Выходит с 2006 г.

СИСТЕМЫ ВЫСОКОЙ ДОСТУПНОСТИ

№ 2, т. 14, 2018

Highly available systems

Журнал включен в перечень ВАК

Главный редактор — академик Академии криптографии Российской Федерации **В. И. Будзко**

Редакционная коллегия:

Л.П. Андрианова, чл.-корр. РАН В.Л. Арлазаров, д.ф.-м.н. А.П. Баранов, к.т.н. В.Г. Беленков, д.т.н. В.Н. Захаров, д.т.н., проф. П.Д. Зегжда, д.т.н., проф. Л.А. Калиниченко, д.т.н., проф. Б.Н. Оныкий, д.т.н. М.Ю. Сенаторов, д.т.н., проф. И.Н. Синицын (зам. гл. редактора), акад. РАН И.А. Соколов, к.ф.-м.н. Г.К. Столяров (Беларусь), д.ф.-м.н., проф. В.М. Фомичев, д.т.н. А.В. Шмид, Di Walter H. Mayer (Австрия)

Editor-in-Chief – Academicion of Russian Federation Cryptography Academy **V.I. Budzko**

Editorial Board:

L.P. Andrianova, Corresponding Member RAS V.A. Arlazarov, Dr.Sc. (Phys.-Math.) A.P. Baranov, Ph.D. (Eng.) V.G. Belenkov, Dr.Sc. (Phys.-Math.), Prof. V.M. Fomichev, Dr.Sc. (Eng.) Prof. L.A. Kalinichenko, Dr.Sc. (Eng.), Prof. B.N. Onykii, Dr.Sc. (Eng.) M.Yu. Senatorov, Ph.D. (Eng.) A.V. Shmid, Dr.Sc. (Eng.), Prof. I.N. Sinitsyn (Deputy Editor), Academician RAS I.A. Sokolov, Ph.D. (Phys.-Math.) G.K. Stolyarov (Belarus), Dr.Sc. (Eng.) V.N. Zakharov, Dr.Sc. (Eng.), Prof. P.D. Zegzhda, Dr.Sc. (Eng.) Walter H. Mayer (Austria)

Журнал издается под научно-методическим руководством Федерального исследовательского центра «Информатика и управление» Российской академии наук.

СОДЕРЖАНИЕ

CONTENTS

Все статьи, представленные в данном выпуске журнала, соответствуют номенклатуре специальностей научных работников (Приказ Минобрнауки РФ от 11.08.2009 № 294) по отраслям технических наук.

Journal «Sistemy' vy'sokoj dostupnosti» («Highly available systems»).
The journal covers scientific and engineering problems of ensuring confidentiality, availability, and integrity for the class of information-telecommunication systems of high availability (HA ITS), which contain such critical technologies of development

Необходимую информацию о журнале и полный список опубликованных статей, а также аннотации к ним Вы найдете на нашем сайте http://www.radiotec.ru

Учредитель: ООО «Издательство «Радиотехника».

Лицензия № 065229. Свидетельства о регистрации ПИ № ФС 77-25037 от 12 июля 2006 г.
Сдано в набор 06.02.2018 г. Подписано в печать 06.03.2018 г.
Печ. л. 9,5. Тираж 400 экз. Изд. № 115.
Адрес Издательства «Радиотехника»: 107031, Москва, К-31, Кузнецкий мост, д. 20/6. Тел./факс 621-4837.
E-mail: info@radiotec.ru
http: // www. radiotec.ru /

Дизайн и допечатная подготовка ООО «САЙНС-ПРЕСС».
Отпечатано с предоставленных готовых файлов в полиграфическом центре ФГУП Издательство «Известия».
127254, ул. Добролюбова, д. 6. Контактный телефон (495) 650-38-80. izv-udprf.ru. Заказ №.

ISSN 2072-9472

© ООО «Издательство «Радиотехника», 2018 г.

Незаконное тиражирование и перевод статей, включенных в журнал, в электронном и любом другом виде запрещено и карается административной и уголовной ответственностью по закону РФ «Об авторском праве и смежных правах»

УДК 004.031.42; 004.415.2; 004.056

Об одном подходе к организации систем электронного документооборота

© Авторы, 2018
© ООО «Издательство «Радиотехника», 2018

Г.П. Акимова – к.т.н., вед. науч. сотрудник, Институт системного анализа ФИЦ ИУ РАН (Москва)
E-mail: akimova@isa.ru
А.Ю. Даниленко – к.ф.-м.н., вед. программист, Институт системного анализа ФИЦ ИУ РАН (Москва)
E-mail: pashkina@isa.ru
Е.В. Пашкина – науч. сотрудник, Институт системного анализа ФИЦ ИУ РАН (Москва)
E-mail: pashkin@isa.ru
М.А. Пашкин – науч. сотрудник, Институт системного анализа ФИЦ ИУ РАН (Москва)
E-mail: pashkin@isa.ru
А.А. Подрабинович – вед. программист, Институт системного анализа ФИЦ ИУ РАН (Москва)
E-mail: podrabinovich@isa.ru
И.В. Туманова – вед. программист, Институт системного анализа ФИЦ ИУ РАН (Москва)
E-mail: tumanova-irin@mail.ru

Предложен подход к созданию систем электронного документооборота (СЭД), основанный на управлении деловыми процессами, а не документами. Рассмотрены технологические и функциональные особенности таких систем, сделан вывод о необходимости поддержки бумажного документооборота на всех этапах внедрения и эксплуатации СЭД. Описан подход к формированию требований по обеспечению информационной безопасности для технологии блокчейн.

Ключевые слова: *электронный документооборот, блокчейн, информационная безопасность.*

The article proposes an approach to the creation of electronic document management systems (EDS), based on the management of business processes, rather than documents. The technological and functional features of such systems are considered, the conclusion is made about the need to support paper workflow at all stages of the implementation and operation of the EDS. An approach to the formation of information security requirements for blockchain technology is proposed.

Keywords: *electronic document management, blockchain, information security.*

В последние годы наметилась тенденция к росту использования электронных средств обмена данными в государственных органах, в том числе с применением систем электронного документооборота (СЭД). В первую очередь, это вызвано темпами развития информационных технологий и скоростью передачи данных, что, порой, играет решающую роль при принятии решений. Немаловажную роль в этом росте играет поддержка руководства страны, в частности, принятие документа «Положение о системе межведомственного электронного документооборота»: «МЭДО представляет собой систему федерального масштаба. Она нацелена на организацию взаимодействия систем электронного документооборота между различными ведомствами, которыми являются государственные организации, органы государственной власти РФ всех уровней, как федеральные, так и региональные. Взаимодействие между СЭД осуществляется путем обмена сообщениями и уведомлениями, а также электронными документами» [9].

Однако не менее активно развиваются и технологии перехвата информации, учащаются попытки взлома не только компьютеров, но и хранящихся на них баз данных, электронной почты. Как следствие, среди организаций растет интерес не просто к системам, обрабатывающим получаемую корреспонденцию, а к защищенным системам, в которых имеются средства защиты информации, достаточные для обеспечения информационной безопасности электронных документов. Такие информационные системы корректно работают совместно со стандартными средствами защиты информации из состава операционных систем, СУБД и аппаратного обеспечения, а также имеют собственные средства защиты данных.

Актуальность проводимой работы также подтверждается тем, что в настоящее время по данным ФСТЭК [1] имеется только пять систем класса СЭД, прошедших сертификацию для работы с конфиденциальной информацией, включая персональные данные. Из них всего одна СЭД, сертифицированная на работу со сведениями, составляющими государственную тайну, – это «ИВК БюрократЪ™». Такая статистика, в частности, означает, что в большинстве случаев СЭД не могут применяться для работы с документами, содержащими сведения, составляющие государственную тайну, хотя документы этой кате-

гории представляют более 90% процентов всего документооборота специальных служб и министерства обороны, более 30% всего документооборота силовых ведомств и не менее 15% всего документооборота остальных государственных структур, госкорпораций и крупных коммерческих компаний.

Цель работы – рассмотреть нетипичный подход к организации системы электронного документооборота как такового и использованию средств защиты данных, в частности.

Традиционная организация электронного документооборота

Понятие электронного документа при всей своей интуитивной очевидности до сих пор не формализовано на законодательном уровне. Если опираться на moreq2 [2], то электронным документом называется то, что обычно называют файлами, то есть любая информация в электронном виде. Также вводится понятие метаданных как «данных, описывающих контекст, содержание (контент) и структуру документов, а также управление документами во времени». В СЭД, ориентированных на отечественные стандарты делопроизводства [3−5], принято рассматривать электронный документ как совокупность регистрационной карточки (РК) (содержит регистрационную информацию, состав которой и правила формирования определяются инструкциями по делопроизводству) и присоединенных файлов, также содержащих любую информацию в электронном виде. При некоторых условиях РК может считаться аналогом метаданных, однако понятие метаданных значительно шире. В общем случае набор информации, удовлетворяющий приведенному выше определению, содержится не только в РК, но и других файлах, а также записях в базах данных, системных журналах, протоколах работы с документами и конкретных пользователей.

Согласно [2], «СЭД в первую очередь представляет собой программное приложение для управления электронными документами». Также можно сказать, что СЭД – это любая автоматизированная информационная система (АИС), в которой есть движение документов и совместная работа с ними [6].

Сегодня деятельность разработчиков СЭД практически не регулируется. Развивая программные продукты и реализуя проекты по внедрению, разработчики и поставщики в той или иной степени ориентируются на нормативные документы следующих категорий:

документы, регулирующие бумажный документооборот, например, [5, 7];

документы, регулирующие обработку информации в электронном виде [8, 9];

нормативные документы, определяющие порядок обработки информации определенных категорий, в частности, [10−13];

документы общеюридического плана, регулирующие основные отношения в обществе и государстве [14, 15].

Не удивительно, что в такой ситуации не существует типовых СЭД, подходящих для всех организаций. На рынке присутствуют платформенные решения, на основе которых реализуются системы для конкретных заказчиков, в качестве примеров такого подхода приведем [16−18]. В частности, в рамках МЭДО [9] предусмотрен только обмен сообщениями, содержащими документы для согласования, утверждения или ознакомления. Никаких действий, связанных с контролем исполнения или маршрутизацией движения документов, в рамках этой системы не предполагается.

Предлагаемый подход к логике работы с системой

В первую очередь, предлагается перенести акцент при работе с СЭД с РК документа на сам документ. В настоящее время, руководствуясь имеющейся технологией работы с бумажными документами, все основные операции в электронных системах производятся с РК, которые передаются вместе с электронными документами: в них фиксируются все проводимые действия с документом, при просмотре его в системе в первую очередь показывается карточка, поиск документов производится, в основном, по значениям его реквизитов, которые являются составной частью РК, и т.д. При этом как бы принижается роль самого документа, который на самом деле явился причиной появления его РК.

Предлагается в СЭД вернуть документу его значимость и при выполнении операции просмотра в первую очередь показывать именно текст документа, а не его РК. Безусловно, данная модернизация должна иметь статус настраиваемой, поскольку имеются объективные ситуации, когда не всем сотрудникам разрешено просматривать текст документа. В этом случае следует использовать обычную технологию просмотра информации о документе.

Вторым важным моментом является переход от управления документами к управлению бизнес-процессами (сходный подход применяется в некоторых СЭД, например, [19]). При таком подходе возможна реализация процесса без документа, с одной стороны, и появление документа или проекта документа в виде приложенного файла в процессе его исполнения, с другой. В ходе выполнения бизнес-процесса могут возникать новые маршруты движения документов, появляться новые задачи, но бизнес-процесс при этом останется первичным. Помимо расширения логики работы, связанной с обработкой документов, добавляется возможность управления заданиями, созданными в рамках бизнес-процесса и не обязательно привязанными к конкретному документу. Такой подход, однако, не исключает использование привычной технологии работы, когда в первую очередь в системе регистрируется документ (заводится его РК), а затем с ним выполняются обычные действия.

Подключение возможности в рамках системы обмениваться мгновенными сообщениями позволит обеспечить быстрый обмен текстовой информацией между пользователями. При этом правила обмена информацией должны соответствовать правилам, используемым в СЭД, то есть в сообщении может содержаться информация разного уровня конфиденциальности в соответствии с правами доступа данного пользователя.

Для решения задачи работы с информацией различной степени конфиденциальности, в том числе секретными сведениями, предлагается провести сегментацию программного обеспечения системы, а именно: выделение фрагментов, реализующих деловую логику, и отделение их от встроенных средств защиты.

В целом, предлагаемый подход к построению СЭД, с одной стороны, приближает технологию к привычной бумажной, поскольку ориентирован на содержание документа и то, ради чего документ образовался, – на деловые процессы, а с другой, обеспечивает все преимущества электронного документооборота в части скорости обмена документами, обеспечения разнородного, качественного и быстрого поиска документа, защиты информации и т.д.

Функциональные особенности

Предлагаемый процессо-ориентированный подход существенно отличается от традиционного СЭД в части политики управления доступом к информационным объектам. Разумеется, это не относится к письмам внутренней почтовой системы, которые доступны для создания всем пользователям, а после отправки возможно их чтение только адресатами и отправителем.

При организации процессо-ориентированного электронного документооборота необходимо учитывать, что вся нормативная база регулирует доступность именно документов, а не данных деловых процессов. Это означает, что почти вся логика работы традиционных СЭД в этой части должна быть сохранена. Отличия должны быть в процедуре изменения прав, которая может быть привязана к формированию задач, предусматривающих работу с документами. Отдельного рассмотрения требует вопрос установления прав на сами процессы и задачи при том, что в процессе могут обрабатываться документы разных уровней конфиденциальности, доступные разным пользователям по дискреционной модели. Представляется, что универсальная логика работы в этой части невозможна, она должна формироваться для каждой организации отдельно. Это, в свою очередь, означает, что процессо-ориентированные СЭД должны иметь гибкие механизмы настройки, причем более сложные, чем СЭД традиционной архитектуры. Особое внимание следует обратить на вопросы включения процессов и задач в перечень объектов защиты при формулировании политики безопасности, а также присвоения им категорий конфиденциальности.

При разработке СЭД как традиционной архитектуры, так и процессо-ориентированных, могут быть использованы элементы технологии блокчейн. Подробно эта тема применительно к различным информационным системам рассмотрена в цикле статей [20−23], поэтому здесь остановимся только на проблемах, связанных с обеспечением информационной безопасности. Строго говоря, сама технология блокчейн и ее элементы не могут рассматриваться в качестве полноценного средства защиты данных, поскольку на настоящий момент не существует нормативной базы с требованиями к реализации таких механизмов безопасности.

Представляется, что такие требования должны исходить из того, что вероятность успешной атаки с целью несанкционированного изменения прав доступа, модификации документа или искажения ин-

формации об авторстве [20, 21] должна быть достаточно мала, например, 0,0001. Исходя из этой величины следует рассчитать параметры технологии блокчейн для ее обеспечения. Такими параметрами могут, в частности, быть следующие:

число независимых серверов, на которых хранится информация, искажение которой рассматривается;

требуемая длина блока;

число блоков, следующих за блоком, в который включена транзакция, для признания транзакции легитимной;

требования к алгоритмам хэширования, применяемым для формирования цепочки блоков;

число серверов, которые должны подтвердить легитимность запрошенного действия, и другие особенности процедуры подтверждения такого действия.

- Описан подход к организации СЭД, который предполагает, по сути, переход от управления документами и процедурами их обработки к управлению деловыми процессами организации, то есть позволяет обеспечить автоматизацию бизнес-процессов, связанных с обработкой документов, и осуществлять управление заданиями. Преимущества такого изменения логики работы очевидны, они следуют из возможности целостной автоматизации работы всего коллектива, а не только той его части, которая занята работой с документами.

  Предлагаемые новшества не затрагивают привычные приемы работы и не требуют существенной переработки нормативной базы как в части работы с документами, так и в части обеспечения безопасности, но заметно расширяют возможности при автоматизации деловых процессов.

  Применение элементов технологии блокчейн в СЭД возможно, но для полноценного ее использования требуется серьезная доработка нормативных документов.

Литература

1. Система сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00. Государственный реестр сертифицированных средств защиты информации. URL = https://fstec.ru/component/attachments/download/489.
2. Типовые требования по управлению электронными официальными документами. Спецификация MoReq-2. Текст на английском языке доступен по адресу http://dlm-network.org/moreq2.
3. Системы электронного документооборота. Взаимодействие систем управления документами. Требования к электронному сообщению. ГОСТ Р53898-2010.
4. Типовая инструкция по делопроизводству в федеральных органах исполнительной власти. Утверждена приказом Министерства культуры и массовых коммуникаций РФ от 8 ноября 2005 г. № 536.
5. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов. ГОСТ Р 6.30-2003. Утв. постановлением Госстандарта РФ от 3 марта 2003 г. № 65-ст.
6. *Даниленко А.Ю.* Безопасность систем электронного документооборота: Технология защиты электронных документов. № 13. УРСС. 2015. 232 с.
7. Делопроизводство и архивное дело. Термины и определения. ГОСТ Р 51141-98. Утв. постановлением Госстандарта РФ от 27 февраля 1998 г. № 28.
8. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27 июля 2006 г. № 149-ФЗ.
9. Об утверждении Положения о системе межведомственного электронного документооборота. Постановление Правительства РФ от 22 сентября 2009 г. № 754.
10. Об утверждении Порядка проведения классификации информационных систем персональных данных. Приказ ФСТЭК России, ФСБ России, Минкомсвязи России от 13 февраля 2008 г. № 55/86/20. Российская газета. 12.04.2008.
11. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК № 21 от 18 февраля 2013 г. URL = http://fstec.ru/component/content/article/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/692-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21.
12. Положение о методах и способах защиты информации в информационных системах персональных данных, приложение к приказу ФСТЭК России от 5.02.2010 № 58. URL = http://www.fstec.ru/_docs/doc_781.doc.
13. Федеральный закон о персональных данных от 27 июля 2006 г. № 152-ФЗ.
14. Доктрина информационной безопасности РФ. URL = http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/a9dab8eb1e146cddc32569e70028f78f.
15. Кодекс РФ об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. Статья 13.12. Нарушение правил защиты информации.
16. *Савенко Т.А.* Электронный документооборот в системе электронного правительства // Экономика и социум. Институт управления и социально-экономического развития. Саратов. 2017. № 10. С. 359−361.
17. *Мясоедова Л.И.* Электронный документооборот в автоматизированных системах таможенных органов Российской Федерации // Сб. статей Междунар. научно-практич. конф. «Наука в информационном обществе». 2017. Изд-во: «Антровита». С. 62−71.

18. *Двоеносова Г.А.*, *Султанова Э.Р.* Электронный документооборот в структуре электронного правительства республики Татарстан // Делопроизводство. 2010. № 4. С. 30–38.
19. *Афиногенов В.* Автоматизация документооборота: от процесса к документу // PC Week Review: Документооборот. Май 2013.
20. *Акимова Г.П.*, *Даниленко А.Ю.*, *Пашкина Е.В.*, *Подрабинович А.А.* Применение технологии блокчейн в информационных системах. Часть 1. Защищенный электронный документооборот // Системы высокой доступности. 2018. Т. 14. № 1. С. 3–7.
21. *Даниленко А.Ю.*, *Пашкина Е.В.*, *Пашкин М.А.*, *Соловьев А.В.* Применение технологии блокчейн в информационных системах. Часть 2. Подтверждение авторства и обеспечение целостности // Системы высокой доступности. 2018. Т. 14. № 1. С. 9–11.
22. *Акимова Г.П.*, *Даниленко А.Ю.*, *Пашкина Е.В.*, *Пашкин М.А.*, *Соловьев А.В.* Применение технологии блокчейн в информационных системах. Часть 3. Цифровая экономика и сохранность электронных документов // Системы высокой доступности. 2018. Т. 14. № 1. С. 13–19.
23. *Акимова Г.П.*, *Пашкина Е.В.*, *Пашкин М.А.*, *Соловьев А.В.*, *Тарханов И.А.* Применение технологии блокчейн в информационных системах. Часть 4. Концептуальное решение задачи обеспечения сохранности электронных документов в условиях цифровой экономики // Системы высокой доступности. 2018. Т. 14. № 1. С. 20–26.

Поступила ██ ██████ 20██ г.

On one approach to the organization of electronic document management systems

© Authors, 2018
© Radiotekhnika, 2018

G.P. Akimova – Ph.D.(Eng.), Leading Research Scientist, Institute for Systems Analysis of FRC CSC RAS (Moscow)
E-mail: akimova@isa.ru
A.Yu. Danilenko – Ph.D.(Phys.-Math.), Leading Programmer, Institute for Systems Analysis of FRC CSC RAS (Moscow)
E-mail: pashkina@isa.ru
E.V. Pashkina – Research Scientist, Institute for Systems Analysis of FRC CSC RAS (Moscow)
E-mail: pashkin@isa.ru
M.A. Pashkin – Research Scientist, Institute for Systems Analysis of FRC CSC RAS (Moscow)
E-mail: pashkin@isa.ru
A.A. Podrabinovich – Leading Programmer, Institute for Systems Analysis of FRC CSC RAS (Moscow)
E-mail: podrabinovich@isa.ru
I.V. Tumanova – Leading Programmer, Institute for Systems Analysis of FRC CSC RAS (Moscow)
E-mail: tumanova-irin@mail.ru

In recent years, there has been a trend towards an increase in the use of electronic means of data exchange in state bodies, including the use of electronic document management systems (EDS), this is due to the pace of information technology development, as well as data transmission speed, which sometimes plays a decisive role in making solutions.
The concept of electronic document for all its intuitive evidence has not yet been formalized at the legislative level. In EDS, focused on domestic standards of record keeping, it is customary to treat an electronic document as a collection of a registration card containing registration information and attached files containing any information in electronic form. At present, the activities of EDS developers are practically not regulated; in their work they rely on documents regulating paperwork, documents regulating the processing of information in electronic form, as well as documents of the general audit plan.
Authors are offered to transfer the accent when working with the EDS from the registration card of the document to the document itself, which will allow the document to return its significance. The second proposal is to move from document management to managing business processes. With this approach, it is possible to implement the process without a document on the one hand, and the appearance of the document (s) in the course of the work. This does not exclude the use of the usual technology of work, when the document is first created, and then the usual actions are performed with it.
The proposed approach does not in any way contradict the standard business logic of the EDS. In particular, such systems can work together with electronic archives, i.e. ensure the delivery of documents to the archive storage, viewing documents in the archive, issuing archival materials to users. There is also the possibility of supporting paperwork. The proposed process-oriented approach differs significantly from the traditional EDS in terms of access control to information objects, since the entire regulatory framework governs the availability of documents, rather than business process data. While developing the EDS both traditional architecture and process-oriented, the elements of blockchain technology can be used, although this technology and its elements can not be considered a full-fledged data protection tool, since at the moment there is no regulatory framework with requirements for the implementation of such security mechanisms.

References

1. Sistema sertifikatsii sredstv zashchity informatsii po trebovaniyam bezopasnosti informatsii № ROSS RU.0001.01BI00. Gosudarstvennyy reyestr sertifitsirovannykh sredstv zashchity informatsii. URL = https://fstec.ru/component/attachments/download/489.
2. Tipovyye trebovaniya po upravleniyu elektronnymi ofitsial'nymi dokumentami. Spetsifikatsiya MoReq-2. Tekst na angliyskom yazyke dostupen po adresu http://dlm-network.org/moreq2.

3. Sistemy elektronnogo dokumentooborota. Vzaimodeystviye sistem upravleniya dokumentami. Trebovaniya k elektronnomu soobshcheniyu. GOST R53898-2010.
4. Tipovaya instruktsiya po deloproizvodstvu v federal'nykh organakh ispolnitel'noy vlasti. Utverzhdena prikazom Ministerstva kul'tury i massovykh kommunikatsiy RF ot 8 noyabrya 2005 g. № 536.
5. Unifitsirovannaya sistema organizatsionno-rasporyaditel'noy dokumentatsii. Trebovaniya k oformleniyu dokumentov. GOST R 6.30-2003. Utv. postanovleniyem Gosstandarta RF ot 3 marta 2003 g. № 65-st.
6. *Danilenko A.Yu.* Bezopasnost' sistem elektronnogo dokumentooborota: Tekhnologiya zashchity elektronnykh dokumentov. № 13. URSS. 2015. 232 s.
7. Deloproizvodstvo i arkhivnoye delo. Terminy i opredeleniya. GOST R 51141-98. Utv. postanovleniyem Gosstandarta RF ot 27 fevralya 1998 g. № 28.
8. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii. Federal'nyy zakon ot 27 iyulya 2006 g. № 149-FZ.
9. Ob utverzhdenii Polozheniya o sisteme mezhvedomstvennogo elektronnogo dokumentooborota. Postanovleniye Pravitel'stva RF ot 22 sentyabrya 2009 g. № 754.
10. Ob utverzhdenii Poryadka provedeniya klassifikatsii informatsionnykh sistem personal'nykh dannykh. Prikaz FSTEK Rossii, FSB Rossii, Minkomsvyazi Rossii ot 13 fevralya 2008 g. № 55/86/20. Rossiyskaya gazeta. 12.04.2008.
11. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. Prikaz FSTEK № 21 ot 18 fevralya 2013 g. URL = http://fstec.ru/component/content/article/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/692-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21.
12. Polozheniye o metodakh i sposobakh zashchity informatsii v informatsionnykh sistemakh personal'nykh dannykh, prilozheniye k prikazu FSTEK Rossii ot 5.02.2010 № 58. URL = http://www.fstec.ru/_docs/doc_781.doc.
13. Federal'nyy zakon o personal'nykh dannykh ot 27 iyulya 2006 g. № 152-FZ.
14. Doktrina informatsionnoy bezopasnosti RF. URL = http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/a9dab8eb1e146cddc32569e70028f78f.
15. Kodeks RF ob administrativnykh pravonarusheniyakh ot 30 dekabrya 2001 g. № 195-FZ. Stat'ya 13.12. Narusheniye pravil zashchity informatsii.
16. *Savenko T.A.* Elektronnyy dokumentooborot v sisteme elektronnogo pravitel'stva // Ekonomika i sotsium. Institut upravleniya i sotsial'no-ekonomicheskogo razvitiya. Saratov. 2017. № 10. S. 359–361.
17. *Myasoyedova L.I.* Elektronnyy dokumentooborot v avtomatizirovannykh sistemakh tamozhennykh organov Rossiyskoy Federatsii // Sb. statey Mezhdunar. nauchno-praktich. konf. «Nauka v informatsionnom obshchestve». 2017. Izd-vo: «Antrovita». S. 62–71.
18. *Dvoyenosova G.A., Sultanova E.R.* Elektronnyy dokumentooborot v strukture elektronnogo pravitel'stva respubliki Tatarstan // Deloproizvodstvo. 2010. № 4. S. 30–38.
19. *Afinogenov V.* Avtomatizatsiya dokumentooborota: ot protsessa k dokumentu // PC Week Review: Dokumentooborot. May 2013.
20. *Akimova G.P., Danilenko A.YU., Pashkina Ye.V., Podrabinovich A.A.* Primeneniye tekhnologii blokcheyn v informatsionnykh sistemakh. Chast' 1. Zashchishchennyy elektronnyy dokumentooborot // Sistemy vysokoy dostupnosti. 2018. T. 14. № 1. S. 3–7.
21. *Danilenko A.YU., Pashkina Ye.V., Pashkin M.A., Solov'yev A.V.* Primeneniye tekhnologii blokcheyn v informatsionnykh sistemakh. Chast' 2. Podtverzhdeniye avtorstva i obespecheniye tselostnosti // Sistemy vysokoy dostupnosti. 2018. T. 14. № 1. S. 9–11.
22. *Akimova G.P., Danilenko A.YU., Pashkina Ye.V., Pashkin M.A., Solov'yev A.V.* Primeneniye tekhnologii blokcheyn v informatsionnykh sistemakh. Chast' 3. Tsifrovaya ekonomika i sokhrannost' elektronnykh dokumentov // Sistemy vysokoy dostupnosti. 2018. T. 14. № 1. S. 13–19.
23. *Akimova G.P., Pashkina Ye.V., Pashkin M.A., Solov'yev A.V., Tarkhanov I.A.* Primeneniye tekhnologii blokcheyn v informatsionnykh sistemakh. Chast' 4. Kontseptual'noye resheniye zadachi obespecheniya sokhrannosti elektronnykh dokumentov v usloviyakh tsifrovoy ekonomiki // Sistemy vysokoy dostupnosti. 2018. T. 14. № 1. S. 20–26.

