceedings. Edited by Alexander Elizarov, Boris Novikov, Sergey Stupnikov. Kazan: Kazan Federal University, 2019, pp. 339–351.

Соловьев Александр Владимирович, Федеральное государственное учреждение «Федеральный исследовательский центр "Информатика и управление" Российской академии наук», г. Москва, Россия. Главный научный сотрудник, доктор технических наук. Количество печатных работ: 125. Область научных интересов: системный анализ, системы управления базами данных, теория надежности, математическое моделирование, долговременное хранение электронных документов. E-mail: soloviev@isa.ru

Баканова Нина Борисовна, Институт Прикладной Математики им. М.В. Келдыша Российской Академии Наук», г. Москва, Россия. Зав. сектором, доктор технических наук. Количество печатных работ: 60. Область научных интересов: системный анализ, управление и обработка информации, проектирование информационных систем, поддержка принятия решений, проблемно-ориентированные системы, экспертные системы. E-mail: nina@keldysh.ru

Methodology for Modeling the Stability of Digital Data

A. V. Solovyev[I], N. B. Bakanova[II]

[I] Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia
[II] M.V. Keldysh, Institute of Applied Mathematics of the Russian Academy of Sciences, Moscow, Russia

Abstract. The article proposes a methodology for modeling the stability of digital data to destabilizing effects in the process of long-term keeping. The stability of digital data to destabilizing influences in the article is understood as the ability to recover in a minimum period of time both the data itself and the operability of applications responsible for the interpretation of this data, as well as the operability of other software and hardware, without which the use of digital data is not possible. This article provides a statement of the problem of stability of digital data. A review of the problems of ensuring resistance to destabilizing influences is carried out, the relationship between the identified problems is shown. It is concluded that it is necessary to comprehensively solve the identified problems by developing a methodology for modeling sustainability. The main result of the research is the proposed methodology for modeling the stability of digital data. The main provisions of the methodology, as well as limitations and assumptions in its implementation are given in the article. In conclusion, it is concluded that it is necessary to model sustainability in the context of rapid digitalization. Possible areas of application of the proposed methodology are given. The areas for further research on the development of methodological and algorithmic apparatus for modeling the stability of digital data are identified.

Keywords: digital data, long-term keeping, sustainability, destabilizing impacts, digitalization.

DOI 10.14357/20718632210207

References

1. Bakanova, N. B., and Solovyev, A. V. 2019. Problemy dolgovremennoy sokhrannosti bol'shikh dannykh [Problems of long-term keeping of big data] // Informatsionnyye tekhnologii i vychislitel'nyye sistemy [Information Technology and Computing Systems]. 2: 44–53. doi: 10.14357/2071863219020.
2. Solovyev, A. V. 2020. Long-Term Digital Documents Storage Technology // Lecture Notes in Electrical Engineering. 641: 901–911. doi: 10.1007/978-3-030-39225-3_97.
3. Solovyev, A. V. 2017. Elektronnyye arkhivy: razrabotka matematicheskoy modeli elektronnogo dokumenta pri dolgovremennom khranenii [Electronic archives: development of mathematical models of electronic documents for long-term storage] // Informatsionnyye tekhnologii i vychislitel'nyye sistemy [Information Technology and Computing Systems]. 1: 46–61.
4. Akimova, G. P., Solovyev, A. V., and Tarkhanov, I. A. 2019. Modelirovaniye nadezhnosti raspredelonnykh informatsionnykh sistem [Modeling the reliability of distributed information systems] // Informatsionnyye tekhnologii i vychislitel'nyye sistemy [Information Technology and Computing Systems]. 3: 79–86. doi: 10.14357/20718632190307.
5. Taylor, Z. and Ranganathan, S. 2013. Designing High Availability Systems: DFSS and Classical Reliability Techniques with Practical Real Life Examples. Wiley. 480 p. ISBN: 9781118739839.
6. Schmidt, K. 2006. High Availability and Disaster Recovery: Concepts, Design, Implementation. Springer. 422 p. ISBN: 9783540345824.
7. Budzko, V. I., Melnikov, D. A., and Fomichev, V. M. 2019. Osnovy organizatsii obespecheniya informatsionnoy bezopasnosti i kiberustoychivosti v tsentralizovannykh informatsionno-telekommunikatsionnykh sistemakh vysokoy dostupnosti [The information security and cyber resilience managing basics in the centralized information telecommunication systems of high availability] // Sistemy vysokoy dostupnosti [High availability systems]. 15(1): 70–77.
8. Casti, J. 1979. Connectivity, complexity, and catastrophe in large-scale systems. Chichester etc. International Institute for Applied Systems Analysis. 220 p. ISBN 0 471 27661.
9. Poston, T., Stewart I. 1978. Catastrophe theory and its applications. Surveys and Reference Works in Mathematics, Pitman, London. 491 p.
10. Solovyev, A. V. 2021. Human Reliability Assessment in Control Systems // Lecture Notes in Electrical Engineering. 729. doi: 10.1007/978-3-030-71119-1_62.
11. Akimova, G. P., Pashkina, E. V., and Solovyev, A. V. 2007. Situatsionno-analiticheskiye tsentry, kak sposob snizheniya vliyaniya chelovecheskogo faktora na prinyatiye upravlencheskikh resheniy pri ekspluatatsii bol'shikh informatsionnykh sistem [Situational analytical centers as

a way to reduce the influence of the human factor on managerial decision-making in the operation of large information systems] // Trudy ISA RAN [Proceedings of the ISA RAS]. 29: 113–122.

12. Devyatkin D. A., Grigoriev O. G., Sochenkov I. V., Tikhomirov I. A., Zubarev D. V. 2019. Expert Assignment Method Based on Similar Document Retrieval // Data Analytics and Management in Data Intensive Domains: XXI In-ternational Conference DAMDID/RCDL'2019 (October 15–18, 2019, Kazan, Russia). Conference Proceedings: 339–351.

Solovyev A.V. Chief Researcher, Doctor of Technical Sciences. Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia. E-mail: soloviev@isa.ru

Bakanova N.B. Head of sector, Doctor of Technical Sciences. M.V. Keldysh, Institute of Applied Mathematics of the Russian Academy of Sciences, 4 Miusskaya Square, Moscow, 125047, Russia. E-mail: nina@keldysh.ru