УДК 519.876

Информационная технология построения многомасштабных моделей в задачах вычислительного материаловедения

© Авторы, 2018
© ООО «Издательство «Радиотехника», 2018

К.К. Абгарян – к.ф.-м.н., зав. отделом, ФИЦ «Информатика и управление» РАН (Москва);
зав. кафедрой, Московский авиационный институт (национальный исследовательский университет)
E-mail: kristal83@mail.ru

Сформулирована постановка многомасштабных научных проблем, включающих в себя явления несопоставимых пространственных и/или временных масштабов, решение которых невозможно без учета всех факторов, играющих ключевые роли в таких задачах. Представлены основные положения разработанной информационной технологии построения многомасштабных моделей с использованием таких новых понятий, как «базовая модель-композиция» и «Многомасштабная Композиция», для их описания использован теоретико-множественный аппарат. Показано на актуальном классе задач о новых полупроводниковых материалах, что такой подход может использоваться при исследовании многомасштабных физических процессов или явлений, когда возникает задача объединения имеющихся моделей, отнесенных к разным пространственно-временным уровням, в едином вычислительном процессе.

Ключевые слова: *информационная технология, многомасштабная модель, Многомасштабная Композиция, теоретико-множественный аппарат, новые полупроводниковые материалы.*

The multiscale scientific problems are formulated including modeling the phenomena of incomparable spatial and/or temporal scales when solution cannot be achieved without taking into account all the factors that play key roles. The basic principles of the developed information technology for constructing multiscale models with the use of such new concepts as «basic model-composition» and «multiscale composition» are presented. For their description a set theory techniques are used. On the actual class of problems for new semiconductor materials it is shown that such an approach can be used in the study of multiscale physical processes or phenomena when the problem arises of combining existing models related to different space/time levels in a computational process.

Keywords: *information technology, multiscale model, multiscale composition, set theory techniques, new semiconductor materials.*

Основная часть математических моделей, применяемых для изучения физических процессов и явлений, предназначена для их описания в одном пространственно-временном масштабе. Исследование многомасштабных научных проблем, включающих в себя явления несопоставимых пространственных и/или временных масштабов, невозможно без учета всех факторов, играющих ключевые роли в таких задачах. В случаях, когда необходимо в рамках одной модели провести исследование многомасштабного физического процесса или явления, возникает проблема соединить имеющиеся модели, что требует разработки теоретических основ их объединения. На практике возникает много задач такого типа.

Ц е л ь р а б о т ы – провести теоретическое исследование проблемы многомасштабного моделирования и разработать новую математическую технологию построения многомасштабных моделей в проблемно-ориентированной области.

В данной работе рассмотрены проблемы материаловедения. Для решения задач, возникающих в области создания новых материалов с заданными свойствами, сегодня широко применяются новые подходы к построению математических моделей и информационных систем на их основе [1]. Применение технологий многомасштабного моделирования позволяет:

объяснить многие явления и процессы, включая исследование структурных особенностей материалов на нескольких масштабах и изучение их трансформаций при различных внешних воздействиях;

получать качественно новые результаты в области прогнозирования свойств материалов;

выстраивать взаимосвязи между структурой и свойствами, что, в свою очередь, дает возможность синтезировать композиционные структуры, включая полупроводниковые гетероструктуры, обладающие заданным набором свойств;

решать задачи оптимизации состава и структуры композиционных материалов;

изучать проблемы, для которых применение известных методов математического моделирования не дало адекватных результатов.

Использование методов многомасштабного моделирования, как последовательных, так и параллельных, предоставляет широкие возможности для исследования многокомпонентных и гетерогенных структур, структур с дефектами, позволяет прогнозировать магнитные, транспортные и другие свойства материалов.

Для разработки программных систем применяется модельно-ориентированный подход, который был развит в работах Ю.И. Бродского [2]. Особенностью модельно-ориентированного подхода в данной работе является использование информационных структур, объединяющих данные и методы их обработки. Поскольку в задачах вычислительного материаловедения, как правило, имеют дело с композиционными объектами, такие информационные структуры названы моделями-композициями. Базовым математическим моделям поставлены в соответствие математические объекты, названные базовыми композициями (БК). Для их описания используется теоретико-множественный аппарат [2, 3], который позволяет передать вычислительную сущность исходных математических моделей. БК являются композиционными элементами, из которых, согласно представленной в работе технологии, строятся Многомасштабные Композиции (МК) – информационные аналоги многомасштабных моделей, при помощи которых передается содержание многомасштабных вычислительных процессов. Далее на базе МК конструируются сложные иерархические программные системы, применяемые для решения задач материаловедения, в том числе полупроводникового.

В данной работе рассмотрены БК со структурой одного вида (состоят из данных и методов их обработки). В приведенном описании в БК может использоваться один или несколько процессов, в которых задействованы внутренние характеристики модели (фазовые переменные и данные-свойства).

Базовую модель-композицию можно представить, как объединение основных множеств разного структурного типа VX_{ij}, MA_{ij}, E_{ij}, $\left\{MA_{ij}^k\right\}_{k=1}^{p}$, $\left\{E_{ij}^k\right\}_{k=1}^{p}$, где i – номер масштабного уровня, $i=\overline{0,L}$, L – число рассматриваемых уровней; j – номер базовой модели-композиции на текущем масштабном уровне, $j=\overline{0,N}$, N – число моделей на i-м уровне; k – номер элементарного процесса БК.

Опишем основные множества:

$VX_{ij}=\left\{V_{ij},X_{ij}\right\}$ – множество данных, включающее множество входных данных V_{ij} (внешние характеристики модели) и множество выходных данных X_{ij} (фазовых переменных и данных-свойств модели);

MA_{ij} – множество методов обработки данных (модели и алгоритмы);

E_{ij} – множество событий, отнесенных к описанию выполняемых в рамках БК элементарных процессов;

$\left\{MA_{ij}^k\right\}_{k=1}^{p}$ – множество реализаций моделей и алгоритмов в зависимости от элементарного процесса p;

$\left\{E_{ij}^k\right\}_{k=1}^{p}$ – множество реализаций событий по элементарным процессам.

Множество методов обработки данных опишем подробнее: $MA_{ij}=\left\{M_{ij},A_{ij}\right\}=\left\{s_{ij},f_{ij},a_{ij},a_{i,\ldots,i^*,j}\right\}$. Множество моделей M_{ij}, входящих в множество MA_{ij}, состоит из статических s_{ij} и динамических f_{ij} методов обработки. Алгоритмические модели (алгоритмы) a_{ij}, $i=\overline{0,L}$, $j=\overline{1,N}$ могут быть специализированными, то есть используемыми только в данной конкретной модели с определенного масштабного уровня, или универсальными, применяемыми в различных моделях с разных масштабных уровней $a_{i,\ldots,i^*,j}$.

О п р е д е л е н и е 1. Под базовой моделью-композицией MC_i^j будем понимать однопараметрическое семейство основных множеств, задействованных в общем вычислительном процессе, разного структурного типа, включая данные (входные и выходные) и методы их обработки:

$$MC_i^j=\left\langle\left\{VX_{ij},MA_{ij},E_{ij},\left\{MA_{ij}^k\right\}_{k=1}^{p},\left\{E_{ij}^k\right\}_{k=1}^{p}\right\}\right\rangle,$$

где $VX_{ij}=\left\{V_{ij},X_{ij}\right\}$; $MA_{ij}=\left\{M_{ij},A_{ij}\right\}$; $\left\{MA_{ij}^k\right\}_{k=1}^{p}=\left\{MA_{ij}^1,MA_{ij}^2,\ldots,MA_{ij}^p\right\}$; $\left\{E_{ij}^k\right\}_{k=1}^{p}=\left\{E_{ij}^1,E_{ij}^2,\ldots,E_{ij}^p\right\}$.

Параметром семейства основных множеств является число элементарных процессов в базовой модели-композиции p. Индексы i и j позволяют идентифицировать MC_i^j на пространственном уровне i по

ее номеру j.

Структуру модели-композиции удобно представить в виде таблицы.

Таблица. ***Структура модели-композиции***

<table>
<tr><td colspan="4">Базовая модель-композиция «НАЗВАНИЕ» MC_i^j</td></tr>
<tr><td>№</td><td colspan="3">Название и обозначение множеств структурных элементов, подмножеств</td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Множество данных VX_{ij}</td><td colspan="2">V_{ij} – множество входных данных</td></tr>
<tr><td rowspan="2">$X_{ij} = \{p_v, d_p\}$ –множество выходных данных (внутренние характеристики)</td><td>Фазовые переменные p_v</td></tr>
<tr><td>Данные-свойства d_p</td></tr>
<tr><td rowspan="4">2</td><td rowspan="4">Множество методов обработки данных (модели и алгоритмы)
$MA_{ij} = \{M_{ij}, A_{ij}\} = \{s_{ij}, f_{ij}, a_{ij}, a_{i,\ldots,i^*,j}\}$</td><td rowspan="2">$M_{ij}$ – множество моделей</td><td>s_{ij} – статические</td></tr>
<tr><td>f_{ij} – динамические</td></tr>
<tr><td rowspan="2">A_{ij} – множество алгоритмов</td><td>$\tilde{a}_{ij}$ – подмножество алгоритмов, исп. только на i -м уровне масштаба (локальные)</td></tr>
<tr><td>$\tilde{a}_{i,\ldots,i^*,j}$ – подмножество алгоритмов, исп. на нескольких уровнях $i,\ldots,i^*$ (универсальные)</td></tr>
<tr><td>3</td><td colspan="3">Множество событий и реализаций событий по процессам E_{ij}, $\{E_{ij}^k\}_{k=1}^p$</td></tr>
<tr><td>4</td><td colspan="3">Множество реализаций методов обработки данных $MA_{ij}^k = \{MA_{ij}^k\}_{k=1}^p$</td></tr>
</table>

Такое представление полностью описывает структуру базовой модели-композиции и задает шаблон, который будет заполняться конкретными данными при создании реальных экземпляров БК для решения практических задач математического моделирования.

Под Композицией K будем понимать объединение экземпляров БК в более сложные математические объекты, состоящие из двух и более элементов. Композиция в некотором смысле является аналогом понятия модель-комплекс, введенного в работе [2].

О п р е д е л е н и е 2. Под Композицией $K_i^{j^*}$ будем понимать однопараметрическое семейство, полученное из экземпляров БК с одного масштабного уровня за счет объединения их основных множеств разного структурного типа в общем вычислительном процессе.

Здесь i принимает одно из значений от 0 до L в зависимости от масштабного уровня, к которому отнесена K, а j^* обозначает совокупность номеров $j_1, j_2, \ldots, j_n$ базовых моделей-композиций на соответствующем масштабном уровне. В качестве параметра выступает $p = p_{j_1} + p_{j_2} + \ldots + p_{j_n} = \sum_{k=1}^{n} p_{j_k}$, указывающий на число процессов в K и зависящий от числа процессов во всех задействованных БК, входящих в нее ($p \geq 2$).

Таким образом, Композиция может быть описана как

$$K_i^j = \left\langle \left\{ VX_{ij}, MA_{ij}, E_{ij}, \left\{ MA_{ij}^k \right\}_{k=1}^p, \left\{ E_{ij}^k \right\}_{k=1}^p \right\} \right\rangle,$$

где j обозначает подмножество $\{j_1, j_2, \ldots, j_n\}$ номеров БК, входящих в состав $K_i^j = K_i^{j_1, j_2, \ldots, j_n}$; i – номер масштабного уровня, на котором создается Композиция.

В определенном смысле K_i^j схожа с базовой моделью-композицией, так как представляет собой совокупность основных множеств разных структурных типов, связанных общим вычислительным процессом. Однако ее структуру можно представить набором таблиц, соответствующих экземплярам входящих в нее БК, расположенных в определенном порядке.

Пусть на i-м масштабном уровне имеются $MC_i^{j_1}$ и $MC_i^{j_2}$, где j_1, j_2 – номера соответствующих БК на масштабном уровне i, а p_{j_1} и p_{j_2} – обозначения числа элементарных процессов в БК. Составим Композицию $K_i^j = K_i^{j_1,j_2}$ из $MC_i^{j_1}$ и $MC_i^{j_2}$. Основными множествами K_i^j с процессом p, объединяющим процессы p^{j_1} и p^{j_2}, будут: $V_{ij} = V_{ij_1} \cup V_{ij_2}$, $X_{ij} = X_{ij_1} \cup X_{ij_2}$, $MA_{ij} = MA_{ij_1} \cup MA_{ij_2}$, $E_{ij} = E_{ij_1} \cup E_{ij_2}$, $\left\{MA_{ij}^k\right\}_{k=1}^{p} = \left\{MA_{ij_1}^k\right\}_{k=1}^{p_{j_1}} \cup \left\{MA_{ij_2}^k\right\}_{k=1}^{p_{j_2}}$, $\left\{E_{ij^*}^k\right\}_{k=1}^{p} = \left\{E_{ij_1}^{\mathrm{k}}\right\}_{\mathrm{k}=1}^{p_{j_1}} \cup \left\{\mathrm{E}_{ij_2}^{\mathrm{k}}\right\}_{\mathrm{k}=1}^{p_{j_2}}$.

Объединение основных множеств $VX_{ij} = VX_{ij_1} \cup VX_{ij_2}$ означает, что

$$V_{ij_1} \cup V_{ij_2} = \left\{v : \left(v \in V_{ij_1}\right) \cup \left(v \in V_{ij_2}\right)\right\}, \quad X_{ij_1} \cup X_{ij_2} = \left\{x : \left(x \in X_{ij_1}\right) \cup \left(x \in X_{ij_2}\right)\right\},$$
$$MA_{ij_1} \cup MA_{ij_2} = \left\{m : \left(m \in MA_{ij_1}\right) \cup \left(m \in MA_{ij_2}\right)\right\}, \quad E_{ij_1} \cup E_{ij_2} = \left\{e : \left(e \in E_{ij_1}\right) \cup \left(e \in E_{ij_2}\right)\right\}.$$

Объединение множеств $\left\{MA_{ij_1}^k\right\}_{k=1}^{p_{j_1}}$ и $\left\{MA_{ij_2}^k\right\}_{k=1}^{p_{j_2}}$ означает, соответственно,

$$\left\{MA_{ij_1}^1, \ldots, MA_{ij_1}^{p_{j_1}}, MA_{ij_2}^1, \ldots, MA_{ij_2}^{p_{j_2}}\right\}.$$

Аналогично, $\left\{E_{ij_1}^k\right\}_{k=1}^{p_{j_1}} \cup \left\{E_{ij_2}^k\right\}_{k=1}^{p_{j_2}} = \left\{E_{ij_1}^1, \ldots, E_{ij_1}^{p^{j_1}}, E_{ij_2}^1, \ldots, E_{ij_2}^{p_{j_2}}\right\}$.

Создание K из двух различных экземпляров БК осуществляется за счет того, что происходит объединение их основных множеств соответственно структурному типу в одном вычислительном процессе. Важным элементом такого объединения является выделение параметров, которые передаются после окончания работы из одной БК в другую в качестве входных данных.

При создании Композиций, состоящих из двух БК одного уровня, например, MC_i^j и $MC_i^{j^*}$, выделим локальные параметры. Локальными будем называть параметры $v \in X_{ij} \cap V_{ij^*}$, где $X_{ij} \in MC_i^j$ – множество выходных данных MC_i^j, а $V_{ij^*} \in MC_i^{j^*}$ – множество входных данных $MC_i^{j^*}$:

$$X_{ij} \cap V_{ij^*} = \left\{v : \left(v \in X_{ij}\right) \cap \left(v \in V_{ij^*}\right), v \in VX_{ij^*}\right\}.$$

Далее приведем описание МК, позволяющее представить следующую информацию: из каких именно моделей-композиций с каких масштабных уровней она состоит, сколько и какие процессы задействованы в ее работе, каким образом происходит обмен данными между моделями-композициями с разных уровней.

О п р е д е л е н и е 3. Под МК будем понимать однопараметрическое семейство, полученное из экземпляров БК с разных масштабных уровней за счет объединения в общем вычислительном процессе их основных множеств разного структурного типа, включая данные (входные и выходные) и методы их обработки.

МК будем обозначать через $MK_{i,i^*,\ldots,i^{***}}^{i,j;i^*,j^*;\ldots;i^{***},j^{***}}$, где $i, i^*, \ldots, i^{***}$ – номера масштабных уровней, задействованных в данной МК; $j, j^*, \ldots, j^{***}$ – номера БК на конкретном масштабном уровне. В определенном смысле $MK_{i,i^*,\ldots,i^{***}}^{i,j;i^*,j^*;\ldots;i^{***},j^{***}}$ схожа с БК, так как представляет собой объединение основных множеств разных структурных типов, связанных общим вычислительным процессом. Ее структуру, так же, как и структуру K, можно представить набором таблиц, соответствующих экземплярам входящих в нее БК, расположенных в определенном порядке, соответствующем иерархии масштабов, задействованных в ней.

Пусть на i-м масштабном уровне имеется экземпляр MC_i^j и на i^*-м масштабном уровне экземпляр $MC_{i^*}^{j^*}$, где j, j^* – номера базовых моделей-композиций на масштабных уровнях i и i^* соответственно.

Составим Многомасштабную Композицию $MK_{i,i^*}^{ij;i^*j^*}$ из двух экземпляров базовых композиций MC_i^j и $MC_{i^*}^{j^*}$. Основными множествами, как и в случае создания композиции, будут: $V_{ij} \cup V_{i^*j^*}$, $X_{ij} \cup X_{i^*j^*}$, $MA_{ij} \cup MA_{i^*j^*}$, $E_{ij} \cup E_{i^*j^*}$, $\left\{MA_{ij}^k\right\}_{k=1}^{p} \cup \left\{MA_{i^*j^*}^k\right\}_{k=1}^{p^*}$, $\left\{E_{ij}^k\right\}_{k=1}^{p} \cup \left\{E_{i^*j^*}^k\right\}_{k=1}^{p^*}$, где p и p^* – число процессов в БК MC_i^j и $MC_{i^*}^{j^*}$ соответственно.

МК можно описать следующим образом:

$$MK_{i,i^*}^{ij;i^*j^*} = \left\langle \left\{ V \cup V_{i^*j^*}, X_{ij} \cup X_{i^*j^*}, MA_{ij} \cup MA_{i^*j^*}, E_{ij} \cup E_{i^*j^*}, \left\{MA_{ij}^k\right\}_{k=1}^{p} \cup \left\{MA_{i^*j^*}^k\right\}_{k=1}^{p^*}, \left\{E_{ij}^k\right\}_{k=1}^{p} \cup \left\{E_{i^*j^*}^k\right\}_{k=1}^{p^*} \right\} \right\rangle.$$

Число процессов в МК равно сумме $p + p^*$.

Связующими элементами между вычислительными моделями с разных масштабных уровней, входящими в МК, являются глобальные параметры, которые играют основную роль при передаче информации между масштабными уровнями.

Пусть необходимо составить $MK_i^j = MK_{i^*,i^{**}}^{i^*,j^*;i^{**},j^{**}}$ из $MC_{i^*}^{j^*}$ и $MC_{i^{**}}^{j^{**}}$. В этом случае под глобальными параметрами $\breve{v} \in VX_{ij} = \left\{ V_{i^*j^*} \cup V_{i^{**}j^{**}}, X_{i^*j^*} \cup X_{i^{**}j^{**}} \right\}$ будем понимать элементы (параметры), относящиеся к множеству $X_{i^*j^*} \cap V_{i^{**}j^{**}}$, образованному в результате пересечения двух множеств выходных данных $X_{i^*j^*}$ с нижнего масштабного уровня и входных данных $V_{i^{**}j^{**}}$ с верхнего масштабного уровня:

$$X_{i^*j^*} \cap V_{i^{**}j^{**}} = \left\{ \breve{v} : \left(\breve{v} \in X_{i^*j^*}\right) \cap \left(\breve{v} \in V_{i^{**}j^{**}}\right), \breve{v} \in VX_{ij} \right\}.$$

Кроме того, при построении МК используются базовые модели-композиции специального вида, обозначенные DB_i, где i – номер масштабного уровня, $i = \overline{0, L}$, L – число рассматриваемых уровней. Они требуются для хранения и передачи дополнительной информации, необходимой для работы БК соответствующего уровня.

Такой подход может использоваться для описания многомасштабной технологии, применяемой в ходе предсказательного моделирования структурных особенностей и различных свойств полупроводниковых наносистем [4–6]. Покажем, как он работает на примере актуальной задачи в данной области.

Одной из современных тенденций развития высокочастотной полупроводниковой техники является стремление к достижению максимальных концентраций носителей заряда при максимально возможной их подвижности. Особенности электронных свойств новых полупроводниковых наноматериалов во многом связаны с их характерными размерами. Проведение натурных экспериментов по выращиванию новых полупроводниковых гетероструктур с заданными свойствами, широко применяемых в полупроводниковой электронике, сопряжено с большими временными и финансовыми затратами. В связи с этим весьма актуальным является применение методов многомасштабного моделирования для решения задач такого класса.

Рассмотрим следующий пример. Для расчета проводящих свойств новых многослойных гетероструктур была построена МК «РАСЧЕТ КОНЦЕНТРАЦИИ И ПОДВИЖНОСТИ НОСИТЕЛЕЙ В ГЕТЕРОСТРУКТУРЕ» $MK_{0,1,3,4}^{1,1;1,2;3,1;3,2;4,1}$, которая состоит из пяти базовых моделей-композиций с четырех масштабных уровней:

с 0-го уровня используется базовая модель-композиция «АТОМ A_0^i» (MC_0^1);

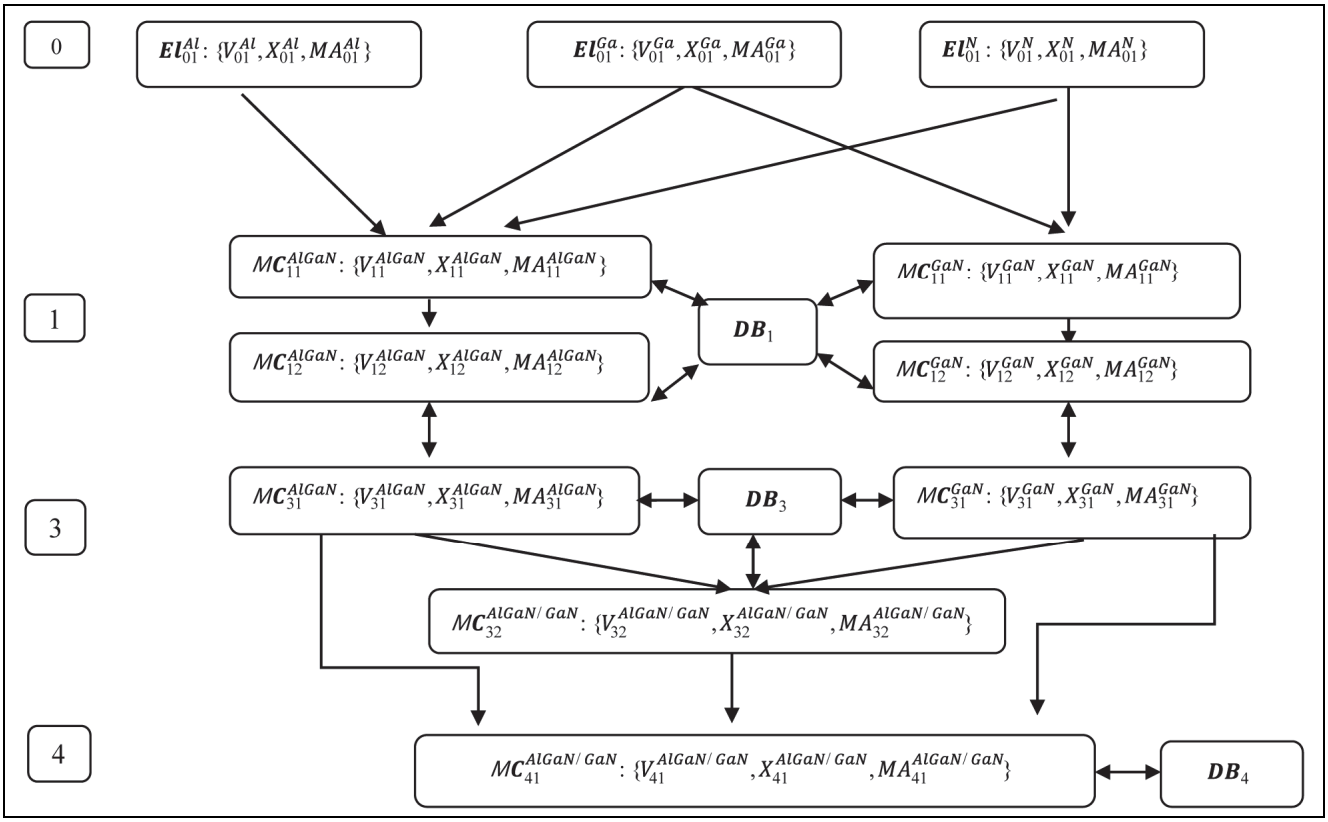
с 1-го уровня – БК «КРИСТАЛЛОХИМИЧЕСКАЯ ФОРМУЛА» (MC_1^1) и БК «КВАНТОВО-МЕХАНИЧЕСКАЯ ЯЧЕЙКА» (MC_1^2);

- с 3-го уровня – БК «НАНОРАЗМЕРНЫЙ СЛОЙ» (MC_3^1) и БК «ГЕТЕРОИНТЕРФЕЙС» (MC_3^2);

- с 4-го уровня – БК «ГЕТЕРОСТРУКТУРА» (MC_4^1).

На рисунке представлена структура многомасштабной композиции для расчета концентрации и подвижности носителей заряда в двухслойной полупроводниковой гетероструктуре $Al_vGa_{1-v}N/GaN$. Выделено четыре пространственно-временных масштабных уровня. Указаны экземпляры БК и последовательность их использования в вычислительном процессе. По данной МК была построена информационная система, где каждой из используемых БК соответствует программный модуль, в котором реализована конкретная математическая модель. Так, например, базовой модели-композиции «КРИСТАЛЛОХИМИЧЕСКАЯ ФОРМУЛА» (MC_1^1) соответствует программный модуль, в котором реализована модель ионно-атомных радиусов, позволяющая по заданной химической формуле рассчитывать метрические параметры кристаллических структур. Для уточнения полученных параметров и расчета энергетических характеристик заданной структуры применяются квантово-механические расчеты в рамках теории функционала электронной плотности [7], реализованные в пакете VASP (http://cms.mpi.univie.ac.at/vasp/), которому соответствует базовая модель-композиция «КВАНТОВО-МЕХАНИЧЕСКАЯ ЯЧЕЙКА» (MC_1^2). Далее на уровне гетероструктуры используется математическая модель, основанная на системе уравнений Шредингера–Пуассона, позволяющая рассчитать распределение электронов в системе с учетом квантовых эффектов. Расчет подвижности носителей осуществляется с учетом основных механизмов рассеяния.

Вычисления проводились с применением высокопроизводительных программных средств МСЦ РАН и ЦКП ФИЦ ИУ РАН. Результаты тестовых расчетов верифицировались по экспериментальным данным, собранным в ходе выращивания аналогичных структур методом молекулярно-лучевой эпитаксии в Институте физики полупроводников СО РАН. Было получено хорошее согласование экспериментальных и расчетных данных [5, 6].



Структура МК для расчета свойств гетероструктуры $Al_vGa_{1-v}N/GaN$

- Как видно на рисунке, при таком подходе вычислительный процесс естественно распараллеливается, что существенно увеличивает скорость расчета значений концентрации и подвижности носителей в рассматриваемом типе гетероструктур и позволяет собирать и накапливать для дальнейшей обработки информацию по схеме структура–свойства. Данная МК может применяться для аналогичных расчетов полупроводниковых гетероструктур с другим химическим составом, что существенно расширяет возможности по сбору и анализу материаловедческих данных. Разработанная информационная технология многомасштабного моделирования может применяться для решения обратных задач по определению химического состава и структурных характеристик полупроводниковых гетероструктур, обладающих заданным набором свойств, что создает основу для решения ряда оптимизационных задач, актуальных для современной СВЧ-электроники.

Работа выполнена при финансовой поддержке РФФИ, проект № 16-08-01178.

Литература

1. *Lesard* Introduction to Computational Materials Science. Fundamentals to Applications. Cambridge University Press. 2013. 414 с.
2. *Бродский Ю.И.* Модельный синтез и модельно-ориентированное программирование М.: ВЦ РАН. 2013. 142 с.
3. *Куратовский К.*, *Мостовский А.* Теория множеств. М.: Мир. 1970. 416 с.
4. *Абгарян К.К.* Применение оптимизационных методов для моделирования многослойных полупроводниковых наносистем // Труды Института системного анализа РАН. Динамика неоднородных систем. 2010. Т. 53(3). С. 6–9.
5. *Абгарян К.К.* Задачи оптимизации наноразмерных полупроводниковых гетероструктур // Известия ВУЗов. Материалы электронной техники. 2016. Т. 19. № 2. С. 112–118.
6. *Абгарян К.К.*, *Ревизников Д.Л.* Численное моделирование распределения носителей заряда в наноразмерных полупроводниковых гетероструктурах с учетом поляризационных эффектов // ЖВМ и МФ. 2016. Т. 56. № 1. С. 155–166.
7. *Kohn W.*, *Sham L.J.* // Phys. Rev. 1965. 140. A1133.

Поступила 20 апреля 2018 г.

Information technology of the construction of multi-scale models in problems of computational materials science

© Authors, 2018
© Radiotekhnika, 2018

K.K. Abgaryan – Ph.D.(Phys.-Math.), Head of Department, FRC «Computer Science and Control» RAS (Moscow); Head of Department, Moscow Aviation Institute (National Research University)
E-mail: kristal83@mail.ru

The multiscale scientific problems are formulated including modeling the phenomena of incomparable spatial and/or temporal scales when solution cannot be achieved without taking into account all the factors that play key roles. The basic principles of the developed information technology for constructing multiscale models with the use of such new concepts as «basic model-composition» and «Multiscale Composition» are presented. For their description a set theory techniques are used. On the actual class of problems for new semiconductor materials it is shown that such an approach can be used in the study of multiscale physical processes or phenomena when the problem arises of combining existing models related to different space/time levels in a computational process. The developed information technology of multiscale modeling can be used to solve inverse problems in determining the chemical composition and structural characteristics of semiconductor heterostructures with a given set of properties, which creates the basis for solving a number of optimization problems relevant to modern microwave electronics.

References

1. *Lesard* Introduction to Computational Materials Science. Fundamentals to Applications. Cambridge University Press. 2013. 414 p.
2. *Brodsky Yu.I.* Model'nyj sintez i model'no-orientirovannoe programmirovanie. M.: VC RAN. 2013. 142 s.
3. *Kuratovskij K., Mostovskij A.* Teoriya mnozhestv. M.: Mir. 1970. 416 s.
4. *Abgaryan K.K.* Primenenie optimizacionnyh metodov dlya modelirovaniya mnogoslojnyh poluprovodnikovyh nanosistem // Trudy Instituta sistemnogo analiza RAN. Dinamika neodnorodnyh sistem. 2010. T. 53(3). S. 6–9.
5. *Abgaryan K.K.* Zadachi optimizacii nanorazmernyh poluprovodnikovyh geterostruktur // Izvestiya VUZov. Materialy ehlektronnoj tekhniki. 2016. T. 19. № 2. S. 112–118.
6. *Abgaryan K.K., Reviznikov D.L.* Numerical simulation of the distribution of charge carrier in nanosized semiconductor heterostructures with account for polarization effects // Computational Mathematics and Mathematical Physics. 2016. T. 56. № 1. P. 161–172.
7. *Kohn W.*, *Sham L.J.* // Phys. Rev. 1965. 140. A1133.

УДК 621

Разработка метода «относительных разниц» при определении мета и геоданных для ГИС

© Авторы, 2018
© ООО «Издательство «Радиотехника», 2018

А.В. Воронин – к.т.н., доцент, вед. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: aleksey.v.v@mail.ru

Рассмотрено решение задачи разработки метода «относительных разниц» (МтОР) при определении мета и геоданных для геоинформационных систем (ГИС), отличающегося от известных учетом данных контроля и управления, циркулирующих в инфокоммуникационных системах, маркирующий мета и геоданные, а также позволяющего сократить время и повысить эффективность анализа мета и геоданных, транслируемых в современных инфокоммуникационных системах.

Ключевые слова: *геоинформационная система (ГИС), метод, метаданные, геоданные, метод «относительных разниц» (МтОР), модель.*

The article continues the thematic series of the articles devoted to the geoinformation systems (GISs), which considers the solution of the problem of developing the method of «relative differences» (MtRD) when determining meta and geodata for GIS, which differs from known by taking into account the control and management data circulating in infocommunication systems, marking meta and geodata, allowing to reduce the time and improve the efficiency of meta and geodata analysis broadcast in modern infocommunication systems.

Keywords: *geoinformation system (GIS), method, metadata, geodata, method of «relative differences» (MtRD), model.*

Методы и способы анализа данных на современном этапе развития ситуационных центров не соответствуют требованиям, предъявляемым к геоинформационным системам (ГИС) нового поколения. Одним из основных требований является актуальность мета и геоданных, подвергаемых анализу в ситуационном центре. Поддержание данных в актуальном состоянии является нетривиальной задачей. В настоящее время для поддержания мета и геоданных в актуальном состоянии осуществляется их регулярное, периодическое обновление из каналов инфокоммуникационных систем с использованием статистических методов обработки и анализа данных [1−5]. Применяемые при этом статистические модели битовых последовательностей не позволяют учесть качественное изменение, произошедшее на современном этапе развития инфокоммуникационных систем [6−12], а именно: наличие и увеличение объемов передачи управляющей информации в цифровых потоках, транслируемых инфосистемами.

Ц е л ь р а б о т ы – разработать метод «относительных разниц» для анализа цифровых потоков по определению управляющей информации, включая информацию геопозиционного характера, в рамках детерминированного факторного анализа с использованием критерия полноты транслируемых мета и геоданных для ГИС, а также актуализации и систематизации знаний о данных, передаваемых в потоках.

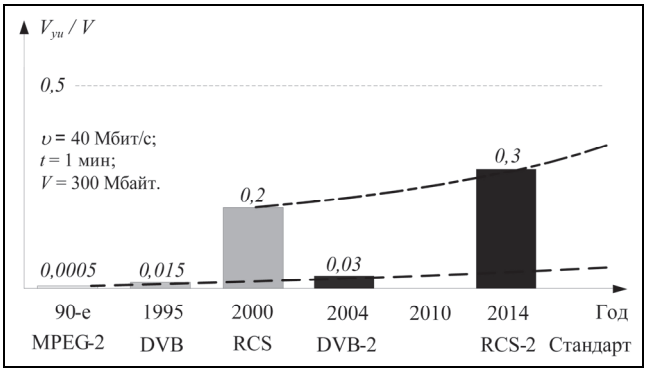


Рис. 1. График роста объема управляющей информации относительно общего объема передаваемых данных (на примере потоков, транслируемых в инфокоммуникационных системах VSAT)

Модель цифрового потока, учитывающая системные связи и закономерности композиции плоскостей управления и данных

Наличие и увеличение объемов передачи управляющей информации (рис. 1) обусловлено тем, что мировой рынок инфокоммуникационных систем претерпевает существенную модернизацию. Это связано как с достижениями в области научно-технического прогресса, так и с востребованностью на мировом рынке hi-tech-услуг передачи больших объемов информации для реализации широкого спектра мультимедийных услуг.

Разнообразие инфокоммуникационных си-

стем и архитектур их построения формируют многообразие информационно-коммуникационного мира. Сопряжение устройств (систем, сетей) обеспечивается через стандартизованные преобразователи интерфейсов различных уровней эталонной модели взаимодействия открытых систем (ЭМВОС).

Функциональность и мобильность современных hi-tech-устройств, а также сложность архитектур построения информационных систем выдвигают требование пространственного и сетевого позиционирования устройств в геосреде. В результате в транслируемых структурах наряду с информацией содержатся команды управления как системного, сервисного характера, так и позиционирования: координаты местоположения, условия электромагнитного доступа, адресная информация различных уровней ЭМВОС. Управляющая информация передается для обеспечения функционирования системы, а также для снижения сложности ее управления со стороны потребителя услуги.

Исследованием управляющей информации в цифровых потоках инфокоммуникационных систем для отображения местоположения объекта в пространстве занимается телегеоинформатика [13], которая рассматривает вопросы построения и поддержания в рабочем состоянии hi-tech-систем с учетом позиционирования объектов на местности. Системы при этом, как правило, имеют развитую топологию построения. Предлагается расширение модели взаимодействия открытых телекоммуникационных систем посредством введения на физическом уровне модуля позиционирования инфокоммуникационного объекта. Получение исходных данных, позволяющих определить (рассчитать) местоположение объекта в геопространстве (слой специализированных геоданных), обуславливает необходимость разработки модели цифрового потока, отражающей системные связи и закономерности композиции плоскостей управления и данных (рис. 2).

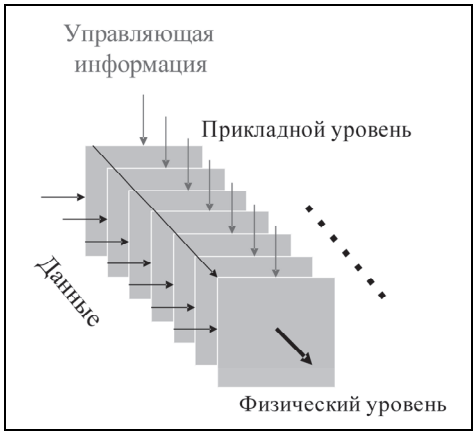


Рис. 2. Композиция плоскостей управления и данных на различных уровнях ЭМВОС

Наличие в цифровых потоках разнородной управляющей информации на всех уровнях ЭМВОС является характерной особенностью цифровых потоков, транслируемых в современных инфокоммуникационных сетях.

Управляющая информация – это данные, содержащие параметры характеристик, команды управления на всех уровнях ЭМВОС, обеспечивающие передачу пользовательских данных и функционирование объекта в частности и в целом.

В настоящий момент известны следующие модели трафиков, используемые при перспективном планировании инфокоммуникационных систем, прогнозировании их производительности, регулировании и организации управления в режиме реального времени:

модель эластичного трафика, которая способна учитывать изменения скорости потока в соответствии с изменениями пропускной способности сети (электронная почта, передача файлов, сетевые новости, интерактивные приложения);

модель неэластичного трафика, которая не способна учитывать изменения скорости потока (мультимедийные приложения, речь, видео);

статистические модели трафика, определяющие трафик как вероятностный процесс дискретного времени с отсутствующей функцией автокорреляции (процессы Пуассона и Бернулли);

статистические модели трафика, определяющие трафик как вероятностный процесс дискретного времени, вводя в зависимость случайную последовательность – наличие функции автокорреляции (модель Маркова);

модели, представляющие трафик как поток жидкости, характеризуемый скоростью потока и емкостью трафика (требует значительных вычислительных ресурсов при моделировании трафика);

авторегрессионные модели трафика, которые описывают трафик линейной функцией (линейные авторегрессионные модели);

модель видеотрафика, которая представляет собой поток данных как результат совокупности действия разнородных процессов, описываемых различными функциями и выражениями.

Однако ни одна из приведенных моделей не учитывает современную тенденцию развития инфор-

мационно-коммуникационного мира, заключающуюся в увеличении доли управляющей информации (включая гео-), транслируемой в цифровых потоках. При этом необходимо отметить, что пакетная архитектура построения потоков позволяет легко вводить и динамично регулировать данные управления в цифровом потоке.

Исходя из вышеизложенного, предлагается модель [14], учитывающая мультиплексный характер построения современных цифровых потоков, которая позволит также учитывать долевое соотношение данных трафика и управления, передаваемых на всех уровнях ЭМВОС:

$$\text{ЦП} = \sum_{n=1}^{N} \text{ЭП}_n + \sum_{k=1}^{K} \text{ЭП}_k \,, \tag{1}$$

где ЦП – цифровой поток; ЭП – элементарные потоки, формирующие цифровой поток; N – число элементарных потоков данных в цифровом потоке; K – число элементарных потоков управляющей информации в цифровом потоке.

Выражение (1) описывает ЦП как сумму ЭП. ЦП содержит как ЭП данных, так и управляющей информации. Кроме этого, каждый ЭП, содержащий данные, включает в себя наряду с данными и протоколы вышележащих уровней ЭМВОС с управляющей информацией соответствующего уровня:

$$\text{ЭП}_{n_j} = \sum_{l=1}^{L} D_l + \sum_{h=1}^{H} D_h \,, \tag{2}$$

где анализируются данные D на j-уровне ЭМВОС; L – число протоколов управляющей информации на j-уровне ЭМВОС; H – число протоколов с данными на j-уровне ЭМВОС.

В результате мультиплексную модель транспортного цифрового потока данных можно представить следующим выражением:

$$\text{ЦП} = \sum_{j=1}^{J} \left[\sum_{n=1}^{N} \left(\sum_{l=1}^{L} D_l + \sum_{h=1}^{H} D_h \right)_n + \sum_{k=1}^{K} \text{ЭП}_k \right]_j , \tag{3}$$

где J – число уровней ЭМВОС.

Конкретизация модели с учетом интенсивности следования байт-кратных пользовательских и управляющих данных имеет вид

$$\vartheta t = \sum_{j=1}^{J} \left[\sum_{n=1}^{N} \left(\sum_{h=1}^{H} V_h + \sum_{l=1}^{L} \lambda_l d_l 8t \right)_n + \sum_{k=1}^{K} \lambda_k d_k 8t_k \right]_j , \tag{4}$$

где λ – интенсивность следования данных; d – размер данных в байтах; υ – информационная скорость трансляции данных; V – объем данных; t – время.

Предложенная модель позволяет систематизировать знания о данных, передаваемых в потоках, рассчитать эффективность использования емкости контейнера потока по передаче полезной нагрузки, синтезировать метод обработки цифровых потоков по определению управляющей информации, включая информацию геопозиционного характера, с использованием критерия полноты (соответствия объемов) и актуальности транслируемой управляющей информации и пользовательских данных.

Была проведена проверка адекватности разработанной модели по критерию полноты (соответствия объемов) транслируемой управляющей информации и пользовательских данных в реальных и моделируемых ЦП. В качестве исходных данных при моделировании цифровых потоков использовались: интенсивность следования и размер управляющих данных согласно стандартам ISO/IEC 13818, ETSI EN 300486, ETSI EN 301790 [6–8]; информационная скорость трансляции данных реальных ЦП до $\upsilon = 40$ Мбит/с при объеме выборок реализаций до $V = 300$ Мбайт и времени наблюдения $t = 1$ мин. Результаты проверки адекватности разработанной модели следующие: 0,98 для стандарта ISO/IEC 13818; 0,95 для ETSI EN 300486; 0,93 для ETSI EN 301790.

Показатели адекватности обусловлены наличием на практике временного дрожания (джиттера) следования управляющих данных.

В результате первой части исследований разработана мультиплексная модель цифрового потока данных, транслируемых в инфокоммуникационных системах, представленная выражением (3) и предназначенная для систематизации знаний о данных, передаваемых в потоках, расчета эффективности использования емкости контейнера потока по передаче полезной нагрузки, синтеза метода обработки цифровых потоков по определению управляющей информации, включая информацию геопозиционного характера, с использованием критерия полноты транслируемой управляющей информации.

Метод «относительных разниц» при определении мета и геоданных для ГИС

Анализ модели позволяет сделать вывод о возможности вычленения управляющих данных из ЦП для актуализации мета и геоданных в ГИС. При этом, учитывая, что управляющая информация байт-кратна, имеет периодичность следования и транслируется на всех уровнях ЭМВОС, возможно выделение данных с учетом числа элементарных потоков управляющей информации в цифровом потоке K и числа протоколов управляющей информации L на каждом j-уровне ЭМВОС относительно пользовательских данных в цифровом потоке (с учетом N и H на каждом j-уровне ЭМВОС).

В связи с полученным результатом целесообразно при разработке метода анализа данных цифровых потоков по определению объема данных управления для актуализации использовать математический и методологический аппарат детерминированного факторного анализа [15, 16].

Выбор модели (аддитивной, мультипликативной, смешанной) [15] для проведения факторного анализа определяется рассматриваемым числом элементарных потоков и протоколов управляющей информации в цифровом потоке, а также рассматриваемых уровней ЭМВОС на основе выражения (4).

В качестве факторов при мультипликативной модели выступают размер данных и их число, определяемое как

$$B = \lambda t . \tag{5}$$

В качестве результата – объем транслируемых данных управляющей информации

$$V_{\text{уи}} = Bd . \tag{6}$$

При аддитивной модели в качестве факторов выступают: общий объем транслируемых данных ТД и объем пользовательских данных $V_{\text{пд}}$. В качестве результата – объем транслируемых данных управляющей информации $V_{\text{уи}}$. Для конкретного уровня ЭМВОС и цифрового потока данных, состоящего из элементарного потока пользовательских данных и элементарного потока данных управления, использующих по одному протоколу, модель имеет вид

$$V_{\text{уи}} = \text{ТД} - V_{\text{пд}} . \tag{7}$$

Смешанная модель определяется выражением (4).

При анализе осуществляется вычленение всей (критерий полноты) управляющей информации относительно пользовательских данных при различном объеме на разных уровнях ЭМВОС и в элементарных потоках (определение того, на каком уровне или в каком элементарном потоке управляющих данных больше – лучший результат). Целесообразно данную операцию осуществлять как относительную разность значений изменения факторов, влияющих на результат, на разных уровнях или в элементарных потоках.

В методе «относительных разниц» (МтОР) для анализа цифровых потоков по определению объема данных управляющей информации используются относительные приросты факторных показателей (выраженные в виде коэффициентов или процентов). Введение коэффициентов особенно актуально в случае маркирования уровня или потока, содержащего геоданные (координаты, сетевая или почтовая адресация). Также МтОР использует прием нарастающего итога.

Реализацию счетной процедуры при использовании МтОР по анализу цифровых потоков (мультиплексная модель) с целью определения объема управляющей информации рассмотрим для инфокоммуникационной системы VSAT (актуализируются данные двух таблиц управления: NIT (стандарт ETSI EN 300486) и RMT (стандарт ETSI EN 301790), содержащихся в ЦП). Схема счетной процедуры представлена на рис. 3.

На первом этапе определяется относительное отклонение каждого факторного показателя в процентах, в рассматриваемом случае это

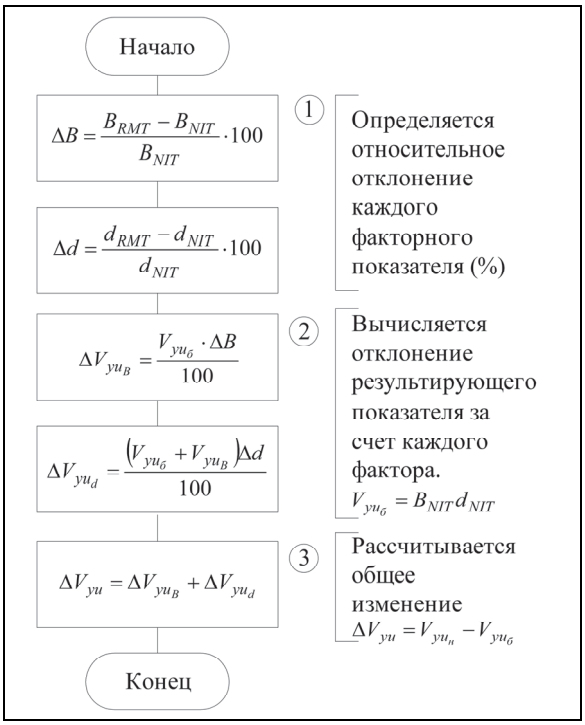


Рис. 3. Схема счетной процедуры при использовании МтОР (инфокоммуникационная система VSAT, актуализируются данные таблиц управления: NIT (стандарт ETSI EN 300486) и RMT (стандарт ETSI EN 301790))

$$\Delta B = \frac{B_{\text{RMT}} - B_{\text{NIT}}}{B_{\text{NIT}}} \cdot 100\,, \tag{8}$$

$$\Delta d = \frac{d_{\text{RMT}} - d_{\text{NIT}}}{d_{\text{NIT}}} \cdot 100\,. \tag{9}$$

На втором этапе вычисляется отклонение результирующего показателя за счет каждого фактора согласно выражениям

$$\Delta V_{\text{уи}_B} = \frac{V_{\text{уи}_\text{б}} \Delta B}{100}, \tag{10}$$

$$\Delta V_{\text{уи}_d} = \frac{\left(V_{\text{уи}_\text{б}} + V_{\text{уи}_B}\right)\Delta d}{100}, \tag{11}$$

где $V_{\text{уи}_\text{б}}$ – базовое значение результирующего показателя, в рассматриваемом случае равное

$$V_{\text{уи}_\text{б}} = B_{\text{NIT}} d_{\text{NIT}}\,. \tag{12}$$

Расчет влияния первого фактора производится умножением базовой величины результирующего показателя на относительный прирост первого фактора.

Расчет влияния второго фактора осуществляется суммированием базовой величины результирующего показателя с его изменением за счет первого фактора с последующим умножением полученной суммы на относительный прирост второго фактора.

Если в исходной модели число факторов более двух, то влияние последующих факторов определяется аналогично: к базовой величине результативного показателя прибавляют его прирост за счет предыдущих факторов, затем результат умножается на относительный прирост рассматриваемого фактора.

На третьем этапе общее изменение $\Delta V_{\text{уи}}$ рассчитывается как

$$\Delta V_{\text{уи}} = V_{\text{уи}_\text{н}} - V_{\text{уи}_\text{б}}\,, \tag{13}$$

где $V_{\text{уи}_\text{н}}$ – управляющая информация с учетом данных в таблицах NIT и RMT; $V_{\text{уи}_\text{б}}$ – управляющая информация с учетом данных только в таблице NIT.

При этом оно определяется как сумма изменений результирующего показателя за счет изменения каждого фактора:

$$\Delta V_{\text{уи}} = \Delta V_{\text{уи}_B} + \Delta V_{\text{уи}_d}\,. \tag{14}$$

В рассматриваемом примере МтОР позволяет проанализировать влияние интенсивности следования NIT и RMT на периоде наблюдения 5 мин и для различных размеров таблиц. Исходные данные для расчета представлены в табл. 1. Результаты расчета с использованием МтОР представлены в табл. 2.

Результаты расчета свидетельствуют, что в первом и третьем варианте отклонение результативного показателя отрицательное, вначале следует анализировать таблицу NIT. Во втором и четвертом варианте отклонение результативного показателя положительное, большее влияние вносит фактор размера данных, в первую очередь следует анализировать данные управления, размещенные в таблице RMT.

Таблица 1. ***Исходные данные для расчета МтОР цифрового потока по определению управляющей информации***

Таблицы управления	Размер (байт)				Интенсивность следования (табл./мин)			
	Вариант				Вариант			
	1	2	3	4	1	2	3	4
NIT	450	150	450	150	6	6	3	3
RMT	150	450	150	450	3	3	6	6

Таблица 2. ***Результаты расчета цифрового потока с использованием МтОР по определению объема управляющей информации***

Показатель	Вариант			
	1	2	3	4
$\Delta V_{\text{уи}}$	−11 250	2 250	−2 250	11 250
$\Delta V_{\text{уи}B}$	−6 750	−2 250	6 750	2 250
$V_{\text{уи}d}$	−4 500	4 500	−9 000	9 000

В результате второй части исследований разработан МтОР по анализу данных цифровых потоков для определения объема данных управления с целью их актуализации в ГИС. При разработке использован математический и методологический аппарат детерминированного факторного анализа. Выбор модели (аддитивной, мультипликативной, смешанной) для проведения факторного анализа определяется рассматриваемым числом элементарных потоков и протоколов управляющей информации в цифровом потоке, а также уровней ЭМВОС на основе выражения, полученного в первой части исследования. Сущность метода заключается в принятии решения на основе использования результатов расчета относительных приростов факторных показателей (выраженных в виде коэффициентов или процентов). Введение коэффициентов особенно актуально в случае маркирования уровня или элементарного потока, содержащего мета и геоданные.

- В ходе проведенного исследования разработаны мультиплексная модель цифрового потока данных, транслируемых в инфокоммуникационных системах, и метод «относительных разниц» при определении и актуализации мета и геоданных для ГИС. Модель (выражение (4)) позволяет систематизировать знания о данных, передаваемых в потоках, рассчитывать эффективность использования емкости контейнера потока по передаче полезной нагрузки, синтезировать метод обработки цифровых потоков по определению управляющей информации, включая информацию геопозиционного характера, с использованием критерия полноты транслируемой управляющей информации. Метод «относительных разниц» позволяет определять и актуализировать мета и геоданные для ГИС. При этом используется математический и методологический аппарат детерминированного факторного анализа. Сущность метода заключается в принятии решения на основе использования результатов расчета относительных приростов факторных показателей, в основе которого лежат математические выражения разработанной модели цифрового потока данных, циркулирующих в инфокоммуникационной системе. Полученные в ходе исследований модель и метод позволяют также определять очередность обработки данных управления, оценивать количественный их объем, и, следовательно, обоснованно определять размер оперативной или постоянной памяти для хранения в базах данных ГИС.

Литература

1. *Вентцель Е.С.*, *Овчаров Л.А.* Теория вероятностей и ее инженерные приложения: Учеб. пособие для вузов. Изд. 2-е. М.: Высшая школа. 2000. 480 с.
2. *Кормен Томас Х., Лейзерсон Чарльз И., Ривест Рональд Л., Штайн Клиффорд* Алгоритмы: построение и анализ. Изд. 2-е. Пер. с англ. М.: Издательский дом «Вильямс». 2007. 1296 с.
3. *Айвазян С.А., Мхитарян В.С.* Прикладная статистика. Основы эконометрики: Теория вероятностей и прикладная статистика. Учебник для вузов: В 2-х томах. Т. 1. Изд. 2-е. М.: ЮНИТИ ДАНА. 2001. 656 с.
4. *Айвазян С.А.* Прикладная статистика. Классификация и снижение размерности. М.: Мир. 1989.
5. *Загоруйко Н.Г.* Прикладные методы анализа данных и знаний. Новосибирск: Изд-во института математики. 1999. 269 с.
6. ISO/IEC 13818 (6 частей): «Кодирование динамических изображений и звуковой информации». Женева: ISO.
7. ETSI EN 300 468: «Цифровое телевизионное вещание: сервисная информация в системах цифрового телевизионного вещания». Франция: ETSI. 2008. 111 с.
8. ETSI EN 301 790: «Цифровое телевизионное вещание (DVB): интерактивный канал для спутниковых систем доставки». Франция: ETSI. 2005. 117 с.
9. ETSI EN 302 307 v1.1.1: «Цифровое телевизионное вещание (DVB-S2): кадровая структура, канальное кодирование, модуляция, интерактивный сервис». Франция: ETSI. 2004. 74 с.
10. *Воронин А.В.*, *Иванов В.Н.*, *Сомов А.М.* Цифровое телевизионное и радиовещание: монография. В 3-х частях. Ч. 1. Цифровое телевизионное вещание / Под ред. д.т.н., проф. *А.М. Сомова*. М.: Горячая линия – Телеком. 2017. 255 с.
11. Comsys. The Comsys VSAT Report. England: «Communication Systems Limited». 2013. 1553 p.
12. *Голиков А.М.* Сети и системы радиосвязи и средства их информационной защиты: Учеб. пособие. Томск: Томск. гос. ун-т систем упр. и радиоэлектроники. 2007. 392 с.

13. *Hassan A. Karimi* Telegeoinformatics: Location-Based Computing and Services. USA: CRC Press LLC. 2004. 377 p.
14. Пат. РФ на полезную модель № 94785 от 27.05.2010. Устройство анализа сетевого трафика / *Воронин А.В., Иванов В.Н., Усовик С.В.*; 12 с.
15. *Черкасова И.О.* Анализ хозяйственной деятельности. СПб.: Издательский Дом «Нева». 2003. 192 с.
16. *Какке Л.А.*, *Кошевая И.П.* Анализ финансово-хозяйственной деятельности предприятия: Пособие. Изд. 2-е, испр. и доп. М.: ИД «ФОРУМ»: ИНФРА-М. 2007. 288 с.

Поступила ▮▮ ▮▮▮▮▮▮ 20▮▮ г.

The development of the method of «relative differences» when determining meta and geodata for GIS

© Authors, 2018
© Radiotekhnika, 2018

A.V. Voronin – Ph.D.(Eng.), Associate Professor, Leading Research Scientist,
FRC «Computer Science and Control» RAS (Moscow)
E-mail: aleksey.v.v@mail.ru

The article continues the thematic series of the articles devoted to the geoinformation systems (GISs), which considers the solution of the problem of developing the method of «relative differences» (MtRD) when determining meta and geodata for GIS, which differs from known by taking into account the control and management data circulating in infocommunication systems, marking meta and geodata, allowing to reduce the time and improve the efficiency of meta and geodata analysis broadcast in modern infocommunication systems. The model and method obtained during the research make it possible to determine the sequence of processing control data, to estimate the quantitative volume of these controls, and, consequently, to determine the size of operational or permanent memory for storage in GIS databases.

References

1. *Ventcel' E.S., Ovcharov L.A.* Teoriya veroyatnostej i ee inzhenernye prilozheniya [Theory of Probability and its Engineering Applications]: Ucheb. posobie dlya vuzov [tutorial for universities]. Izd. 2-e. M.: Vysshaya shkola [2nd ed. Moscow: Higher School]. 2000. 480 p.
2. *Kormen Thomas H., Leizerson Charl'z I., Rivest Ronald L., Shtajn Clifford* Algoritmy: postroenie i analiz [Algorithms: construction and analysis]. Izd. 2-e. Per. s angl. M.: Izdatel'skij dom «Vil'yams» [2nd ed. Trans. from English. M.: Publishing house «Williams»]. 2007. 1296 p.
3. *Ajvazyan S.A., Mhitaryan V.S.* Prikladnaya statistika. Osnovy ehkonometriki: Teoriya veroyatnostej i prikladnaya statistika. [Applied statistics. Fundamentals of Econometrics: Theory of Probability and Applied Statistics]. Uchebnik dlya vuzov. [Textbook for high schools]. V 2-h tomah. T. 1. Izd. 2-e. M.: YUNITI DANA. 2001. 656 p.
4. *Ayvazyan S.A.* Prikladnaya statistika. Klassifikaciya i snizhenie razmernosti [Applied statistics. Classification and reduction of dimensionality]. M.: Mir. 1989.
5. *Zagorujko N.G.* Prikladnye metody analiza dannyh i znanij [Applied methods of data and knowledge analysis]. Novosibirsk: Izd-vo instituta matematiki [Publishing house of the Institute of Mathematics]. 1999. 269 p.
6. ISO/IEC 13818 (6 chastej): Kodirovanie dinamicheskih izobrazhenij i zvukovoj informacii [Encoding of dynamic images and sound information]. Zheneva: ISO.
7. ETSI EN 300 468: Cifrovoe televizionnoe veshchanie: servisnaya informaciya v sistemah cifrovogo televizionnogo veshchaniya [Digital television broadcasting: service information in digital television broadcasting systems]. Francia [France]: ETSI. 2008. 111 p.
8. ETSI EN 301 790: Cifrovoe televizionnoe veshchanie (DVB): interaktivnyj kanal dlya sputnikovyh sistem dostavki [Digital television broadcasting (DVB): an interactive channel for satellite delivery systems]. Franciya [France]: ETSI. 2005. 117 p.
9. ETSI EN 302 307 v1.1.1: Cifrovoe televizionnoe veshchanie (DVB-S2): kadrovaya struktura, kanal'noe kodirovanie, modulyaciya, interaktivnyj servis [Digital television broadcasting (DVB-S2): frame structure, channel coding, modulation, interactive service]. Franciya [France]: ETSI. 2004. 74 p.
10. *Voronin A.V., Ivanov V.N., Somov A.M.* Cifrovoe televizionnoe i radioveshchanie: monografiya [Digital television and radio broadcasting: monograph]. V 3-h chastyah. Ch. 1. Cifrovoe televizionnoe veshchanie [Digital television broadcasting] / Pod red. d.t.n., prof. *A.M. Somova* [Under the editorship of Professor *A.M. Somov*, PhD in Technical Sciences]. M.: Goryachaya liniya – Telekom [Moscow: Hot line – Telecom]. 2017. 255 p.
11. Comsys. Otchet VSAT Comsys [The Comsys VSAT Report]. Angliya [England]: OOO Kommunikacionnye sistemy [Communication Systems Limited]. 2013. 1553 p.
12. *Golikov A.M.* Seti i sistemy radiosvyazi i sredstva ih informacionnoj zashchity [Networks and systems of radio communication and means of their information protection]: Ucheb. posobie [textbook. manual]. Tomsk: Tomsk. gos. un-t sistem upr. i radioehlektroniki [Tomsk State University of Control and Radioelectronics]. 2007. 392 p.
13. *Hassan A. Karimi* Telegeoinformatika: vychisleniya i servisy dlya ukazaniya tekushchego mestopolozheniya [Telegeoinformatics: Location-Based Computing and Services]. USA: CRC Press LLC. 2004. 377 p.
14. Pat. RF na poleznuyu model' [Network traffic analysis device. Patent for utility model] № 94785 ot [dated] 27.05.2010. Ustrojstvo analiza setevogo trafika / *Voronin A.V., Ivanov V.N., Usovik S.V.*; 12 p.
15. *Cherkasova I.O.* Analiz hozyajstvennoj deyatel'nosti [Analysis of economic activity]. SPb: Izdatel'skij Dom «Neva» [St. Petersburg: Publishing House «Neva»]. 2003. 192 p.
16. *Kakke L.A., Koshevaya I.P.* Analiz finansovo-hozyajstvennoj deyatel'nosti predpriyatiya [Analysis of the financial and economic activities of the enterprise]: Posobie. Izd. 2-e., ispr. i dop. [Textbook. 2nd ed., rev. and additional]. M.: ID «FORUM»: INFRA-M. 2007. 288 p.

УДК 004.6.056: 004.75

Реализация инфраструктуры процессинга цифровых активов

© Авторы, 2018
© ООО «Издательство «Радиотехника», 2018

А.В. Домашев – начальник отдела, НТЦ «Атлас» (Москва)
E-mail: domix@stcnet.ru
А.Ю. Щербаков – д.т.н., профессор, гл. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: x509@ras.ru

Предложено понятие инфраструктуры процессинга цифровых активов (ИПЦА). Изложены основные принципы и подходы к процессингу цифровых активов в рамках проектов федеральных законов и подходов к регулированию криптовалют.

Ключевые слова: *криптовалюта (КВ), цифровые активы (ЦА), электронная подпись (ЭП), удостоверяющий центр (УЦ), криптовалютный кошелек (КВК), инфраструктура процессинга цифровых активов (ИПЦА).*

The concept of digital asset processing infrastructure is proposed, the basic principles and approaches to digital asset processing within the framework of Federal laws and approaches to cryptocurrency regulation are outlined.

Keywords: *cryptocurrency (CC), digital assets (DA), electronic signature (DS), the certification authority (CA), cryptocurrency wallet (CW), infrastructure processing of digital assets (IPDA).*

Массовое применение новых финансовых технологий, включая общедоступные цифровые активы (криптовалюты), порождает для национальной экономики целый ряд проблем, среди которых, в первую очередь, неподконтрольность государству процессов обращения денежных средств, снижение собираемости налогов, возможность «отмывания» денег и финансирования незаконных бизнесов, запрещенных общественных и политических организаций, и, как следствие, дестабилизация экономических и политических процессов на национальном уровне.

Кроме того, необходимо отметить, что вовлечение граждан и организаций в уже сложившиеся процессы оборота и использования криптовалют зарубежного происхождения делают возможным вмешательство других стран, обладающих значительной массой криптовалюты, либо имеющих возможность ее производства (майнинга), в отечественные финансовые рынки также с целью их дестабилизации, создания панических тенденций и негативного влияния на политическую и общественную жизнь.

В соответствии с проектом ФЗ «О цифровых финансовых активах» (внесен Министерством Финансов РФ 25.01.18) [1] вводится понятие «цифровой финансовый актив» – это имущество в электронной форме, созданное с использованием шифровальных (криптографических) средств. Права собственности на данное имущество удостоверяются путем внесения цифровых записей в реестр цифровых транзакций. К цифровым финансовым активам относятся криптовалюта и токен. Закон определяет, что цифровые финансовые активы не являются законным средством платежа на территории РФ. В нижеследующем тексте понятие «токен» используется не в том смысле, в котором его определяет федеральный закон.

Далее проект вводит понятие оператора обмена цифровых финансовых активов – это юридическое лицо, осуществляющее сделки по обмену цифровых финансовых активов одного вида на цифровые финансовые активы другого вида и/или по обмену цифровых финансовых активов на рубли или иностранную валюту.

Операторами обмена цифровых финансовых активов согласно проекту ФЗ могут быть только юридические лица, которые созданы в соответствии с законодательством РФ и осуществляют виды деятельности, указанные в статьях 3−5 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг», или юридические лица, являющиеся организаторами торговли в соответствии с Федеральным законом от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах».

Кроме того, согласно терминам, предлагаемым в проекте, вводится понятие «цифровой кошелек» – это программно-техническое средство, позволяющее хранить информацию о цифровых записях и обеспечивающее доступ к реестру цифровых транзакций.

Цифровой кошелек открывается оператором обмена цифровых финансовых активов только после прохождения процедур идентификации его владельца в соответствии с Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных пре-

ступным путем, и финансированию терроризма». В предлагаемой ниже концепции цифровой кошелек фигурирует в виде «криптовалютного кошелька» (КВК). Требование процедур идентификации владельца предопределяет необходимость описанных ниже процедур по формированию инфраструктуры процессинга цифровых активов (ИПЦА), связанных с выпуском соответствующих сертификатов. Предлагаемый подход опирается на концепцию изолированной криптовалютной сети, изложенную в [2].

Ц е л ь р а б о т ы – рассмотреть основные принципы и подходы к процессингу цифровых активов в рамках проектов федеральных законов и подходов к регулированию криптовалют.

Терминология

Перед тем как перейти к подробному рассмотрению протокола ИПЦА, зафиксируем общие и специальные используемые термины и сокращения.

Общие термины и сокращения: ЭП – электронная подпись; HSM – Hardware Security Module; УЦ – удостоверяющий центр; БД – база данных.

Специальные термины и сокращения: ИПЦА – инфраструктура процессинга цифровых активов; ЦПЦА – центр процессинга цифровых активов; ГУЦ – головной УЦ; КВ – криптовалюта (вид цифрового финансового актива); КВК – криптовалютный кошелек; ОКВК – оператор КВК; УЦ УК – УЦ управления клиентами; КВС – криптовалютная сеть; АВ КВК – агент восстановления КВК; БД АВ КВК – база данных агента восстановления КВК.

Концепция инфраструктуры процессинга цифровых активов

В соответствии со статьей 4 проекта Федерального закона «Особенности обращения цифровых финансовых активов» владельцы цифровых финансовых активов вправе совершать сделки по обмену цифровых финансовых активов одного вида на цифровые финансовые активы другого вида и/или по обмену цифровых финансовых активов на рубли, иностранную валюту и/или иное имущество *только через оператора обмена цифровых финансовых активов*.

Таким образом, описана схема, в рамках которой должны работать аккредитованные биржи криптовалют (операторы обмена цифровых активов). Уже существующие биржи при их желании обслуживать российских клиентов в соответствии с федеральным законом должны будут «встроиться» в ИПЦА.

Описываемая схема дает возможность уже действующим авторитетным биржам работать на российском рынке, при этом работа с КВК (ЦК) полностью контролируется.

Предложения по реализации инфраструктуры процессинга цифровых активов

В данном разделе представлена концепция реализации ИПЦА. Информация в этом разделе представляет собой описание подхода к решению данной задачи и не учитывает многие вопросы практической реализации, которые рассмотрены в следующих разделах.

Кроме того, в представленной схеме аутентификация и авторизация конечных пользователей базируется исключительно на сертификатах и разрешениях, которые соответствующий УЦ включит в них. Данная модель является статической в том смысле, что не позволяет динамически управлять разрешениями конечных пользователей, и поэтому на практике может быть не достаточной и тогда необходимо реализовать более гибкие модели управления.

В процессе описания схемы работы ИПЦА будут рассмотрены различные подходы к тому факту, известен ли конечному пользователю его реальный адрес в среде криптовалюты.

П е р в ы й п о д х о д заключается в том, что, несмотря на то, что он не может воспользоваться самостоятельно секретных ключом КВК, реальный адрес КВК конечному пользователю известен (это означает, что ему известен открытый ключ КВК).

В т о р о й п о д х о д заключается в том, что конечному пользователю не известен и открытый ключ КВК, то есть он не знает и адреса КВК, которым он управляет.

Выбор того или иного подхода определяется исключительно характеристиками деятельности, которую хочет организовать ЦПЦА. Однако очевидно, что знание пользователем его реального адреса оказывает прямое влияние на характеристики анонимности в среде ИПЦА.

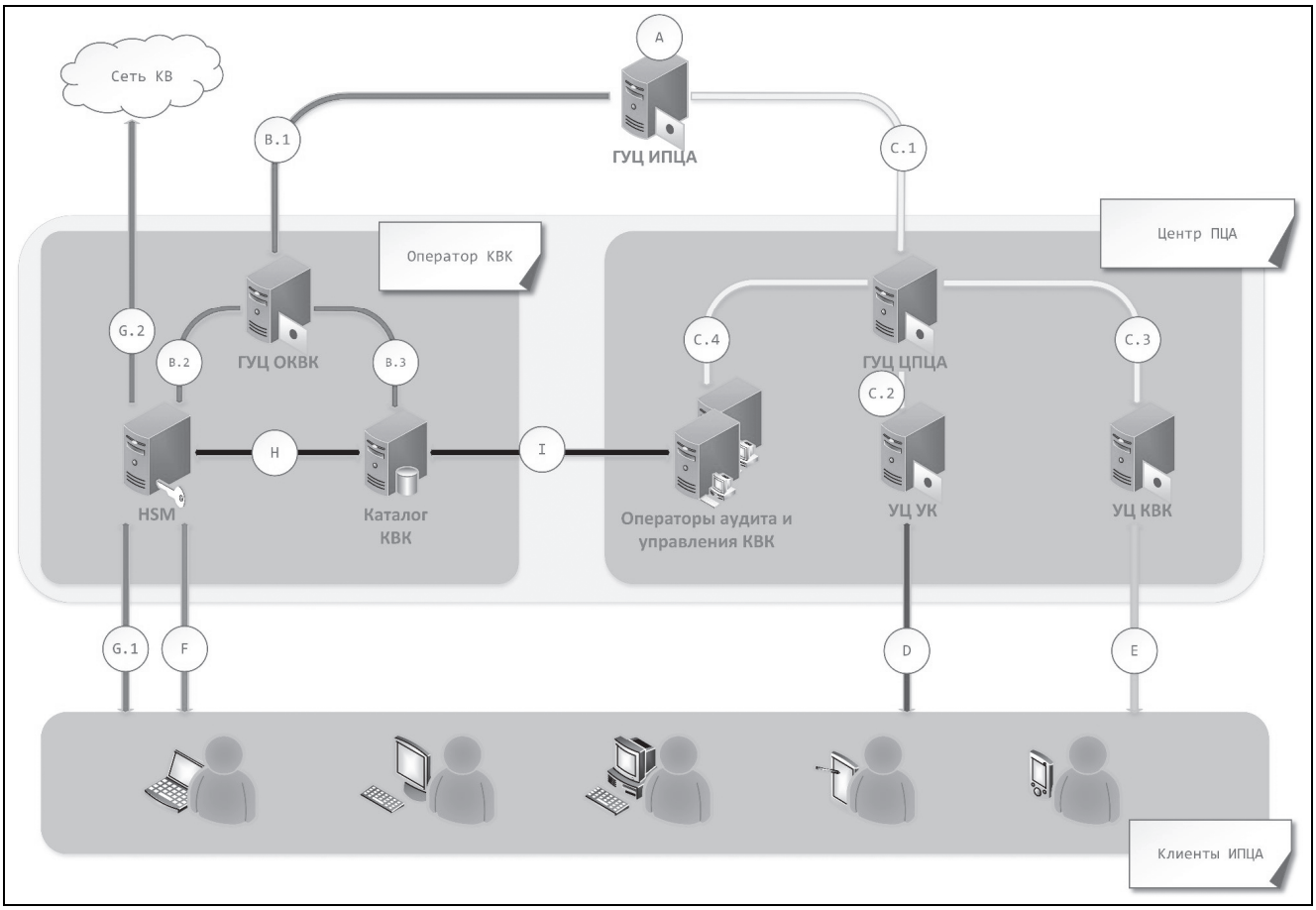


Схема ИПЦА

Общая схема предлагаемой ИПЦА приведена на рисунке. Рассмотрим основные этапы инициализации и работы ИПЦА.

Этап A. *Инициализация ГУЦ ИПЦА.*

ГУЦ ИПЦА может быть связан с органами «Роскрипторегулирования», либо с другим органом, регулирующим деятельность операторов цифровых активов.

Этап B. *Инициализация ОКВК.*

Инициализация ОКВК начинается с получения его ГУЦ сертификата (ccw_op_head_ca_cert) у ГУЦ ЦПЦА (шаг B.1). Шаг B.1 является регистрацией нового ОКВК в системе.

ОКВК (см. рисунок) состоит из двух основных элементов: ГУЦ и HSM. Для завершения инициализации ОКВК HSM генерирует секретный ключ (ccw_op_hsm_private_key) и получает сертификат (ccw_op_hsm_cert) открытого ключа у своего ГУЦ (шаг B.2).

Этап C. *Инициализация ЦПЦА.*

Инициализация ЦПЦА, как и ОКВК, начинается с получения его ГУЦ сертификата (dapc_op_head_ca_cert) у ГУЦ ЦПЦА (шаг C.1). Шаг C.1 является регистрацией нового ЦПЦА в системе.

ЦПЦА (см. рисунок) состоит из четырех основных элементов: ГУЦ, УЦ УК, УЦ КВК и БД АВ КВК. Для завершения инициализации УЦ УК и УЦ КВК запрашивают сертификаты открытых ключей (dapc_op_end_user_ca_cert и dapc_op_ccw_ca_cert), необходимых для их активации (шаг C.2 и C.3 соответственно).

После активации всех УЦ инициализируется БД операторов восстановления. Для этого оператор (операторы) восстановления генерируют секретные ключи и запрашивают сертификаты открытых ключей у своего ГУЦ (шаг C.4).

Этап D. *Регистрация клиента в ЦПЦА.*

Этап регистрации, как и в остальных случаях, представляет собой запрос и получение сертификата (end_user_dapc_cert) у ЦПЦА. Обработку этих запросов в рамках ЦПЦА ведет УЦ УК (см. рисунок). Таким образом, клиент получает сертификат открытого ключа с включенными в него разрешениями (end_user_dapc_perms), который в дальнейшем он будет использовать для аутентификации при обращении к сервисам ИПЦА.

Какие данные клиент должен предъявить для получения сертификата, а также какие данные будут внесены в его сертификат, зависит от политики соответствующего ЦПЦА. Кроме этого, важным моментом, который должен определить ЦПЦА, являются параметры доступа к каталогу сертификатов. Будет ли он публичным, доступным только аутентифицированным клиентам или закрытым, также определяется текущей политикой.

Э т а п E . *Получение сертификата КВК.*

К настоящему моменту клиент, зарегистрировавшись в ЦПЦА и получив соответствующий сертификат, имеет возможность обращаться к сервисам ИПЦА.

Поскольку в рамках ИПЦА клиент работает с КВК посредством ОКВК и не владеет секретным ключом кошелька, то для идентификации КВК предлагается использовать специальный сертификат, к которому ОКВК и будет привязывать реальный КВК и на котором будет производиться шифрование и ЭП информации, связанной с этим кошельком. Кроме того, использование для каждого КВК отдельного сертификата позволит ЦПЦА проводить в случае необходимости целевую блокировку кошелька просто путем отзыва соответствующего сертификата.

Таким образом, на этом этапе клиент обращается к УЦ КВК, проходит аутентификацию и запрашивает сертификат КВК (end_user_ccw_cert). Аутентификация может быть проведена по протоколу TLS с использованием штатной возможности клиентской аутентификации. При обращении за сертификатом КВК клиент может указать разрешения (end_user_ccw_perms), которые он хотел бы получить. Например, тип криптовалюты, максимальный объем кошелька, возможность обращения к внешним шлюзам ИПЦА и др. Конкретный перечень разрешений сертификата и требования к его получению определяются политикой ЦПЦА.

После успешного получения сертификата КВК клиент может обращаться с запросами к ОКВК.

Э т а п F . *Подключение реального КВК к сертификату клиента.*

На этом этапе клиент обращается к соответствующему ОКВК для создания для него КВК. Запрос подписывается на сертификате, полученном от ЦПЦА на этапе E. Таким образом, ОКВК имеет возможность проверить полномочия клиента для создания КВК.

После проверки валидности запроса HSM оператора создает (или использует уже созданную) ключевую пару КВК (ccw_private_key и ccw_public_key). Из открытого ключа формируется токен открытого ключа (ccw_public_key_token), а из секретного ключа – токен секретного ключа (ccw_private_key_token).

Токен ccw_private_key_token получается путем шифрования и подписи ccw_private_key на сертификате оператора КВК ccw_op_hsm_cert, полученном на этапе B (шаг B.2). В состав токена также входит идентификатор сертификата конечного пользователя end_user_ccw_cert_id. Включение идентификатора необходимо, чтобы ОКВК мог при обращении проверить соответствие идентификатора сертификата конечного пользователя, который к нему обратился, и идентификатора сертификата из токена.

Токен ccw_public_key_token также может быть получен путем шифрования и подписи на сертификате ОКВК ccw_op_hsm_cert, если есть необходимость в скрытии от клиента реального адреса КВК. В противном случае достаточно только подписи. В состав ccw_public_key_token также входит идентификатор сертификата end_user_ccw_cert_id.

После этого оба токена (ccw_private_key_token и ccw_public_key_token) направляются клиенту в ответ на его запрос.

Таким образом, после этого шага клиент владеет всей необходимой информацией для осуществления криптовалютных транзакций в ИПЦА.

Э т а п G . *Проведение транзакции для КВК.*

Теперь для проведения транзакции клиенту необходимо сформировать параметры транзакции и подписать запрос сертификатом end_user_ccw_cert, полученным на этапе E.

Для формирования транзакции конечный пользователь должен по соответствующим каналам получить целевые адреса в виде токенов ccw_public_key_token. Получить он их может в результате непо-

средственного взаимодействия с другими пользователями (например, по электронной почте) или ЦПЦА может предусмотреть какой-либо общедоступный каталог для размещения такой информации (например, непосредственно в свойствах сертификатов в каталоге УЦ КВК).

Получив запрос, ОКВК проводит следующие действия (ш а г G . 2):

1) проверяет валидность подписи запроса;

2) расшифровывает (если необходимо) ccw_public_key_token отправителя транзакции;

3) проверяет подпись ccw_public_key_token отправителя транзакции;

4) расшифровывает ccw_private_key_token отправителя транзакции и получает секретный ключ КВК ccw_private_key;

5) проверяет подпись ccw_private_key_token отправителя транзакции;

6) расшифровывает (если необходимо) ccw_public_key_token получателей транзакции;

7) проверяет подпись ccw_public_key_token получателей транзакции;

8) проверяет валидность сертификатов end_user_ccw_cert получателей транзакции;

9) проверяет валидность сертификатов end_user_dapc_cert получателей транзакции;

10) формирует и подписывает запрашиваемую транзакцию на ключе ccw_private_key отправителя транзакции;

11) отправляет транзакцию в сеть соответствующей криптовалюты;

12) отправляет конечному пользователю подписанное подтверждение проведения транзакции.

Таким образом, представленная схема гарантирует, что конечные пользователи ИПЦА имеют возможность передавать транзакции только другим зарегистрированным пользователям ИПЦА.

После приведения описания работы ИПЦА должно стать более понятным предложенное ранее деление «полнофункционального» ЦПЦА (серая область на рисунке) на два независимых компонента: собственно ЦПЦА и ОКВК. В области ОКВК собраны компоненты, работающие непосредственно с транзакциями конечных пользователей и криптовалютными средами. Организация, заинтересованная в создании для каких-либо целей ЦПЦА, может и не иметь таких специфических компетенций. Задача «малого» ЦПЦА – это управление подключением конечных пользователей к ИПЦА. Кроме того, введение дополнительного независимого оператора, безусловно, повышает и уровень доверия конечных пользователей к системе в целом.

И еще одно замечание в отношении ОКВК. Как можно заметить из приведенного описания, ОКВК не хранит результатов своих операций. Результаты всем проведенных им операций отправляются или конечным пользователям, или в криптовалютную сеть. Это очень выгодное свойство с точки зрения простоты реализации HSM и оператора в целом. Однако, конечно, возможности такой реализации могут не удовлетворить запросы организатора ЦПЦА.

В следующих разделах рассматриваются дополнительные компоненты ИПЦА, которые позволяют динамически управлять разрешениями конечных пользователей.

Дополнительные компоненты инфраструктуры процессинга цифровых активов

При описании базовых принципов функционирования ИПЦА, изложенных в предыдущем разделе, были для упрощения опущены несколько важных компонентов. Этими компонентами являются каталог КВК, а также операторы аудита и управления (см. рисунок).

Как уже отмечалось, «статическая» модель управления разрешениями, в которой разрешения конечных пользователей хранятся в сертификате и могут быть изменены только перевыпуском соответствующего сертификата, не всегда может удовлетворить запросы ЦПЦА. Таким образом, для хранения каталога конечных пользователей, связанных с ними КВК и соответствующих разрешений вводится компонент каталог КВК. Со стороны ЦПЦА текущими разрешениями, хранящимися в каталоге, управляет оператор управления КВК.

В связи с введением новых компонент этап F может быть дополнен шагом H (см. рисунок) на котором будут проверены текущие разрешения конечного пользователя на проведение запрошенной транзакции.

Помимо управления разрешениями, ЦПЦА, безусловно, может быть заинтересован в текущем аудите транзакций конечных пользователей. Для этого оператор аудита КВК может также обратиться

в каталог КВК и, получив соответствующую информацию, проводить аудит целевой криптовалютной сети.

ЦПЦА может быть заинтересован в том, чтобы при необходимости проводить операции с КВК конечных пользователей. Это может быть, прежде всего, связано с необходимостью обеспечения возможности возвращения средств транзакции, признанной по каким-либо причинам недействительной. Для этого оператор администрирования КВК должен иметь доступ к секретным ключам КВК. Наиболее очевидная схема реализации данного требования – это дополнение этапа F шагом создания токена секретного ключа, зашифрованного на сертификате оператора администрирования КВК, полученном на шаге С.4 (см. рисунок). Этот токен может быть, в зависимости от требований оператора, сохранен в каталог КВК или напрямую передан ЦПЦА для хранения и использования.

Таким образом, дополненная компонентами каталога КВК и операторами аудита и администрирования ИПЦА приобретает возможности динамического управления разрешениями при работе с КВК, аудита пользовательских транзакций и возвращения полностью или частично уже проведенных транзакций.

- Предлагаемая схема позволяет в полной мере учесть интересы государства в формируемой инфраструктуре обслуживания цифровых финансовых активов. При выдаче сертификата клиенту будет проводиться его обязательная аутентификация, операции с КВК регистрируются и управляются путем управления соответствующими сертификатами, кроме того, возможна легитимная отмена транзакций.

  Данная схема также позволит выполнить условия проекта федерального закона и обеспечить централизованное подключение бирж криптовалюты и контроль их работы в рамках обслуживания российских клиентов, а также сбор необходимой информации для противодействия отмыванию доходов (в соответствии с № 115-ФЗ) и начисления необходимых налоговых выплат.

  В РАН разработаны уникальные технологии, позволяющие реализовать описанные выше процедуры контроля и управления движением цифрового актива с возможностью применения привычных финансовых и бухгалтерских практик для криптовалют.

Литература

1. Проект ФЗ «О цифровых финансовых активах» (внесен Министерством Финансов РФ 25.01.18). URL = https://www.minfin.ru/ru/document/?id_4=121810.
2. *Домашев А.В.*, *Щербаков А.Ю.* Синтез универсальной изолированной криптовалютной сети // Системы высокой доступности. 2017. Т. 13. № 4. С. 31–38.

Поступила ■■ ■■■■■■ 20■■ г.

Implementation of the infrastructure processing digital assets

© Authors, 2018
© Radiotekhnika, 2018

A.V. Domashev – Head of Department, STC «Atlas» (Moscow)
E-mail: domix@stcnet.ru
A.Yu. Scherbakov – Dr.Sc.(Eng.), Professor, Main Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: x509@ras.ru

The concept of digital asset processing infrastructure is proposed, the basic principles and approaches to digital asset processing within the framework of Federal laws and approaches to cryptocurrency regulation are outlined. The RAS has developed unique technologies that make it possible to implement the described procedures for controlling and controlling the movement of a digital asset with the possibility of applying the usual financial and accounting practices for crypto-currencies.

References

1. Proekt FZ «O czifrovy'x finansovy'x aktivax» (vnesen Ministerstvom Finansov RF 25.01.18). URL = https://www.minfin.ru/ru/document/?id_4=121810.
2. *Domashev A.V.*, *Shherbakov A.Yu.* Sintez universal'noj izolirovannoj kriptovalyutnoj seti // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 4. S. 31–38.

УДК 004.383.5

Подход и системно-технические решения по построению систем видеоотображения повышенной доступности и высокой информационной емкости

© Авторы, 2018
© ООО «Издательство «Радиотехника», 2018

Е.С. Агафонов – гл. специалист, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: eagafonov@ipiran.ru
Э.Р. Корепанов – к.т.н., зав. отделом, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: ekorepanov@ipiran.ru
В.С. Шоргин – к.т.н., ст. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: vshorgin@ipiran.ru

Показано, что программно-управляемые видеоконтроллеры позволяют в полной мере использовать потенциал современного видеооборудования за счет возможности доработки управляющего программного обеспечения (ПО). Рассмотрена возможность построения системы видеоотображения на базе программно согласованных видеоконтроллеров с целью оптимизации стоимости решения и повышения доступности.

Ключевые слова: *программно-управляемый видеоконтроллер, система видеоотображения повышенной доступности, экономически-эффективный видеоконтроллер.*

Software-based video controllers make it possible to take full advantage of the modern video equipment capacity due to the possibility of the control software improvement. The article considers the possibility of creating a video wall system based on software-coordinated video controllers in order to optimize the cost of the solution and increase its availability.

Keywords: *software-based video wall controller, high-availability video wall, Cost-Effective video controller.*

Данная статья открывает тематический цикл, посвященный вопросам рационального построения современных и перспективных систем видеоотображения высокой информационной емкости. Как известно [1], при решении задач построения систем видеоотображения высокой информационной емкости используют видеостену, которая представляет собой единый экран коллективного пользования, собранный из нескольких независимых устройств отображения информации (LCD-панели, светодиодные экраны, проекторы, кубы и т.д.). Для объединения экранов видеостены в единое информационное видеопространство используют контроллеры видеостены (видеоконтроллеры).

Видеоконтроллер – это специализированное устройство, предназначенное для приема, обработки, отображения и управления мультимедийной информацией на видеостене. Фактически, видеоконтроллер позволяет объединить различные устройства отображения информации в единое информационное пространство – сделать единую рабочую область без какой-либо жесткой привязки к конкретным устройствам отображения и к их фактическим габаритным размерам. Видеоконтроллер комплектуется видеокартами (для подключения источников отображения информации), картами видеозахвата (для подключения физических источников видеосигнала) и картами аппаратного декодирования IP-потоков (для захвата и декодирования IP-потоков), которые размещаются на единой высокопроизводительной шине передачи данных (рис. 1).

Одной из важных характеристик видеоконтроллеров является число видеовыходов, то есть число видеопанелей, которые могут быть к нему подключены для образования единого видеопространства. Числом видеовыходов видеоконтроллера определяется, какой размерности видеостена может им обслуживаться. Например, для видеостены размерностью 6×4 потребуется видеоконтроллер с не менее чем 24-мя видеовыходами.

Видеоконтроллер – довольно дорогостоящее изделие, стоимость которого растет ступенчато-экспоненциально в зависимости от числа видеовыходов. Это обусловлено тем, что чем больше видеовыходов должен обслуживать видеоконтроллер, тем более высокие требования предъявляются к его основным элементам – видеокартам, шине передачи данных и управляющей инфраструктуре. Простые (и, соответственно, недорогие) видеокарты имеют ограниченные производителем возможности (например, совместная работа в контроллере только двух видеокарт) и не могут обеспечивать облуживание ви-

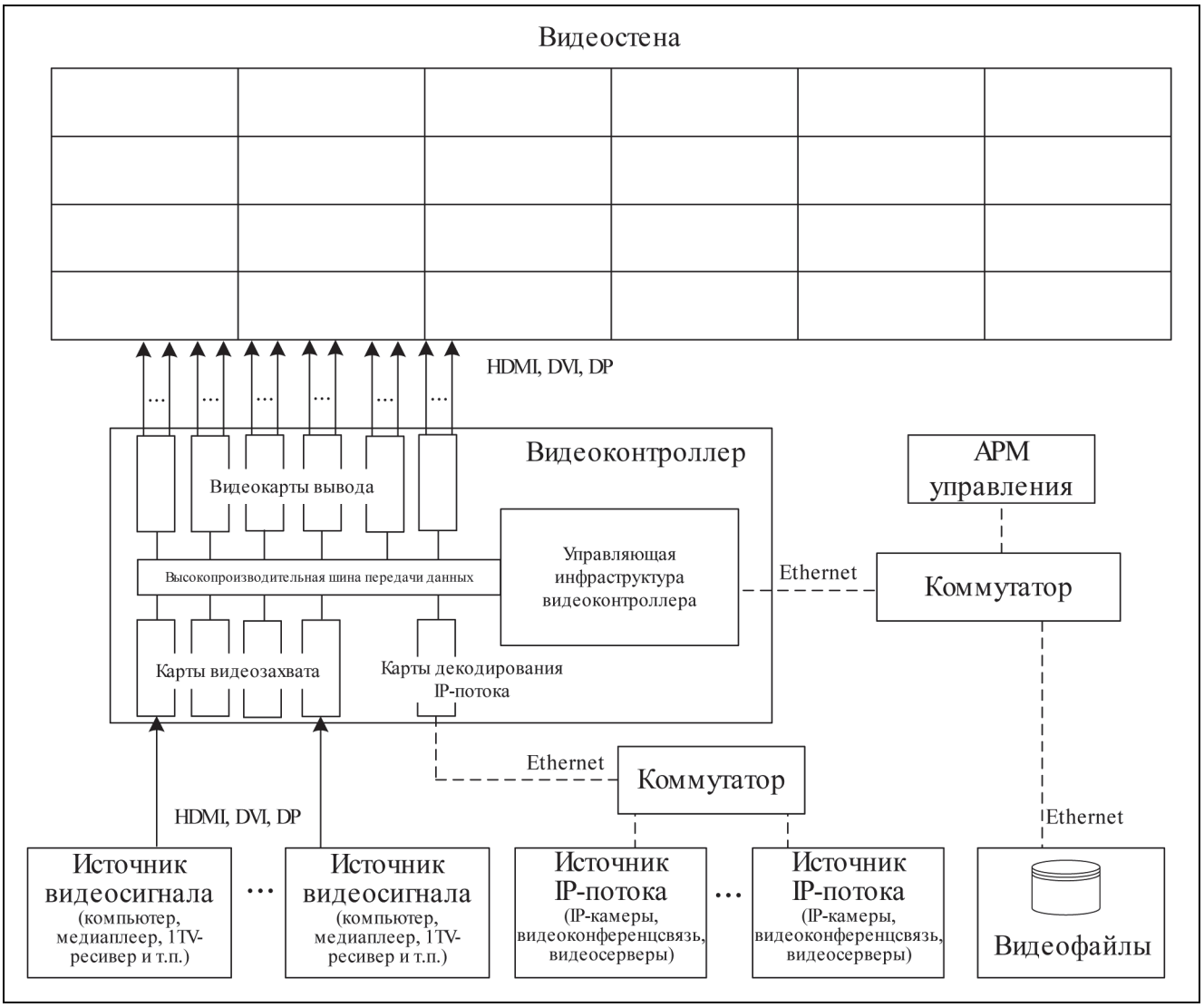


Рис. 1. Типовая архитектура системы отображения информации с применением видеоконтроллера

деостен высокой размерности. Видеокарты большей производительности и без существенных ограничений на устанавливаемое число в одном контроллере существенно дороже. Например [2], при использовании видеокарт одного из ведущих мировых производителей видеооборудования – Matrox Graphics – единый видеоконтроллер с 24-мя видеовыходами обходится значительно дороже, чем два отдельных видеоконтроллера с суммарно теми же 24-мя видеовыходами. Возможность комбинирования различных плат на нескольких контроллерах открывает перспективы выбора рационального подхода к построению системы видеоотображения. Таким образом, имеет место фактор нелинейного роста стоимости видеоконтроллера.

При построении видеостен большой размерности (4×4 и выше) совместное использование нескольких сравнительно недорогих видеоконтроллеров потенциально является более предпочтительным, нежели использование одного дорогостоящего видеоконтроллера с большим числом видеовыходов. Проблема реализации данной схемы заключается в том, что два (и более) автономных видеоконтроллера не могут формировать единое видеопространство (выводить общий контент на всю видеостену). Каждый видеоконтроллер может обслуживать только непосредственно подключенные к нему видеопанели (свою зону ответственности). С использованием штатного программного обеспечения (ПО) производителей видеокарт согласовать работу нескольких видеоконтроллеров и «развернуть картинку» на всю видеостену не получится, а данная возможность является определяющей для создания единого информационного пространства.

Ц е л ь р а б о т ы – обеспечить согласованную работу в едином информационном пространстве нескольких недорогих видеоконтроллеров, обслуживающих общую видеостену.

Для достижения указанной цели необходимо:

1) реализовать программное управление, которое будет координировать выводимый видеоконтроллерами сигнал для формирования целостного изображения на видеостене;

2) обеспечить все видеоконтроллеры системы единым контентом вне зависимости от того, какую часть этого контента отображает тот или иной видеоконтроллер;

3) синхронизировать выводимый разными видеоконтроллерами контент.

В качестве примера рассмотрим видеостену, состоящую из 24-х видеопанелей и обслуживаемую двумя видеоконтроллерами. При этом первые 12 видеопанелей подключены к первому видеоконтроллеру, а вторые 12 – ко второму (рис. 2).

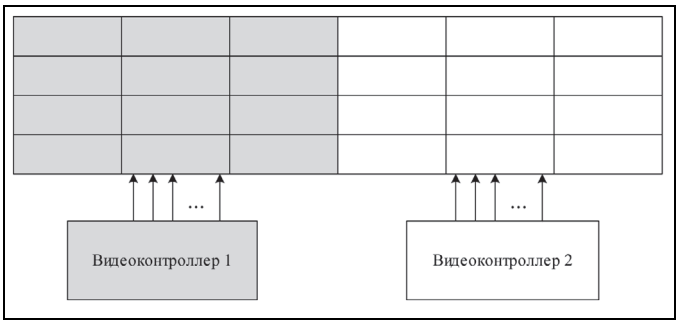


Рис. 2. Схема видеостены, обслуживаемой двумя видеоконтроллерами

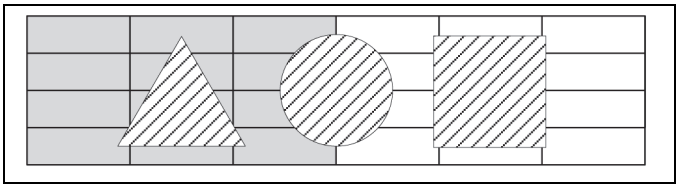


Рис. 3. Размещение контента на едином информационном пространстве

В зависимости от размещения на видеостене контент может обрабатываться:

только одним из видеоконтроллеров, если полностью умещается на обслуживаемых им панелях (изображения треугольника и квадрата на рис. 3);

сразу несколькими видеоконтроллерами, если разные части «картинки» попадают в зоны ответственности разных видеоконтроллеров (изображение круга на рис. 3).

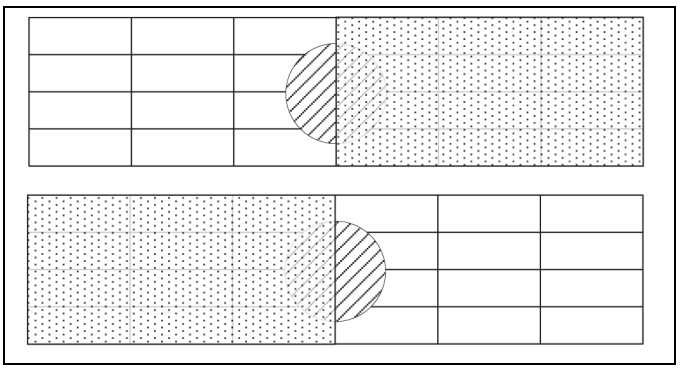


Рис. 4. Контент, формируемый каждым из видеоконтроллеров в отдельности

П е р в ы й в а р и а н т не требует специального рассмотрения, так как в этой ситуации весь функционал отображения выполняется одним видеоконтроллером и координация с другими видеоконтроллерами не требуется.

В о в т о р о м в а р и а н т е каждый из видеоконтроллеров отображает на видеостене только «свою» часть общего контента. Точнее, видеоконтроллер выдает на видеовыходы полную «картинку», но часть ее, выходящая за пределы зоны ответственности, в реальности не отображается (рис. 4).

При этом необходимо обеспечить, чтобы весь совместно отображаемый контент был доступен всем видеоконтроллерам.

Задачей управляющей программы является выдача видеоконтроллерам команд позиционирования контента таким образом, чтобы для наблюдателя они объединялись в единую цельную согласованную «картинку».

В зависимости от вида контента требуются различные способы его согласованного отображения несколькими видеоконтроллерами.

Статическое изображение. На видеостене отображается графический файл одного из поддерживаемых форматов, сохраненный на жестком диске видеоконтроллера, подключенного к нему съемного носителя или на файловом сервере. Это наименее проблемный тип контента, так как он, в силу статичности, не требует синхронизации между участвующими в его отображении видеоконтроллерами. Необходимо лишь обеспечить наличие на всех видеоконтроллерах отображаемого графического файла.

Цифровой видеосигнал. На видеостене отображается видеосигнал от цифрового источника, которым могут являться компьютеры, медиаплееры, TV/SAT-ресиверы и т.п. Подключение осуществляется с ис-

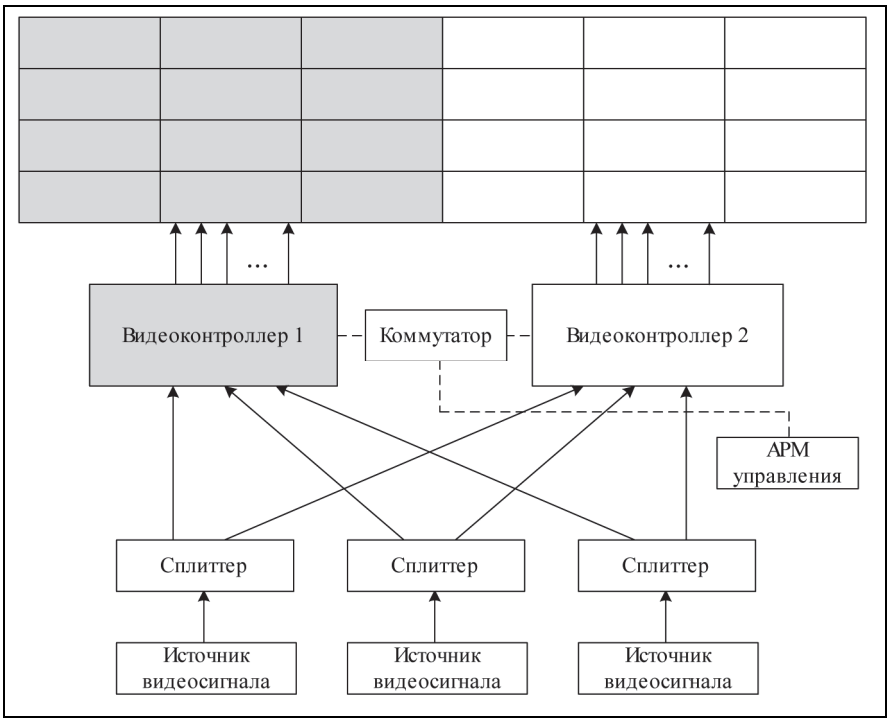


Рис. 5. Схема подключения видеоисточников к нескольким видеоконтроллерам

пользованием распространенных интерфейсов HDMI, DisplayPort, DVI. Возможно подключение устаревших аналоговых сигналов с использованием аналого-цифрового преобразователя. Особенностью данного типа контента является то, что он обрабатывается либо на аппаратном уровне картами видеозахвата видеоконтроллера, либо соответствующими драйверами на очень низком программном уровне. Благодаря этому обработка и последующее отображение «картинки» происходят практически в режиме реального времени и не подвержены воздействиям других процессов, выполняемых операционной системой видеоконтроллера. Для согласованного отображения одного видеосигнала несколькими видеоконтроллерами необходимо, чтобы данный сигнал поступал идентичным образом на физические видеовходы всех видеоконтроллеров. Поэтому для данного типа контента предлагается использование разветвителей сигнала (сплиттеров), дублирующих поступающий исходный видеосигнал сразу на все видеоконтроллеры (рис. 5).

Видеофайл. На видеостене с помощью программного проигрывателя воспроизводится видео из локального видеофайла или от транслируемого по сети источника. Особенностью воспроизведения данного типа контента является использование центрального процессора для обработки (декодирования) поступающих видеоданных. Как известно, центральный процессор постоянно выполняет множество различных задач (в том числе служебных, запускаемых по расписанию или при простое). В связи с этим время, затрачиваемое в данный момент времени на обработку видеосигнала центральными процессорами на разных видеоконтроллерах, может различаться. В результате при совместном использовании нескольких видеоконтроллеров для отображения данного типа контента может возникать явление рассинхронизации: «картинка», выдаваемая одним, менее загруженным видеоконтроллером, опережает «картинку» другого видеоконтроллера, на котором запустился процесс, потребляющий существенные вычислительные ресурсы.

Бороться с этим явлением достаточно сложно. Очевидно, имеет смысл отключить на видеоконтроллерах задачи обслуживания операционной системы (ОС), потребляющие существенные ресурсы: автоматическое обновление ОС и других приложений, периодическая проверка системы антивирусной программой, индексация файлов на дисках и др. Кроме того, аппаратная часть видеоконтроллеров должна быть идентичной и подобранной с определенным запасом по производительности, чтобы по возможности исключить задержки при обработке видеоданных.

Однако указанные меры все равно не гарантируют полной синхронности в отображении видеофайлов. Поэтому необходимо предусмотреть периодическую отправку синхронизирующей команды, период которой можно подобрать в зависимости от характера и периода отображаемого контента. Для наилучшей синхронизации данного типа контента рекомендуется использовать аппаратный медиапроигрыватель, сигнал с которого через сплиттер будет поступать на физические входы видеоконтроллеров (как это рассмотрено выше).

Аппаратно захватываемый IP-поток. Для передачи видеосигнала (особенно на большие расстояния) часто используется IP-трансляция. Видеоданные кодируются с использованием специальных про-

токолов (например, H.264) и передаются по сетевым каналам без применения традиционных видеокабелей и соответствующей аппаратуры приема-передачи видеосигнала. Воспроизведение IP-потока сочетает в себе черты двух рассмотренных выше типов контента: физического сигнала и видеофайлов. Как и физический видеосигнал, IP-поток принимается картами аппаратного декодирования IP-потоков. Как и видеофайлы, захватываемый IP-поток требует обработки (декодирования), сопряженной с затратой определенных вычислительных ресурсов. Но в отличие от программно воспроизводимых видеофайлов, IP-поток обрабатывается на аппаратном уровне или на очень низком программном уровне драйвером и не подвержен воздействиям других процессов, выполняемых операционной системой видеоконтроллера. Благодаря этому, как и при обработке физического сигнала, отображение «картинки» происходит практически в режиме реального времени и не приводит к рассинхронизации изображений, выводимых разными видеоконтроллерами.

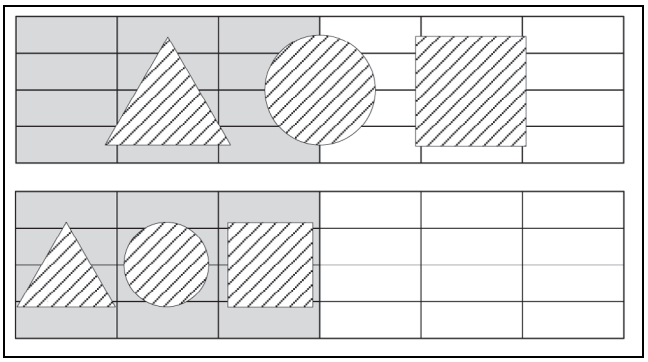


Рис. 6. Перераспределение контента на видеостене при выходе одного видеоконтроллера из строя

Однако следует отметить, что в силу специфики передачи данных по сети рассинхронизация все равно теоретически возможна. Дело в том, что при трансляции IP-потоков существует еще один уровень синхронизации – между источником трансляции и устройством, принимающим сигнал. Этот уровень синхронизации всегда является более приоритетным по сравнению с остальными. Если в силу каких-либо причин (например, в результате потери части пакетов данных) на данном уровне происходит рассинхронизация между источником трансляции и картой захвата IP-потока одного из видеоконтроллеров, то это не отразится на обработке и отображении видеосигнала другими видеоконтроллерами. В результате на видеостене может возникнуть несоответствие частей видеосигнала, отображаемых разными видеоконтроллерами. Такого рода рассинхронизация имеет обычно кратковременный характер и автоматически исправляется на уровне протоколов IP-трансляции (за исключением случаев неисправно функционирующей ЛВС, где доля потерянных пакетов выходит за пределы допустимого).

Таким образом, для всех основных видов контента предложено решение по его синхронизации в едином информационном пространстве видеостены.

В качестве дополнительного плюса использования рассматриваемого системно-технического решения необходимо отметить возможность повышения доступности системы видеоотображения за счет устранения единой точки отказа – единственного видеоконтроллера.

Как уже упоминалось, видеоконтроллеры высокой производительности – очень дорогостоящие изделия. Поэтому при проектировании использующих их систем обычно запасной видеоконтроллер в состав не закладывается в расчете на его бесперебойную работу. Важным достоинством предлагаемой схемы совместного использования нескольких видеоконтроллеров является то, что в случае выхода из строя одного из них остальные продолжают функционировать. Работоспособные видеоконтроллеры не смогут обслуживать ту часть видеостены, которая находится в зоне ответственности вышедшего из строя изделия, но свою часть контента они будут отображать корректно. Более того, с помощь управляющей программы можно перераспределить контент в видепространстве стены таким образом, чтобы на функционирующие видеоконтроллеры переложить отображение наиболее важной информации. Или использовать другой вариант – пропорционально уменьшить размеры отображаемых окон таким образом, чтобы весь необходимый контент уместился на рабочей части видеостены (рис. 6). Данный способ повышения доступности можно отнести к категории «горячего» резервирования, так как перераспределение контента в видеопространстве может быть осуществлено программно без дополнительных действий по переподключению или перезагрузке устройств.

Для некоторых классов систем требуется полное резервирование всего видеопространства (неисправность даже одного видеовыхода недопустима). При использовании традиционных решений, предлагаемых производителями видеооборудования, заказчикам таких систем приходится приобретать в ЗИП дополнительный дорогостоящий видеоконтроллер с большим числом видеовыходов. При использовании

предлагаемого в настоящей статье решения в большинстве случаев достаточно зарезервировать только один из недорогих согласованно работающих видеоконтроллеров.

- Рассмотренное системно-техническое решение построения системы видеоотображения на базе программно согласованных видеоконтроллеров позволяет строить более экономически оправданные системы видеоотображения. Предлагаемое решение применимо для видеостен с большим числом устройств отображения видеоинформации и большинства наиболее распространенных типов контента. Реализация решения обеспечивается разовой разработкой специальной управляющей программы, задачей которой является обеспечение согласованной работы двух и более видеоконтроллеров. Данное решение может рассматриваться как обеспечивающее «горячее» резервирование видеоконтроллеров и повышение доступности всей системы видеоотображения в целом. Изложенный подход был успешно апробирован авторами статьи в начале 2016 г. путем создания пары программно согласованных видеоконтроллеров на безе оборудования Matrox.

Литература

1. *Зацаринный А.А.*, *Чупраков К.Г.* Некоторые аспекты выбора технологии для построения систем отображения информации ситуационного центра // Информатика и ее применения. 2010. Т. 4. № 3. С. 59–68.
2. Matrox Mura User Guide. Quebec. Canada. Matrox Graphics Inc. 2017.

Поступила ██ ██████ 20██ г.

Approach and systemic-technical solutions for increased availability and high information capacity video wall systems construction

© Authors, 2018
© Radiotekhnika, 2018

E.S. Agafonov – Main Specialist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: eagafonov@ipiran.ru
E.R. Korepanov – Ph.D.(Eng.), Head of Department, FRC «Computer Science and Control» RAS (Moscow)
E-mail: ekorepanov@ipiran.ru
V.S. Shorgin – Ph.D.(Eng.), Senior Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: vshorgin@ipiran.ru

The article opens a thematic cycle devoted to the issues of modern and perspective high information capacity video wall systems rational construction. Software-based video controllers make it possible to take full advantage of the modern video equipment capacity due to the possibility of the control software improvement. The article considers the possibility of creating a video wall system based on software-coordinated video controllers in order to optimize the cost of the solution and increase its availability.

References

1. *Zaczarinny'j A.A.*, *Chuprakov K.G.* Nekotory'e aspekty' vy'bora texnologii dlya postroeniya sistem otobrazheniya informaczii situaczionnogo czentra // Informatika i ee primeneniya. 2010. T. 4. № 3. S. 59–68.
2. Matrox Mura User Guide. Quebec, Canada. Matrox Graphics Inc. 2017.

УДК 004.6.056: 004.75

К вопросу об изменении парадигмы информационной безопасности

© Авторы, 2018
© ООО «Издательство «Радиотехника», 2018

Д.И. Правиков – к.т.н., вед. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: d_pravikov@mail.ru
А.Ю. Щербаков – д.т.н., профессор, гл. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: x509@ras.ru

Рассмотрен вопрос об изменении парадигмы информационной безопасности, связанный с формулированием свойств доверия в информационно-телекоммуникационной системе (ИТС). Введена мера доверия, зависящая от ролей и действий в системе. Показано, что валидация свойств доверия возможна в системе распределенных реестров (РР).

Ключевые слова: *информационно-телекоммуникационная система, информационная безопасность, доверие, роль, валидация.*

Consider changing the paradigm of information security associated with the formulation of properties of trust in a telecommunications system, introduced a measure of trust, depending on the roles and actions in the system and it is shown that the validation of the properties of trust are possible in a system of distributed registries.

Keywords: *information and telecommunication system(s), information security, trust, role, validation.*

Объективно любая прикладная наука проходит путь от решения узко поставленных формальных задач и проблем к комплексному осмыслению задачи во взаимосвязи с другими.

Анализ интернет-публикаций и регистрируемых зарубежных патентов в области IT за последнее время (в рамках приблизительно двух-трех последних лет) свидетельствует о том, что намечается некоторое отставание научного и методологического обеспечения теоретической и прикладной информатики от решаемых в этой области актуальных практических задач. Развитие информационных систем как систем массового обслуживания и формирование больших по количественному составу групп пользователей таких систем привело к новым запросам к свойствам по защищенности и качеству обрабатываемой информации. Как следствие, начинают появляться системы, в которых реализовано обеспечение пусть и в неявном виде возникших требований, которые не учитывались в системах предыдущих поколений [1].

Ц е л ь р а б о т ы – рассмотреть вопрос об изменении парадигмы информационной безопасности, связанный с формулированием свойств доверия в информационно-телекоммуникационной системе (ИТС).

Если рассмотреть историю становления информационной безопасности как научного направления, можно выделить ряд э т а п о в, характеризующихся своими базовыми подходами к практическому обеспечению информационной безопасности и связанными, в первую очередь, с использованием при обработке информации средств вычислительной техники.

Э т а п I. Ориентировочно до 1960−70 гг. Объем защищаемых данных незначителен. Обработка данных ведется по большей части вручную. Все вопросы защиты информации решаются в основном с использованием организационных мер.

Э т а п II. Ориентировочно до 2000 г. Объем защищаемых данных возрастает настолько, что его обработка невозможна без применения средств вычислительной техники. Существуют отдельно средства обработки для категорированной информации и средства для обработки открытой информации. Средства вычислительной техники при обработке категорированной информации рассматриваются в качестве «черного ящика», являющегося источником угроз. Разрабатываются меры для повышения «защищенности» и, как следствие, доверия к средствам обработки информации.

Э т а п III. Ориентировочно до 2015 г. Резко возрастает объем обрабатываемой информации. Появляются технологии data mining, big data. Значительная часть конфиденциальной информации вырабатывается путем обработки больших массивов открытых данных. Активно развиваются публичные электронные сервисы.

Происходит изменение глобальных архитектур ИТС. Стратегия развития современного общества в части информационно-телекоммуникационных (или в зарубежной терминологии – инфокоммуникационных) систем предопределяет собой эволюцию в область коллективных вычислений, централизацию

процессов обработки и хранения информации, а также эволюцию в область расширения прикладных и проблемно-ориентированных сервисов и повышения надежности вычислительного процесса ИТС в целом.

Этап IV. Технологии распределенных реестров (РР) и криптовалют получают общественное признание, их внедрение начинает обсуждаться на уровне правительств разных стран.

Приведенный перечень этапов развития подходов к обеспечению информационной безопасности, безусловно, обсуждаем. Существует как минимум несколько публикаций, разнящихся в датировке и содержании этапов, но, как представляется, они принципиально друг другу не противоречат [2]. Вместе с тем, для настоящей статьи принципиально важным является выделение последнего этапа IV, так как он фактически означает появление новой парадигмы в области информационной безопасности.

Перед тем как перейти к ее изложению, следует отметить, что в определенных академических кругах применительно к сложным системам оперируют понятиями физической и информационной замкнутости (или незамкнутости (разомкнутости)).

Парадигма информационной безопасности первых трех описанных этапов (если точнее, то на третьем этапе уже наметился перелом) определяла защиту информации в условиях среды, замкнутой информационно и физически. Любая система защиты от несанкционированного доступа существует тогда, когда информационная среда замкнута (информация перечислена, а, значит, полностью описана, промаркирована, проранжирована и т.п.), замкнута среда обработки в виде соответствующей компьютерной системы и замкнут круг лиц, допущенных к доступу к информации через компьютерную систему. Тогда можно строить правила, их верифицировать, вводить формализацию, разграничивать доступ и т.д.

Если свойство «безопасность» ИТС опирается на понятие «политика безопасности» (ПБ) и при этом постулируется, что ИТС является защищенной в том случае, когда выполнена априорно заданная ПБ, то в настоящее время существует запрос со стороны пользователей на попытку естественного обобщения понятия надежности и защищенности на более широкий класс объектов, категорий и конкретных систем.

Так, вполне очевидно, что некорректно сформулированная ПБ не обеспечивает безопасности, но классическая компьютерная безопасность, тем не менее, утверждает обратное. Так, например, п. 13.2.3 «Проверка соответствия требованиям безопасности» ГОСТ Р ИСО/МЭК ТО 13335-5-2006 предписывает проводить проверку, начиная, в первую очередь, именно с проверки соответствия ПБ. Пусть, например, злоумышленник внес в банковскую систему запись о снятии со счета некоего человека заданной суммы, заведомо меньшей количества денег на счете. Конфиденциальность не нарушена, целостность и доступность тоже. Доказать факт внесения записи, не соответствующей действительности, без внедрения дополнительных механизмов защиты будет весьма сложно.

Исходя из изложенного, можно утверждать, что расширение рамок рассмотрения проблемы в контексте современных требований является весьма актуальной задачей для синтеза надежных и защищенных систем.

Появление технологии РР и ее общественное признание свидетельствует о реализации явочным порядком новых подходов к обеспечению информационной безопасности (в широком смысле понятия).

«Информационная безопасность 2.0» – это защита информации в условиях, когда система замкнута информационно, но разомкнута физически. В данном случае система разомкнута физически в смысле отсутствия фиксированного перечня пользователей, а также состава программно-аппаратных средств. Каким образом и от чего будет, например, защищаться информация в социальной сети, когда не доступен фиксированный перечень ее пользователей, постоянно подключающийся и отключающийся от системы с использованием своих смартфонов и персональных компьютеров?

С одной стороны, многие эксперты, оценивая феномен развития социальных сетей, блогов и других аналогичных сервисов, утверждают, что их популярность обусловлена доверием пользователей к размещаемой в них информации. С другой стороны, в научной и методической литературе последних лет все чаще встречается термины «доверие» и «доверенные системы». Этот процесс отражает объективные закономерности в развитии науки о компьютерных системах. Отечественные источники, в частности ГОСТ Р ИСО/МЭК ТО 13335-5-2006, рекомендуют использовать термин «доверительные отношения» и «доверительная среда». В связи с этим далее будем также использовать данные термины.

Термин «доверие» в применении к ИТС означает эволюцию от узкого понимания надежности и безопасности компонентов системы в сторону общеметодологических вопросов обеспечения выполнимости целевой функции ИТС, то есть той функции, для которой она предназначена и создается.

Доверие – свойство системы, объективно, обоснованно и документально выраженное основание того, что элемент системы (в терминах стандартов – изделие ИТ, продукт ИТ, компонент ИТС, ИТС в це-

лом) отвечает априорно заданной (регламентациями высшего уровня) целевой функции на всем протяжении своего жизненного цикла *и во всех режимах функционирования*.

На современном уровне технологий и развития ИТС для большинства пользователей доверие представляет собой триаду, схематично изображенную на рисунке.

Триада доверия

Доверие к информации подразумевает циркуляцию и использование в ИТС информации, полученной из доверенных источников, либо прошедшую этап валидации. Обратите внимание, что на предыдущих этапах развития информационных технологий информация в систему закладывалась самим пользователем, поэтому она априорно считалась валидной. На текущем этапе возможна ситуация, когда информационное наполнение системы будет передано на аутсорсинг, что повлечет за собой внедрение дополнительных механизмов по проверке ее полноты и достоверности.

Доверие к средствам обработки информации с методической точки зрения на настоящий момент проработано наиболее детально. В том случае, если постулируется необходимость того, что ИТС должна точно соответствовать той целевой функции, для реализации которой она создается, то естественным является рассмотрение жизненного цикла ИТС, начиная с формулирования корректной, непротиворечивой целевой функции и рассмотрения архитектуры ИТС как заданной в терминах системного анализа целостности компонентов ИТС и связей между ними. Считается, что разработанная в соответствии с определенными требованиями к процедуре разработки программно-аппаратная среда является доверенной.

Доверие к механизмам разрешения конфликтов является относительно новым требованием со стороны пользователей ИТС, хотя общество уже давно выработало для себя такие механизмы на уровне общественных отношений.

В частности, раздел 13.2.6 «Обработка инцидентов» ГОСТ Р ИСО/МЭК ТО 13335-5-2006 описывает факт наличия «документированных и осуществимых схем действий при обработке инцидентов», вместе с тем, данное требование носит общий характер и, как правило, не может быть непосредственно реализовано при разработке конкретных систем.

Полагаем, что более продуктивным будет являться подход, когда в системе будут не только реализованы базовые требования по защите информации, но и в явном виде будут присутствовать механизмы выявления и расследования инцидентов в понимании конкретной ИТС, а также обеспечена возможность совершенствования системы защиты по результатам анализа инцидентов. Говоря другими словами, уже на этапе проектирования и разработки системы надо признать факт ее физической незамкнутости.

Кажется, что сторонники РР видят в данной технологии защиту от возможных злоупотреблений оператора ключевого элемента, присутствующего в большинстве систем, построенных по традиционной схеме. Вместе с тем, опыт применения программного обеспечения с открытым кодом показывает низкую эффективность подходов, минимизирующих угрозу наличия недекларированных возможностей (в приведенном примере), путем передачи ответственности широкому, но неопределенному кругу лиц.

Как представляется, идея блокчейна или РР заключается в том, чтобы обеспечить механизм синхронизации мнения пользователя системы и мнения экспертов, контролирующих процесс эксплуатации системы, что фактически и предопределило популярность данной технологии.

Исходя из уровня современного развития информационных технологий, можно предложить следующий подход к построению больших систем: сначала формируется желаемая система общественных отношений, которая затем реализуется в виде соответствующей информационной системы.

Пусть разрабатывается система, реализующая некие абстрактные транзакции. Разработка и эксплуатация такой системы предусматривает, как минимум, роли разработчика, оператора системы, пользователя, экспертов, контролирующих процесс эксплуатации системы, а также злоумышленника. Разработчик создает программно-аппаратные средства, обеспечивающие обработку информации в системе (как минимум, хранение). Оператор системы осуществляет администрирование системы, в частности, наделяет пользователя набором полномочий по вводу и обработке информации. Эксперты, контролирующие процесс эксплуатации системы, на основании представленных из системы данных делают заключение о факте совершения пользователем какого-либо действия, либо отрицают таковое. Злоумышленник реализует свои цели, маскируясь в той или иной степени под действия легального пользователя.

Таблица. ***Возможные действия при эксплуатации системы***

Действие	Штатная работа	Защита от нарушения целостности	Угроза отказуемости	Угроза виртуализации	Защита аутентичности
Пользователь совершил допустимое действие в системе	Да	Да	Да	Нет	Нет
Злоумышленник совершил действие в системе под видом пользователя	Нет	Нет	Нет	Да	Да
Информация о действии занесена в систему корректно	Да	Да	Нет	Да	Да
Информация о действии хранится в системе без изменений	Да	Нет	Да	Да	Да
На основании представленных данных из системы пользователь согласен с фактом совершения действия с представленными параметрами	Да	Нет	Нет	Нет	Нет
На основании представленных данных из системы эксперты согласны с фактом совершения действия с представленными параметрами	Да	Нет	Да	Да	Нет

В представленной таблице описаны шесть возможных действий при эксплуатации системы, ее атаке злоумышленником и расследовании инцидентов. Очевидно, что полный набор составляет $2^6 = 64$ сочетания, поэтому в качестве иллюстрации приводится только пять сочетаний, включая штатную работу. Обратите внимание, что две колонки озаглавлены «Защита…», а две колонки «Угроза …». Для ситуации «защита» мнение экспертов подтверждает мнение пользователя о совершенном действии, при «угрозе» мнения пользователя и экспертов разнятся.

Задав перечень ролей и перечень действий как двоичную функцию, принимающую значение «истинно»/«ложно», можно в виде предикатов описать случаи, на которые требуется организовать реакцию системы. При этом множество случаев, на которые требуется реализовать реакцию системы, можно описать в виде предикатного выражения по аналогии с функциями булевой алгебры.

Опишем это формально. Пусть r_i – i-я базовая роль в проектируемой системе, a_j – j-е базовое действие. Тогда $x_{ij} = f(r_i, a_j)$ – двоичная переменная, описывающая факт выполнения i-й базовой ролью j-го базового действия. С учетом введенных переменных, описание отношений R между ролями в проектируемой ИТС может быть описано как $R = x_{i_1 j_1} \wedge x_{i_1 j_2} \wedge \ldots \wedge x_{i_1 j_k} \vee x_{i_2 j_1} \wedge x_{i_2 j_2} \wedge \ldots \wedge x_{i_2 j_n} \vee \ldots$.

Если отношения выполнения базовыми ролями базовых действий в формуле для R не заданы, то считается, что требование по реагированию на сочетание данных действий в ИТС не предъявляется.

Если в системе задано n базовых ролей, а базовых действий m, то всего двоичных переменных будет задано $n + m$, а значений булевой (двоичной) функции 2^{n+m}.

Для приведенной таблицы $n = 5$ (пользователь, администратор, разработчик, эксперт (аудитор), злоумышленник) и $m = 6$, таким образом, значений функции $2^{11} = 2048$. Тогда функцию, как указано выше, можно задать в виде дизъюнктивной нормальной формы или в виде эквивалентного полинома Жегалкина.

Можно утверждать, что функция f будет зависеть не менее чем от $n + m$ переменных, в противном случае реагирование не зависит от каких-либо действий или ролей.

Отсюда *базовая теорема доверенной системы* (базовая теорема Правикова–Щербакова) формулируется следующим образом: при наличии в системе n базовых ролей и m базовых действий функция реагирования зависит ровно от $n + m$ двоичных переменных, а число значений этой функции равно 2^{n+m}

В приведенной таблице задано шесть реакций из 2048 возможных.

В соответствии с базовой теоремой доверенных систем возможно ввести обоснованную *численную меру доверия D*, равную отношению описанных реакций к общему числу значений функции реагирования: $D = Nr/Nf$, где Nr – число описанных реакций (описанных предикатом значений); $Nf = 2^{n+m}$ – общее число значений функции реагирования.

Система будет тем более доверенной, чем более число описанных предикатом значений будет стремиться к числу значений функции (то есть мера доверия в этом случае будет стремиться к 1).

Почему так важно свойство доверенности? Потому, что на основе информации, обрабатываемой в ИТС, будут приниматься управленческие решения. Большинство ИТС уже по определению являются элементами систем управления.

Далее, если в системе есть контуры управления, для них должны работать основные законы кибернетики. Но обеспечение законов кибернетики потребует новой парадигмы информационной безопасности.

На факт появления технологии РР можно посмотреть еще с одной стороны. Древние греки определяли человека как «двуногое <существо> без перьев». Сейчас же, при современном уровне развития информационных технологий, можно определить человека в прошедшем времени как последовательность транзакций в выделенных им сервисах.

На этом хотелось бы остановиться подробнее. Как говорили многие мыслители, человек, проходя по жизни, оставляет после себя след на земле. Понятие следа весьма условно, но в большинстве случаев может быть сведено к наличию уникальных знаков (символов, образов и т.п.) на общедоступных носителях. Активное использование электронных сервисов приводит к тому, что эти следы начинают перемещаться в сферу информационных технологий. Теперь человек – это его страницы в социальных сетях, его сообщения, лайки, комментарии, репосты, поисковые запросы и т.п. Но человек также может быть представлен его банковскими транзакциями, журналом соединений у операторов сотовой связи, журналом обращения за медицинскими услугами и т.д. В этой связи будет уместным процитировать интервью Е. Касперского, данное им РБК 20 мая 2016 г.: «Человек оставляет огромное количество информации о себе, иногда в самых неожиданных местах, особенно когда путешествует. Покупаете билет на самолет – бах, сразу попали в базу данных. Бронируете гостиницу – бах, в другую. <…> Не надо думать, что за вами будет кто-то шпионить и про вас все узнают. Про вас и так уже все знают, вы и так уже везде наследили».

Может быть, такое настойчивое желание потенциальных пользователей внедрить РР обусловлено тем, что они хотят оставить о себе неискаженный след?

- Констатирован объективный процесс изменения парадигмы информационной безопасности, связанный с формулированием свойств доверия в ИТС, введена мера доверия, зависящая от базовых ролей и действий в системе, и показано, что валидация свойств доверия возможна, в частности, в системе РР.

Литература

1. *Биктимиров М.Р.*, *Щербаков А.Ю.* Проблемы синтеза доверенных систем // Труды ИСА РАН. 2012. Т. 53. С. 264–271.
2. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком. 2004.

Поступила ██ ██████ 20██ г.

To the question about changing the paradigm of information security

© Authors, 2018
© Radiotekhnika, 2018

D.I. Pravikov – Ph.D.(Eng.), Leading Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: d_pravikov@mail.ru
A.Yu. Scherbakov – Dr.Sc.(Eng.), Professor, Main Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: x509@ras.ru

Consider changing the paradigm of information security associated with the formulation of properties of trust in a telecommunications system, introduced a measure of trust, depending on the roles and actions in the system and it is shown that the validation of the properties of trust are possible in a system of distributed registries. Possible actions for the operation of such a system are given.

References

1. *Biktimirov M.R.*, *Shherbakov A.Yu.* Problemy' sinteza doverenny'x sistem // Trudy' ISA RAN. 2012. T. 53. S. 264–271.
2. *Malyuk A.A.* Informaczionnaya bezopasnost': konczeptual'ny'e i metodologicheskie osnovy' zashhity' informaczii. M.: Goryachaya liniya – Telekom. 2004.

УДК 621

Инструментальное программное обеспечение анализа и синтеза стохастических систем высокой доступности (VI)

© Авторы, 2018
© ООО «Издательство «Радиотехника», 2018

И.Н. Синицын – д.т.н., профессор, гл. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: sinitsin@dol.ru
И.В. Сергеев – к.т.н., зам. директора, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: isergeev@ipiran.ru
Э.Р. Корепанов – к.т.н., вед. науч. сотрудник, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: ekorepanov@ipiran.ru
Т.Д. Конашенкова – вед. программист, ФИЦ «Информатика и управление» РАН (Москва)
E-mail: tkonzshenkova@ipiran.ru

Получены вейвлет алгоритмы аналитического моделирования векторов математических ожиданий, ковариационных матриц и матриц ковариационных функций. Приведены тестовые примеры, обобщающие полученные результаты.

Ключевые слова: *аналитическое моделирование, вейвлет каноническое разложение (КРВЛ), вектор математических ожиданий СтП, каноническое разложение (КР), ковариационная матрица, линейная нестационарная СтС, матрица ковариационных функций, стохастическая система (СтС), стохастический процесс (СтП).*

The article proceeds the thematic cycle dedicated to analytical modeling linear nonstationary stochastic systems with high availability based on wavelet and wavelet canonical expansions. Test examples and generalizations are given.

Keywords: *analytical modeling, canonical expansion (CE), covariance matrix, linear nonstationary StS, matrix of covariance functions, stochastic process (StP), stochastic systems (StS), vector of mathematical expectations, wavelet CE.*

Статья продолжает цикл статей по анализу стохастических линейных нестационарных непрерывных систем высокой доступности (СВД) на базе теории вейвлетов.

1. Введение

Среди подходов к повышению оперативности решения задач экспресс аналитического моделирования процессов в стохастических СВД важное место занимают методы, основанные на вейвлет канонических разложениях (КРВЛ). В [1, 2] разработано методическое и инструментальное программное обеспечение для информационных технологий корреляционного анализа и синтеза нестационарных стохастических СВД на основе КРВЛ путем ортогонального разложения элементов матрицы ковариационных функций по двумерным вейвлетам Добеши с компактным носителем.

На базе последовательных рекуррентных алгоритмов построения КР и разработанного вейвлет методического обеспечения в среде MATLAB создано экспериментальное инструментальное программное обеспечение «СтИТ-КР.ВЛ.2».

На основе разработанного методического и инструментального обеспечения проходят испытания специализированные программные средства для оценки ударонадежности вычислительного оборудования. Разработаны тестовые примеры для типовых двумерных нестационарных случайных функций.

Ц е л ь р а б о т ы – развить [1, 2] на случай, когда стохастическая СВД описывается векторно-матричным линейным нестационарным дифференциальным уравнением или нестационарным линейным преобразованием.

В разделе 2 представлены элементы спектрально-корреляционной теории стохастических процессов (СтП) и их линейных преобразований. Раздел 3 посвящен КР СтП. Разделы 4–6 описывают вейвлет алгоритмы аналитического моделирования вектора математических ожиданий, ковариационной матрицы и матрицы ковариационных функций путем решения соответствующих обыкновенных дифференциальных уравнений. В разделах 7 и 8 показано, что применение КРВЛ позволяет существенно сократить время проведения аналитического моделирования даже при использовании последовательных алгоритмов декоррелизации. Заключение содержит выводы и возможные направления обобщений. В приложении приведены два тестовых примера.

2. Линейные стохастические системы

2.1. Уравнения корреляционной теории. Следуя [3, 4], рассмотрим линейную стохастическую систему (СтС) следующего вида:

$$\dot{\mathbf{Y}}_t = \mathbf{a}\mathbf{Y}_t + \mathbf{a}_0 + \mathbf{b}\mathbf{V}, \tag{2.1}$$

где $\mathbf{Y}_t$ – вектор состояния системы размерности $p = n_x$; $\mathbf{a} = \mathbf{a}(t), \mathbf{a}_0 = \mathbf{a}_0(t), \mathbf{b} = \mathbf{b}(t)$ – коэффициенты размерности $(p \times n)$, $(p \times 1)$, $(p \times m)$ соответственно, которые в общем случае могут быть функциями времени t; $\mathbf{V}$ – белый шум размерности n_v, интенсивность которого $\mathbf{v} = \mathbf{v}(t)$ тоже в общем случае может быть функцией времени t.

Для нахождения моментов первого и второго порядка СтП $\mathbf{Y}_t$, определяемого линейным дифференциальным уравнением (2.1), достаточно, чтобы он был белым шумом в широком смысле. Поэтому везде в этом разделе будем считать $\mathbf{V}$ произвольным белым шумом с интенсивностью $\mathbf{v} = \mathbf{v}(t)$.

Представим вектор состояния системы $\mathbf{Y}_t$ формулой

$$\mathbf{Y}_t = \mathbf{Y}(t) = \mathbf{u}(t,t_0)\mathbf{Y}_0 + \int_{t_0}^{t} \mathbf{u}(t,\tau)\mathbf{b}(\tau)\mathbf{V}(\tau)d\tau + \int_{t_0}^{t} \mathbf{u}(t,\tau)\mathbf{a}_0(\tau)d\tau, \tag{2.2}$$

где $\mathbf{u}(t,\tau)$ – матрица, определяемая как функция t однородным дифференциальным уравнением $d\mathbf{u}/dt = \mathbf{a}(t)\mathbf{u}$ и начальным условием $\mathbf{u}(t,\tau) = \mathbf{I} = \mathbf{I}_p$.

Математическое ожидание, ковариационная функция и момент второго порядка вектора состояния системы $\mathbf{Y}_t$ определяются соответственно следующим образом:

$$\mathbf{m}_y(t) = \mathbf{u}(t,t_0)\mathbf{m}_0 + \int_{t_0}^{t} \mathbf{u}(t,\tau)\mathbf{a}_0(\tau)d\tau, \tag{2.3}$$

$$\mathbf{K}_y(t_1 .t_2) = \mathbf{u}(t_1,t_0)\mathbf{K}_0\mathbf{u}(t_2,t_0)^* + \int_{t_0}^{\min(t_1,t_2)} \mathbf{u}(t_1,\tau)\mathbf{b}(\tau)\mathbf{v}(\tau)\mathbf{b}(\tau)^{\mathrm{T}}\mathbf{u}(t_2,\tau)^* d\tau, \tag{2.4}$$

$$\mathbf{\Gamma}_y(t_1 .t_2) = \mathbf{K}_y\mathbf{u}(t_1,t_2)^* + \mathbf{m}_y(t_1 .t_2)^{\mathrm{T}}, \tag{2.5}$$

где $\mathbf{m}_0$ – математическое ожидание начального значения $\mathbf{Y}_0$ вектора состояния $\mathbf{Y}_t$; $\mathbf{K}_0 = \mathbf{K}(t_0,t_0)$ – ковариационная матрица $\mathbf{Y}_0$.

При выводе этой формулы учитывалось, что начальное состояние системы $\mathbf{Y}_0$ не зависит от белого шума $\mathbf{V}(t)$ при $t > t_0$ и что $\mathbf{u}(t,\tau) = 0$ при $\tau > t$. Последним обстоятельством объясняется то, что верхний предел интегрирования равен $\min(t_1 .t_2)$. Кроме того, учитывалось, что коэффициенты уравнений реальных систем всегда действительны, в то время как элементы матрицы $\mathbf{u}(t,\tau)$ могут быть комплексными даже в этом случае.

В практических задачах обычно бывает достаточно найти вероятностные характеристики вектора состояния СтС $\mathbf{Y}_t$ в каждый данный момент t (определяемые одномерным распределением), то есть только значения ковариационной функции $\mathbf{K}_y(t,t) = \mathbf{K}_y(t)$ и момента второго порядка $\mathbf{\Gamma}_y(t,t) = \mathbf{\Gamma}_y(t)$. Само собой разумеется, что все эти величины для линейной системы можно определить по формулам (2.3)–(2.5) при $t_1 = t_2 = t$. Однако в случае линейной СтС их можно вычислить значительно проще – интегрированием соответствующих линейных дифференциальных уравнений:

$$\dot{\mathbf{m}}_y = \mathbf{a}\mathbf{m}_y + \mathbf{a}_0,\ \mathbf{m}(t_0) = \mathbf{m}_0, \qquad \dot{\mathbf{K}}_y = \mathbf{a}\mathbf{K}_y + \mathbf{K}_y\mathbf{a}^{\mathrm{T}} + \mathbf{b}\mathbf{v}\mathbf{b}^{\mathrm{T}},\ \mathbf{K}(t_0) = \mathbf{K}_0, \tag{2.6), (2.7}$$

$$\dot{\mathbf{\Gamma}}_y = \mathbf{a}\mathbf{\Gamma}_y + \mathbf{\Gamma}_y\mathbf{a}^{\mathrm{T}} + \mathbf{b}\mathbf{v}\mathbf{b}^{\mathrm{T}} + \mathbf{a}_0\mathbf{m}_y^{\mathrm{T}} + \mathbf{m}_y\mathbf{a}_0^{\mathrm{T}},\quad \mathbf{\Gamma}(t_0) = \mathbf{\Gamma}_0, \tag{2.8}$$

$$\frac{\partial \mathbf{K}_y(t_1,t_2)}{\partial t_2} = \mathbf{K}_y(t_1,t_2)\mathbf{a}(t_2)^{\mathrm{T}} \text{ при } t_1 < t_2, \mathbf{K}_y(t_1,t_1) = \mathbf{K}_y(t_1) \text{ и при } t_1 > t_2, \mathbf{K}_y(t_1,t_2) = \mathbf{K}_y(t_2,t_1)^{\mathrm{T}}. \quad (2.9)$$

Таким образом, приходим к следующему утверждению.

Т е о р е м а 2 . 1 . *Пусть линейная СтС (2.1) (в общем случае негауссовская) с белым шумом* **V***, понимаемом в широком смысле, допускает с.к. решение с конечными моментами первого и второго порядка. Тогда формулы (2.4)−(2.5) дают интегральное представление моментов первого и второго порядка, а формулы (2.6)−(2.9) – в виде обыкновенных дифференциальных уравнений.*

2.2. Уравнения спектральной теории. Теперь, следуя [3, 4], рассмотрим асимптотически устойчивую стационарную линейную СтС (2.1), находящуюся под действием стационарного белого шума с постоянной интенсивностью $\mathbf{v}$. В этом случае $\mathbf{a}, \mathbf{a}_0, \mathbf{b}$ постоянны, функция $\mathbf{u}(t,\tau)$ зависит только от разности аргументов, $\mathbf{u}(t,\tau) = \mathbf{w}(t-\tau)$, и полученные формулы при $t_0 \to -\infty$ принимают следующий вид:

$$\dot{\mathbf{m}}_y = \mathbf{m} = \int_0^\infty \mathbf{w}(\xi)\mathbf{a}_0 d\xi, \quad \mathbf{K}_y = \mathbf{K} = \int_0^\infty \mathbf{w}(\xi)\mathbf{b}\mathbf{v}\mathbf{b}^{\mathrm{T}}\mathbf{w}(\xi)^* d\xi, \quad (2.10), (2.11)$$

$$\mathbf{k}(\tau) = \mathbf{K}(t+\tau,t) = \int_0^\infty \mathbf{w}(\xi+\tau)\mathbf{b}\mathbf{v}\mathbf{b}^{\mathrm{T}}\mathbf{w}(\xi)^* d\xi \quad (\tau \le 0). \quad (2.12)$$

Следовательно, с течением времени в асимптотически устойчивой стационарной линейной дифференциальной системе под действием стационарного белого шума устанавливается стационарный в широком смысле СтП. Условие асимптотической устойчивости системы является не только достаточным, но и необходимым для существования стационарного СтП.

Поскольку $\mathbf{m}$ и $\mathbf{K}$ в стационарном режиме постоянны, то, полагая в уравнениях (2.6) и (2.7) $\dot{\mathbf{m}} = 0$ и $\dot{\mathbf{K}} = 0$, получим линейные алгебраические уравнения для $\mathbf{m}$ и $\mathbf{K}$:

$$\mathbf{a}\mathbf{m} + \mathbf{a}_0 = 0, \quad \mathbf{a}\mathbf{K} + \mathbf{K}\mathbf{a}^{\mathrm{T}} + \mathbf{b}\mathbf{v}\mathbf{b}^{\mathrm{T}} = 0. \quad (2.13)$$

Если начальные значения $\mathbf{m} = 0$ и $\mathbf{K} = 0$ удовлетворяют уравнениям (2.13), то уравнения (2.6) и (2.7) имеют очевидное решение $\mathbf{m} = \mathbf{m}_0$, $\mathbf{K} = \mathbf{K}_0$. В этом случае при любом t_0 СтП $\mathbf{Y}_t$ будет стационарным в широком смысле.

Уравнения для ковариационной функции $\mathbf{k}(\tau)$ стационарного СтП $\mathbf{X}_t$ в линейной стационарной системе (2.1) имеют вид

$$d\mathbf{k}(\tau)/d\tau = \mathbf{a}\mathbf{k}(\tau), \quad \tau > 0, \quad \mathbf{k}(0) = \mathbf{K}, \quad (2.14)$$

где $\mathbf{k}(\tau) = \mathbf{k}(-\tau)^{\mathrm{T}}$ при $\tau < 0$.

Полученные результаты распространяются на нестационарные линейные системы (2.1) при постоянных $\mathbf{a}, \mathbf{b}, \mathbf{v}$ и произвольной функции времени $\mathbf{a}_0(t)$. В этом случае уравнения для $\mathbf{K}$ и $\mathbf{k}(\tau)$ остаются справедливыми, а $\mathbf{m}$ представляет собой функцию времени, определяемую уравнениями (2.6). Процесс $\mathbf{Y}_t$ в системе, для которого $\mathbf{m}$ определяется уравнением (2.6) при любом начальном условии, а $\mathbf{K}$ и $\mathbf{k}(\tau)$ находятся изложенным здесь способом, будет ковариационно стационарным.

2.3. Корреляционная теория линейных преобразований. Пусть даны математическое ожидание $\mathbf{m}_u(t)$ и ковариационная функция $\mathbf{K}_u(t,t')$ входного сигнала $\mathbf{U}(t)$. Поставим задачу найти $\mathbf{m}_x(s)$ и $\mathbf{K}_x(s,s')$ выходного сигнала $\mathbf{X}(s)$ для линейного преобразования

$$\mathbf{X}(s) = \mathbf{A}\mathbf{U}(t), \quad (2.15)$$

где $\mathbf{A}$ – произвольный линейный оператор.

Эта задача решается просто, если допустить, что операция математического ожидания и оператор $\mathbf{A}$ переместительны. В этом случае справедливы формулы

$$\mathbf{m}_x(s) = \mathbf{A}\mathbf{m}_u(t), \quad \mathbf{K}_x(s,s') = \mathbf{A}_t\overline{\mathbf{A}_{t'}}\mathbf{K}_u(t,t') = \overline{\mathbf{A}_{t'}}\mathbf{A}_t\mathbf{K}_u(t,t'), \quad (2.16), (2.17)$$

$$\mathbf{\Gamma}_x(s,s') = \mathbf{A}_t \overline{\mathbf{A}_{t'}} \mathbf{\Gamma}_u(t,t') = \overline{\mathbf{A}_{t'}} \mathbf{A}_t \mathbf{\Gamma}_u(t,t'), \tag{2.18}$$

где индекс у оператора $\mathbf{A}$ указывает, что этот оператор действует над функцией данного аргумента при фиксированных значениях всех остальных переменных.

Таким образом, в основе корреляционной теории линейных преобразований СФ лежат формулы (2.16) и (2.18).

2.4. Спектральная теория линейных преобразований. Рассмотрим случай операторных линейных уравнений вида

$$\mathbf{Y}_t = \mathbf{\Phi}(D)\mathbf{U}_t, \quad \mathbf{U}_t = \mathbf{U}(t) = \mathbf{m}_u(t) + \int_{-\infty}^{\infty} \mathrm{e}^{\mathrm{i}\omega t}\mathbf{V}(\omega)d\omega, \tag{2.19}$$

где $\mathbf{\Phi}(D)$ – передаточная функция ($D = d/dt$); $\mathbf{U}_t = \mathbf{U}(t)$ – стационарный СтП со спектральной плотностью $\mathbf{s}_u(\omega)$.

Спектральному разложению $\mathbf{U}_t$ соответствует спектральное разложение $\mathbf{Y}_t$

$$\mathbf{Y}_t = \mathbf{m}_x(t) + \int_{-\infty}^{\infty} \mathrm{e}^{\mathrm{i}\omega t}\mathbf{\Phi}(\mathrm{i}\omega)\mathbf{V}(\omega)d\omega, \tag{2.20}$$

причем СтП $\mathbf{Y}_t$ стационарен, а его ковариационная функция и спектральная плотность равны

$$\mathbf{k}_y(\tau) = \int_{-\infty}^{\infty} \mathbf{y}(\omega)\mathrm{e}^{\mathrm{i}\omega\tau}d\omega, \quad \mathbf{s}_y(\omega) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \mathbf{k}_y(\tau)\mathrm{e}^{\mathrm{i}\omega\tau}d\tau = \mathbf{\Phi}(\mathrm{i}\omega)\mathbf{s}_u(\omega)\mathbf{\Phi}(\mathrm{i}\omega)^*. \tag{2.21), (2.22}$$

Взаимная спектральная плотность входного и выходного сигналов системы определяются по формулам

$$\mathbf{s}_{yu}(\omega) = \mathbf{s}_u(\omega)\mathbf{\Phi}(\mathrm{i}\omega), \quad \mathbf{s}_{uy}(\omega) = \mathbf{s}_u(\omega)\mathbf{\Phi}(\mathrm{i}\omega)^* = \mathbf{s}_u(\omega)\mathbf{\Phi}(-\mathrm{i}\omega). \tag{2.23}$$

Приведенные формулы справедливы только для асимптотически устойчивых стационарных систем, работающих в установившемся режиме, то есть при бесконечно долго действующем стационарном входном сигнале. Практически эти формулы применимы, когда время действия входного сигнала превышает время переходного процесса. Если система описывается дифференциальным уравнением и, следовательно, ее передаточная функция рациональна, то выходной сигнал может быть стационарным СтП при любом времени работы системы и специальных начальных условиях. А именно: случайное начальное значение $\mathbf{Y}(t_0) = \mathbf{Y}_0$ следует выбрать так, чтобы ковариационная матрица случайного вектора $\overline{\mathbf{Y}}(t) = [\mathbf{U}_t^{\mathrm{T}}\ \mathbf{Y}_t^{\mathrm{T}}]^{\mathrm{T}}$ не зависела от t. Для этого достаточно взять случайное начальное значение $\mathbf{Y}_0$, для которого

$$\mathbf{K}_{y_0} = \mathbf{k}_y(0) = \int_{-\infty}^{\infty} \mathbf{\Phi}(\mathrm{i}\omega)\mathbf{s}_u(\omega)\mathbf{\Phi}(\mathrm{i}\omega)^* d\omega, \quad \mathbf{K}_{u_0y_0} = \mathbf{k}_{uy}(0) = \int_{-\infty}^{\infty} \mathbf{s}_u(\omega)\mathbf{\Phi}(\mathrm{i}\omega)^* d\omega. \tag{2.24}$$

Для вычисления дисперсий и ковариаций компонент выходного сигнала устойчивой стационарной системы, работающей в установившемся режиме под действием стационарного входного сигнала (практически при достаточно долгом действии входного сигнала), в каждый данный момент времени t достаточно положить в формуле (2.24), определяющей ковариационную функцию выходного сигнала, $t_1 = t_2 = t$. Тогда получим следующую формулу для ковариационной матрицы значения выходного сигнала в момент t:

$$\mathbf{K}_y = \mathbf{k}_y(0) = \int_{-\infty}^{\infty} \mathbf{\Phi}(\mathrm{i}\omega)\mathbf{s}_u(\omega)\mathbf{\Phi}(\mathrm{i}\omega)^* d\omega, \quad \mathbf{K}_{u_0y_0} = \mathbf{k}_{uy}(0) = \int_{-\infty}^{\infty} \mathbf{s}_u(\omega)\mathbf{\Phi}(\mathrm{i}\omega)^* d\omega. \tag{2.25}$$

Выражением (2.25) можно также пользоваться и для вычисления ковариаций компонент входного сигнала с компонентами выходного сигнала по формуле

$$\mathbf{K}_{zy} = \mathbf{k}_{zy}(0) = \int_{-\infty}^{\infty} \mathbf{s}_u(\omega)\mathbf{\Phi}(\mathrm{i}\omega)^* d\omega. \tag{2.26}$$

Таким образом, в основе спектрально-корреляционной теории стационарных СтП лежат следующие два утверждения.

Т е о р е м а 2 . 2 . *Если в условиях теоремы 2.1 белый шум стационарен в широком смысле,* $\mathbf{a}, \mathbf{a}_0$ *и* $\mathbf{b}$ *постоянные, причем матрица* $\mathbf{a}$ *асимптотически устойчива, то в основе корреляционной теории лежат интегральные представления (2.10)−(2.12) и конечные уравнения (2.13), (2.14).*

Т е о р е м а 2 . 3 . *Пусть передаточная функция* $\mathbf{\Phi}(D)$ *линейной стационарной СтС (2.19) асимптотически устойчива, тогда в основе спектрально-корреляционной теории лежат уравнения (2.20)−(2.22), (2.24), (2.25).*

Для уравнения (2.1) основные формулы получаются, если положить

$$\mathbf{\Phi}(\mathrm{i}\omega) = -(\mathbf{a} - \mathrm{i}\omega\mathbf{I}_n)^{-1}\mathbf{b}. \tag{2.27}$$

В том случае, когда для $\mathbf{U}_t$ и $\mathbf{k}_u(\tau)$ используется спектральное представление

$$\mathbf{U}_t = \mathbf{m}_u(t) + \int_{-\infty}^{\infty} \mathrm{e}^{\mathrm{i}\omega t}\mathbf{Z}(d\omega), \quad \mathbf{k}_u(\tau) = \int_{-\infty}^{\infty} \mathrm{e}^{\mathrm{i}\omega\pi}\mathbf{\sigma}(d\omega),$$

формулы для $\mathbf{X}_t, \mathbf{k}_x(\tau), \mathbf{k}_{ux}(\tau)$ принимают вид

$$\mathbf{X}_t = \mathbf{m}_x(t) + \int_{-\infty}^{\infty} \mathrm{e}^{\mathrm{i}\omega t}\mathbf{\Phi}(\mathrm{i}\omega)\mathbf{Z}(d\omega), \quad \mathbf{k}_x(\tau) = \int_{-\infty}^{\infty} \mathrm{e}^{\mathrm{i}\omega\pi}\mathbf{\Phi}(\mathrm{i}\omega)\mathbf{\sigma}(d\omega)\mathbf{\Phi}(\mathrm{i}\omega)^*, \quad \mathbf{k}_{ux}(\tau) = \int_{-\infty}^{\infty} \mathrm{e}^{\mathrm{i}\omega\pi}\mathbf{\sigma}(d\omega)\mathbf{\Phi}(\mathrm{i}\omega)^*.$$

При этом формулы (2.22)−(2.25) и (2.27) сохраняют свой вид.

3. Канонические разложения линейных преобразований

3.1. Скалярные КР. Выразив скалярную СФ X_t каким-нибудь КР

$$X_t = m_x(t) + \sum_v V_v\, x_v(t), \tag{3.1}$$

в силу (2.16) получим КР скалярной СФ $Y(t)$:

$$Y(s) = m_y(s) + \sum_v V_v\, y_v(s), \tag{3.2}$$

где $m_y(s)$ и координатные функции $y_v(s)$ находятся как

$$m_y(s) = Am_x(t), \quad y_v(s) = Ax_v(t). \tag{3.3}$$

Согласно [3, 4], ковариационная функция и дисперсия скалярной СФ $Y(t)$ выразятся формулами

$$K_y(s,s') = \sum_v D_v y_v(s)\overline{y_v(s')}, \qquad D_y(s) = \sum_v D_v \mid y_v(s)\mid^2. \tag{3.4), (3.5}$$

3.2. Векторные КР. Общее линейное преобразование векторной СФ $\mathbf{X}(t) = [X_1(t)\ldots X_n(t)]^{\mathrm{T}}$ можно для каждой компоненты $Y_p(s)$ вектора $\mathbf{Y}(s) = [Y_1(s)\ldots Y_n(s)]^{\mathrm{T}}$ выразить формулой

$$\mathbf{Y}(s)=\mathbf{A}\mathbf{X}(t),\quad Y_p(s)=\sum_{h=1}^{n}A_{ph}X_h(t),\quad p=\overline{1,m}, \tag{3.6}$$

где A_{ph} – произвольные линейные операторы, $p=\overline{1,m}$, $h=\overline{1,n}$.

Предполагая, что операция математического ожидания переместительна со всеми линейными операторами A_{ph}, получим следующую формулу для математического ожидания векторной СФ $\mathbf{Y}(t)$:

$$\mathbf{m}^y(s)=[m_p^y(s)],\quad m_p^y(s)=\sum_{h=1}^{n}A_{ph}m_h^x(t),\quad p=\overline{1,m}. \tag{3.7}$$

На основании формул (3.6) и (3.7) можем записать

$$\mathbf{M}[Y_p^0(s)\overline{Y_q^0(s')}]=\sum_{h,l=1}^{n}\mathbf{M}[A_{ph}^tX_h^0(t)\overline{X_l^0(t')}]=\sum_{h,l=1}^{n}A_{ph}^t\,\overline{A_{ql}^{t'}}\mathbf{M}[X_h^0(t)\overline{X_l^0(t')}], \tag{3.8}$$

где верхние индексы у операторов показывают, к функциям каких аргументов они применяются.

Формула (3.8) дает матрицу ковариационных функций векторной СФ $\mathbf{Y}(t)$, то есть совокупность ковариационных функций и взаимных ковариационных функций всех ее составляющих:

$$\mathbf{K}^y(s,s')=[K_{pq}^y(s,s')],\quad K_{pq}^y(s,s')=\sum_{h,l=1}^{n}A_{ph}^t\overline{A_{ql}^{t'}}K_{hl}^x(t,t'),\quad p,q=\overline{1,m}. \tag{3.9}$$

Полагая в (3.9) $s=s'$, получим соответствующие формулы для дисперсий и ковариаций, составляющих ковариационную матрицу $\mathbf{K}^y(s)=[K_{pq}^y(s,s)]$.

Линейное преобразование векторной СФ на основании принципа суперпозиции при помощи КР СФ сводится к такому же линейному преобразованию вектора математического ожидания и векторных координатных функций.

Выразив векторную СФ $\mathbf{X}(t)$ каким-либо КР, где $\mathbf{X}(t)=[X_1(t)\ldots X_n(t)]^{\mathrm{T}}$,

$$X_p(t)=m_p^x(t)+\sum_v V_v\,x_{vp}(t),\quad p=\overline{1,n}, \tag{3.10}$$

получим КР векторной СФ $\mathbf{Y}(s)=[Y_1(s)\ldots Y_m(s)]^{\mathrm{T}}$,

$$Y_p(s)=m_p^x(s)+\sum_v V_v\,y_{vp}(s),\quad p=\overline{1,m}, \tag{3.11}$$

координатные функции которого определяются формулой

$$y_{vp}(s)=\sum_{h=1}^{n}x_{vh}(t),\quad p=\overline{1,m}. \tag{3.12}$$

Матрица ковариационных функций векторной СФ $\mathbf{Y}(t)$ выразится через составляющие векторных координатных функций $\mathbf{y}_{vp}(s)=[y_{1v}(s)\ldots y_{mv}(s)]$ формулой

$$\mathbf{K}^y(s,s')=[K_{pq}^y(s,s')],\quad K_{pq}^y(s,s')=\sum_{h,l=1}^{n}D_v\mathbf{y}_{vp}(s)\overline{\mathbf{y}_{vq}(s')},\quad p,q=\overline{1,m}. \tag{3.13}$$

Таким образом, приходим к следующему утверждению.

Т е о р е м а 3.1. *Если операторы* $\mathbf{A}$ *и* $\mathbf{M}$ *переместительны и известно КР скалярного или векторного СтП* $\mathbf{X}$ *(3.1) или (3.10), то КР линейного преобразования (2.4.25) определяется соответственно формулами (3.2)−(3.5) или (3.11)−(3.13).*

4. Вейвлет аналитическое моделирование математического ожидания

4.1. Вводные замечания. Рассмотрим систему (2.1) на интервале времени $[t_0, T]$. С помощью замены переменных

$$\bar{t} = (t - t_0)(T - t_0)^{-1} \tag{4.1}$$

сведем (2.1) к соответствующему векторному линейному стохастическому уравнению

$$\mathbf{Y}' = \bar{\mathbf{a}}(\bar{t})\mathbf{Y} + \bar{\mathbf{a}}_0(\bar{t}) + \bar{\mathbf{b}}(\bar{t})\bar{\mathbf{V}}(\bar{t}) \tag{4.2}$$

на интервале $\bar{t} \in [0,1]$ с начальным условием

$$\mathbf{Y}(0) = \mathbf{Y}_0 \tag{4.3}$$

и белым шумом $\mathbf{V}$ с интенсивностью

$$\bar{\mathbf{v}}(\bar{t}) = v\left[(T - t_0)\bar{t} + t_0\right], \tag{4.4}$$

где приняты следующие обозначения:

$$\begin{aligned} &\mathbf{Y}(\bar{t}) = \mathbf{Y}\left[(t - t_0)\bar{t} + t_0\right], \quad \bar{\mathbf{V}}(\bar{t}) = \mathbf{V}\left[(T - t_0)\bar{t} + t_0\right], \quad \bar{\mathbf{a}}(\bar{t}) = (T - t_0)\mathbf{a}\left[(T - t_0)\bar{t} + t_0\right], \\ &\bar{\mathbf{a}}_0(\bar{t}) = (T - t_0)\mathbf{a}_0\left[(T - t_0)\bar{t} + t_0\right], \quad \bar{\mathbf{b}}(\bar{t}) = (T - t_0)\mathbf{b}\left[(T - t_0)\bar{t} + t_0\right]. \end{aligned} \tag{4.5}$$

Штрихом отмечена операция дифференцирования по безразмерному времени $\bar{t}$ согласно (4.1).

4.2. Уравнения для математических ожиданий. Будем использовать для уравнения

$$\mathbf{m}' = \bar{\mathbf{a}} + \bar{\mathbf{a}}_0, \tag{4.6}$$

определяющего математическое ожидание $\mathbf{m} = \mathbf{MY}$, вейвлет версию метода Галеркина–Петрова [10, 11]. Поэтому будем считать, что векторно-матричные функции $\mathbf{m}, \bar{\mathbf{a}}, \bar{\mathbf{a}}_0$ удовлетворяют условию

$$\mathbf{m}, \bar{\mathbf{a}}, \bar{\mathbf{a}}_0 \in L^2[0,1]. \tag{4.7}$$

В дальнейшем для простоты записи положим $t = \bar{t}$.

Как показано в [5], они могут быть разложены по ортогональным вейвлетам Хаара.

4.3. Базовый алгоритм. Следуя [5], определим ортонормированный базис Хаара в следующем виде:

$$w_1(t) = \phi(t) = \phi_{00}(t) = \begin{cases} 1 & \text{при} \quad t \in [0,1], \\ 0 & \text{при} \quad t \notin [0,1], \end{cases} \tag{4.8}$$

$$w_2(t) = \psi(t) = \psi_{00}(t) = \begin{cases} 1 & \text{при} \quad t \in [0,1/2], \\ -1 & \text{при} \quad t \in [1/2,1], \\ 0 & \text{при} \quad t \notin [0,1], \end{cases} \tag{4.9}$$

$$w_i(t) = \psi_{ik}(t) = \begin{cases} \sqrt{2^j} & \text{при} \quad t \in \left[\dfrac{k}{l}, \dfrac{k+0,5}{l}\right], \\ -\sqrt{2^j} & \text{при} \quad t \in \left[\dfrac{k+0,5}{l}, \dfrac{k+1}{l}\right], \\ 0 & \text{при} \quad t \notin \left[\dfrac{k}{l}, \dfrac{k+1}{l}\right], \end{cases} \tag{4.10}$$

где $\phi = \phi(t)$ – масштабирующая функция; $\psi = \psi(t)$ – материнский вейвлет;

$$\begin{aligned} &\phi_{jk} = \phi_{jk}(t) = \sqrt{2^j}\,\phi(2^j t - k); \quad \psi_{jk} = \psi_{jk}(t) = \sqrt{2^j}\,\phi(2^j t - k); \\ &k = 0, 1, \ldots, l-1; \quad i = l + k + 1; \quad i = \overline{2, 2L}; \quad L = 2^J; \end{aligned} \tag{4.11}$$

J – натуральное число, $J > 2$; индекс j в дальнейшем будем опускать.

Кроме того, определим интегралы от вейвлетов Хаара следующим образом:

$$p_i(t) = \int_0^t w_i(\tau) d\tau, \quad i = \overline{1, 2L}, \tag{4.12}$$

где

$$p_1(t) = \begin{cases} 1 & \text{при} \quad t \in [0,1], \\ 0 & \text{при} \quad t \notin [0,1], \end{cases} \qquad p_i(t) = \begin{cases} \sqrt{2^j}\left(t - \dfrac{k}{l}\right) & \text{при} \quad t \in \left[\dfrac{k}{l}, \dfrac{k+0,5}{l}\right], \\ \sqrt{2^j}\left(\dfrac{k+1}{l} - t\right) & \text{при} \quad t \in \left[\dfrac{k+0,5}{l}, \dfrac{k+1}{l}\right], \\ 0 & \text{при} \quad t \notin \left[\dfrac{k}{l}, \dfrac{k+1}{l}\right]. \end{cases}$$

Для каждой составляющей $m_h = m_h(t),\ h = \overline{1, p},$ вектора $\mathbf{m} = \mathbf{m}(t)$ уравнение (4.6) дает такие выражения:

$$\dot{m}_h = \sum_{k=1}^{p} a_{hk}(t) m_k(t) + a_{0k}(t). \tag{4.13}$$

Разложим $\dot{m}_h,\ h = \overline{1, p}$, по ортонормированному базису вейвлетов Хаара:

$$\dot{m}_h = \sum_{i=1}^{2L} c_{hi} w_i(t), \tag{4.14}$$

где

$$c_{hi} = \int_0^t \dot{m}_h(\tau) w_i(\tau) d\tau. \tag{4.15}$$

Тогда решение (4.13) относительно m_h можно представить в виде

$$m_h(t) = \int_0^t \sum_{i=1}^{2L} c_{hi} w_i(\tau) d\tau + m_{0h} = \sum_{i=1}^{2L} c_{hi} p_i(t) + m_{0h}, \quad h = \overline{1, p}. \tag{4.16}$$

После подстановки (4.14)–(4.16) в (4.13) получим соотношение

$$\sum_{i=1}^{2L} c_{hi} w_i(t) = \sum_{k=1}^{p} a_{hk}(t) \left[\sum_{i=1}^{2L} c_{hi} w_i(t) + m_{0h} \right]. \tag{4.17}$$

Проектируя (4.17) на базис $\overline{w}_i(t)$, приходим к системе $(2L \times p)$ линейных уравнений

$$\sum_{i=1}^{2L} c_{hi} \left[w_i(t), w_s(t) \right] = \sum_{k=1}^{p} \sum_{i=1}^{2L} c_{hi} a_{hi}(t) p_i(t), w_s(t) +$$

$$+ m_{0h} \sum_{k=1}^{p} \left[a_{hk}(t), w_s(t) \right] + \left[a_{0h}(t), w_s(t) \right], \quad s = \overline{1, 2L}, \quad l = \overline{1, p}. \tag{4.18}$$

В силу ортонормированности системы вейвлетов Хаара $\overline{w}_i(t)$ из (4.18) получаем

$$c_{hs} = \sum_{k=1}^{p} \sum_{i=1}^{2L} \left[a_{hk}(t) p_i(t), w_s(t) \right] + m_{0h} \sum_{k=1}^{p} \left[a_{hk}(t), w_s(t) \right] + \left[a_{0h}(t), w_s(t) \right], \quad s = \overline{1, 2L}, \quad h = \overline{1, p}. \tag{4.19}$$

Теперь с помощью MATLAB получим искомое разложение для следующих функций:

$$a_{hi}(t)p_i(t)=\sum_{j=1}^{2L} g_j^{hki} w_j(t), \quad i=\overline{1,2L}, \quad h=\overline{1,p}, \quad k=\overline{1,p}, \tag{4.20}$$

$$a_{hk}(t)=\sum_{j=1}^{2L} q_j^{hk} w_j(t), \quad h=\overline{1,p}, \quad k=\overline{1,p}, \qquad a_{0h}(t)=\sum_{j=1}^{2L} \rho_j^{h} w_j(t), \quad h=\overline{1,p}. \tag{4.21), (4.22}$$

Отсюда находим

$$g_s^{hki}=\left[a_{hk}\overline{=}p_i(t), \overline{=}w_s(t)\right], \quad q_s^{hi}=\left[a_{hk}, \overline{=}w_s(t)\right], \quad \rho_s^{h}=\left[a_{0h}, \overline{=}w_s(t)\right]. \tag{4.23}$$

В результате уравнения (4.19) можно записать в следующем окончательном виде:

$$\overline{=}c_{hs}=\sum_{k=1}^{p}\sum_{i=1}^{2L} c_{hi} g_s^{hki} + m_{0h} + m_{0h}\sum_{k=1}^{p} q_s^{hk} + \rho_s^{h}. \tag{4.24}$$

Полученный алгоритм можно сформулировать в виде следующей теоремы.

Т е о р е м а 4 . 1 . *Пусть вектор состояния* $\mathbf{Y}=\mathbf{Y}(t)$ *размерности* p *линейной дифференциальной СтС (4.1) допускает возможность приведения к (4.6). Тогда при заданном уровне разложения* J *вейвлет алгоритм аналитического моделирования математических ожиданий* m_h *в уравнениях (4.13) имеет вид (4.16) при следующих условиях:*

1) функции $p_i(t)$ *определяются из (4.12);*

2) коэффициенты c_{hs} *находятся из системы линейных уравнений (4.24);*

3) коэффициенты g_s^{hki}, q_s^{hk}, ρ_s^{h} *в (4.24) являются коэффициентами ортогонального разложения функций* $a_{hk}(t)p_i(t)$, $a_{hk}(t)$, $a_{0h}(t)$ *в (4.20)–(4.22) соответственно по системе вейвлетов Хаара (4.8)–(4.11) при заданном уровне разложения* J.

5. Вейвлет аналитическое моделирование ковариационной матрицы

Из (2.6) для каждого элемента $K_{r_1r_2}=K_{r_1r_2}(t)$ ковариационной матрицы $\mathbf{K}=\mathbf{K}(t)$ имеем систему обыкновенных дифференциальных уравнений

$$\dot{K}_{r_1r_2}(t)=\sum_{h=1}^{p} a_{r_1h}(t)K_{hr_2}(t)+\sum_{h=1}^{p} K_{r_1h}(t)a_{r_2h}(t)+\sum_{h=1}^{p}\sum_{s=1}^{n} b_{r_1h}(t)\nu_{hs}(t)b_{r_2s}(t), \quad K_{r_1r_2}(0)=K_{0r_1r_2}. \tag{5.1}$$

В силу симметричности ковариационной матрицы $\mathbf{K}$ достаточно составить уравнения только для $r_1=\overline{1,p}$, $r_2=\overline{r,p}$. При этом элементы K_{hr_2} для $h>r_2$ заменяются равными K_{r_2h}, а K_{r_1h} при $r_1>h$ заменяются на K_{hr_1}. В результате размерность ковариационной матрицы $\mathbf{K}$ будет равна $\dfrac{p(p+1)}{2}$.

Введем обозначение

$$B_{r_1r_2}(t)=\sum_{h=1}^{p}\sum_{s=1}^{n} b_{r_1h}(t)\nu_{hs}(t)b_{r_2s}(t), \tag{5.2}$$

тогда, повторяя рассуждение раздела 4, получим следующие формулы:

$$\dot{K}_{r_1r_2}(t)=\sum_{i=1}^{2L} c_i^{r_1r_2} w_i(t), \quad c_i^{r_1r_2}=\int_0^1 \dot{K}_{r_1r_2}(\tau)w_i(\tau)d\tau \quad K_{r_1r_2}(t)=\sum_{i=1}^{2L} c_i^{r_1r_2} p_i(t)+K_{0r_1r_2}. \tag{5.3), (5.4), (5.5}$$

После подстановки (5.2)–(5.5) в (5.1) найдем

$$\sum_{i=1}^{2L} c_i^{\eta_1 r_2} w_i(t) = \sum_{i=1}^{2L}\sum_{h=1}^{p} c_i^{hr_2} a_{\eta_1 h}(t) p_i(t) + \sum_{h=1}^{p} a_{\eta_1 h}(t) K_{0r_2} + \sum_{i=1}^{2L}\sum_{h=1}^{p} c_i^{\eta_1 h} a_{r_2 h}(t) p_i(t) + \sum_{h=1}^{p} a_{r_2 h}(t) K_{0\eta_1 h} + B_{\eta_1 r_2}(t). \quad (5.6)$$

Далее, проецируя (5.6) на базис $w_i(t)$, получим систему из $\frac{1}{2}\times p\times(p+1)\times 2L = p(p+1)L$ обыкновенных линейных уравнений для определения коэффициентов $\overline{\overline{c_i^{\eta_1 r_2}}}$:

$$\sum_{i=1}^{2L} c_i^{\eta_1 r_2}\left(w_i(t), w_s(t)\right) = \sum_{i=1}^{2L}\sum_{h=1}^{\overline{p}} c_i^{hr_2}\left(a_{\eta_1 h}(t) p_i(t), w_s(t)\right) + \sum_{i=1}^{2L}\sum_{h=1}^{p} c_i^{\eta_1 h}\left(a_{r_2 h}(t) p_i(t), w_s(t)\right) +$$

$$+\sum_{h=1}^{p} K_{0hr_2}\left(a_{\eta_1 h}(t), w_s(t)\right) + \sum_{h=1}^{p} K_{0\eta_1 h}\left(a_{r_2 h}(t), w_s(t)\right) + \left(B_{\eta_1 r_2}(t), w_s(t)\right) \quad (5.7)$$

$(r_1 = \overline{1, p}, \quad r_2 = \overline{r_1, p}, \quad s = \overline{1, 2L}).$

С помощью MATLAB находим разложение функций $B_{\eta_1 r_2}(t)$ по системе вейвлетов Хаара $w_j(t)$:

$$B_{\eta_1 r_2}(t) = \sum_{j=1}^{2L} \rho_j^{\eta_1 r_2} w_j(t), \quad (5.8)$$

где

$$\rho_j^{\eta_1 r_2} = \left(B_{\eta_1 r_2}(t), w_j(t)\right). \quad (5.9)$$

Наконец, учитывая ортонормированность вейвлетов Хаара из (5.8) и обозначения (4.22)−(4.24), получим окончательные выражения для коэффициентов $\overline{\overline{c_s^{\eta_1 r_2}}}$:

$$c_s^{\eta_1 r_2} = \sum_{i=1}^{2L}\sum_{h=1}^{p} c_i^{hr_2} g_s^{r_1 hi} + \sum_{i=1}^{2L}\sum_{h=1}^{p} c_i^{\eta_1 h} g_s^{r_2 hi} + \sum_{h=1}^{p} K_{0hr_2} q_s^{\eta_1 h} + \sum_{h=1}^{p} K_{0\eta_1 h} q_s^{r_2 h} + \rho_s^{\eta_1 r_2}. \quad (5.10)$$

Таким образом, приходим к искомому базовому алгоритму.

Т е о р е м а 5 . 1 . *Пусть вектор состояния* $\mathbf{Y} = \mathbf{Y}(t)$ *размерности* $\overline{\overline{p}}$ *линейной дифференциальной системы (4.1) допускает возможность приведения к (4.6). Тогда при заданном уровне разложения* J *вейвлет алгоритм аналитического моделирования ковариационной матрицы при* $r_1 = \overline{1, p}$, $r_2 = \overline{r_1, p}$ *имеет вид (5.5), в котором*

1) функции $p_i(t)$ *описываются формулами (4.12);*

2) коэффициенты $c_i^{\eta_1 r_2}$ *определяются из системы линейных алгебраических уравнений (5.10);*

3) коэффициенты $g_s^{\eta_1 hi}$, $g_s^{r_2 hi}$, $q_s^{\eta_1 h}$, $q_s^{r_2 h}$, $\rho_s^{\eta_1 r_2}$ *в (5.10) являются коэффициентами ортогонального разложения функций* $a_{\eta_1 h}(t)p_i(t)$, $a_{r_2 h}(t)p_i(t)$, $a_{\eta_1 h}(t)$, $a_{r_2 h}(t)$ *и* $B_{\eta_1 r_2}(t)$ *по системе вейвлетов Хаара при заданном уровне разложения* J.

6. Вейвлет аналитическое моделирование ковариационных функций

Из (2.8)−(2.10) для элемента $K_{\eta_1 r_2}(t_1, t_2)$ матрицы ковариационных функций $\mathbf{K}(t_1, t_2)$ в момент t_2 имеем обыкновенное дифференциальное уравнение с соответствующим начальным условием

$$\frac{\partial K_{\eta_1 r_2}(t_1, t_2)}{\partial t_2} = \sum_{h=1}^{p} K_{\eta_1 h}(t_1, t_2) a_{r_2 h}(t_2), \quad (6.1)$$

$$K_{\eta_1 r_2}(t, t) = K(t), \quad r_1, r_2 = \overline{1, p}, \ t_1, t_2 \in [0,1], \ t_1 < t_2. \quad (6.2)$$

Повторяя рассуждения разделов 4 и 5, придем к следующим соотношениям:

$$\frac{\partial K_{\eta r_2}(t_1,t_2)}{\partial t_2}=\sum_{i_1=1}^{2\mathrm{L}}\sum_{i_2=1}^{2L} d_{i_1 i_2}^{\eta_1 r_2} w_{i_1}(t_1) w_{i_2}(t_2)\,,\quad d_{i_1 i_2}^{\eta_1 r_2}=\int_0^1\int_0^1 \frac{\partial K_{\eta r_2}(\tau_1,\tau_2)}{\partial \tau_2} w_{i_1}(\tau_1) w_{i_2}(\tau_2) d\tau_1 d\tau_2 \qquad (6.3),\ (6.4)$$

$$K_{\eta r_2}(t_1,t_2)=\sum_{i_1=1}^{2\mathrm{L}}\sum_{i_2=1}^{2L} d_{i_1 i_2}^{\eta_1 r_2} w_{i_1}(t_1) p_{i_2}(t_2)+\sum_{i=1}^{2L} c_i^{\eta_1 r_2} p_i(t_1)+K_{0\eta r_2}\,, \qquad (6.5)$$

$$\sum_{i_1=1}^{2\mathrm{L}}\sum_{i_2=1}^{2L} d_{i_1 i_2}^{\eta_1 r_2} w_{i_1}(t_1) w_{i_2}(t_2)=\sum_{h=1}^{p} a_{r_2 h}(t_2)\left[\sum_{i_1=1}^{2\mathrm{L}}\sum_{i_2=1}^{2L} d_{i_1 i_2}^{\eta_1 h} w_{i_1}(t_1) p_{i_2}(t_2)+\sum_{i=1}^{2L} c_i^{\eta_1 h} p_i(t_1)+K_{0\eta r_2}\right]. \qquad (6.6)$$

Проецируя (6.6) на базис $w_{s_1}(t_2)$, получим следующую систему $\frac{p(p+1)}{2}\times 2L = p(p+1)L$ уравнений:

$$\sum_{i_1=1}^{2\mathrm{L}}\sum_{i_2=1}^{2L} d_{i_1 i_2}^{\eta_1 r_2} w_{i_1}(t_1)\left[w_{i_2}(t_2), w_{s_2}(t_2)\right]=\sum_{h=1}^{p}\sum_{i_1=1}^{2\mathrm{L}}\sum_{i_2=1}^{2L} d_{i_1 i_2}^{r_2 h} w_{i_1}(t_1)\left[a_{r_2 h}(t_2) p_{i_2}(t_2), w_{s_1}(t_2)\right]+$$

$$+\sum_{h=1}^{p}\sum_{i=1}^{2L} c_i^{\eta_1 h} p_i(t_1)\left[a_{r_2 h}(t_2), w_{s_1}(t_2)\right]+K_{0\eta r_2}\sum_{h=1}^{p}\left[a_{r_2 h}(t_2), w_{s_1}(t_2)\right], \qquad (6.7)$$

$$\sum_{i_1=1}^{2\mathrm{L}} d_{i_1 s_1}^{\eta_1 r_2} w_{i_1}(t_1)=\sum_{h=1}^{p}\sum_{i_1=1}^{2\mathrm{L}}\sum_{i_2=1}^{2L} d_{i_1 i_2}^{\eta_1 h} g_{s_1}^{r_2 h i_2} w_{i_1}(t_1)+\sum_{h=1}^{p}\sum_{i=1}^{2L} c_i^{\eta_1 h} p_i(t_1) q_{s_1}^{r_2 h}+K_{0\eta r_2}\sum_{h=1}^{p} q_{s_1}^{r_2 h}\,. \qquad (6.8)$$

Проектируя (6.8) на базис $\overline{\overline{W}}_{s_2}(t_1)$, получим систему $p(p+1)\times L\times 2L = 2\overline{\overline{p}}(p+1)L^2$ обыкновенных линейных уравнений

$$\sum_{i_1=1}^{2\mathrm{L}} d_{i_1 s_1}^{\eta_1 r_2}\left[w_{i_1}(t_1), w_{s_2}(t_1)\right]=\sum_{h=1}^{p}\sum_{i_1=1}^{2\mathrm{L}}\sum_{i_2=1}^{2L} d_{i_1 i_2}^{\eta_1 r_2} g_{s_1}^{r_2 h i_2}\left[w_{i_1}(t_1), w_{s_2}(t_1)\right]+$$

$$+\sum_{h=1}^{p}\sum_{i=1}^{2L} c_i^{\eta_1 h} q_{s_1}^{r_2 h}\left[p_i(t_1), w_{s_2}(t_1)\right]+\sum_{h=1}^{p}\left[K_{0\eta r_2} q_{s_1}^{r_2 h}, w_{s_2}(t_1)\right]. \qquad (6.9)$$

Далее примем во внимание соотношения

$$p_i(t_1)=\sum_{j=1}^{2L} u_j^i w_j(t_1)\,,\qquad u_j^i=\left[\overline{\overline{p}}_i(t_1), \overline{\overline{W}}_j(t_1)\right]. \qquad (6.10),\ (6.11)$$

Если $s_2=1$, то

$$w_1(t_1)=\begin{cases}1 & \text{при} \quad t_1\in[0,1],\\ 0 & \text{при} \quad t_1\notin[0,1],\end{cases}\qquad \int_0^1 K_{0\eta r_2} q_{s_1}^{r_2 h} w_1(\tau_1) d\tau_1=\int_0^1 K_{0\eta r_2} q_{s_1}^{r_2 h}\,. \qquad (6.12),\ (6.13)$$

Если $s_2=\overline{2,2\mathrm{L}}$, то

$$\int_0^1 w_{s_2}(t_1) dt_1=0\,,\qquad \int_0^1 K_{0\eta r_2} q_{s_1}^{r_2 h}\overline{\overline{W}}_{s_2}(t_1) dt_1\,. \qquad (6.14),\ (6.15)$$

Наконец, учитывая (6.13)–(6.15), получим для определения коэффициентов $d_{i_1 i_2}^{\eta_1 r_2}$ систему обыкновенных линейных уравнений (6.5):

$$d_{1 s_1}^{\eta_1 r_2}=\sum_{h=1}^{p}\sum_{i_2=1}^{2L} d_{1 i_2}^{\eta_1 h} g_{s_1}^{r_2 h i_2}+\sum_{h=1}^{p}\sum_{i=1}^{2L} c_i^{\eta_1 h} q_{s_1}^{r_2 h} u_1^i+\sum_{h=1}^{p} K_{0\eta r_2} q_{s_1}^{r_2 h}\,, \qquad (6.16)$$

$$d^{r_1 r_2}_{s_2 s_1} = \sum_{h=1}^{\overline{=}p} \sum_{i_2=1}^{2L} d^{r_1 r_2}_{s_2 i_2} g^{r_2 h i_2}_{s_1} + \sum_{h=1}^{\overline{=}p} \sum_{i=1}^{2L} {}^{=r_1 h}c_i \, q^{r_2 h}_{s_1} u^{i}_{s_2}, \quad s_2 = \overline{2, 2L}, \; r_1 = \overline{1, p}, \quad r_2 = \overline{r_1, p}, \; s_1 = \overline{1, 2L}. \tag{6.17}$$

Полученные результаты можно сформулировать в виде следующего утверждения.

Т е о р е м а 6 . 1 . *В условиях теорем 4.1 и 5.1 алгоритма вычисления элементов матрицы ковариационных функций, удовлетворяющих (6.1), лежат соотношения (6.5), в которых*

1) функции $W_{i_1}(t_1)$ *имеют вид (4.8)−(4.10);*

2) функции $p_{i_2}(t_2)$ *имеют вид (4.12);*

3) коэффициенты $d^{r_1 r_2}_{i_1 i_2}$ *определяются (6.16);*

4) коэффициенты $q^{r_2 h i_2}_{s}, q^{r_2 h}_{s_1}$ *в (6.16) являются коэффициентами ортонормального разложения функций* $a_{r_2 h}(t) p_{i_2}(t)$, $a_{r_2 h}(t)$, $p_{i_2}(t)$ *по системе вейвлетов Хаара при заданном уровне разложения* J.

7. Применение КРВЛ для экспресс аналитического моделирования

Как следует из теоремы 3.1, применение КРВЛ сводится к построению КРВЛ выходного СтП $\mathbf{Y}$ на основе КРВЛ входного СтП. При этом в силу линейности преобразований оказывается достаточным найти вейвлет решение только одного и того же уравнения для выходных координатных функций КРВЛ $\mathbf{Y}$. Соответствующие алгоритмы получены в разделе 4. Для вычисления ковариационной матрицы и матрицы ковариационных функций достаточно воспользоваться конечными формулами (3.10)−(3.13).

При использовании теорем 4.1, 5.1 и 6.1 порядок уравнений (2.5), (2.6), (2.8) равен $Q = p(p+3)/2$, а при использовании КР достаточно проинтегрировать N_p уравнений для координатных функций, а элементы ковариационной матрицы и матрицы ковариационных функций вычислить по конечным формулам, удержав в КР N членов.

Например [5], для СтС при $p = 100$, $Q = 5150$ и для широкополосной системы с относительной погрешностью по дисперсии 10% достаточно ограничиться $N = 13$ членами КР. Как показано в [1, 2], применение КРВЛ позволяет дополнительно сократить время интегрирования уравнений для координатных функций (приложение 1).

Как показано в [5], для узкополосной системы на частоте ω с точностью до 100% достаточно ограничиться одним членом КР. Применение КРВЛ позволяет вместо интегрирования уравнения для координатной функции использовать конечное вейвлет уравнение (приложение 2).

8. Обобщения КРВЛ

Полученные в [5] обобщения известных ковариационных теорем Пугачева обобщаются на случай, когда с ядром $K(t,s)$ интегрального уравнения, определяющего собственные функции, ассоциируется билинейный функционал. Обозначим через χ^B_H полное линейное пространство, полученное из банахова пространства χ^B введением скалярного произведения для соответствующего гильбертова пространства

$$\langle \mathbf{X}, \mathbf{Y} \rangle = \sum_{v=1}^{\infty} (f_v \, \mathbf{X})(f_v \, \mathbf{Y}). \tag{8.1}$$

Тогда для случайной величины $\mathbf{X}$ и ее ковариационного оператора $\mathbf{K}^{\mathbf{X}}$ имеют место следующие КР:

$$\mathbf{X} = \mathbf{m}^{\mathbf{X}} + \sum_{v=1}^{\infty} V_v \, \mathbf{x}_v, \quad \mathbf{K}^{\mathbf{X}} f = \sum_{v=1}^{\infty} f(x_v) \mathbf{x}_v \quad f \in \chi, \tag{8.2}$$

с.к. сходящиеся в топологии, порожденной нормой пространства χ^B_H.

Т е о р е м а 8 . 1 . *Пусть ни один из векторов* $\mathbf{x}_v$ *не принадлежит замкнутой линейной оболочке остальных векторов, то есть замкнутому в слабой топологии пространства* χ_H^B *подпространству* χ_{vH}^B, *образованному последовательностью* $\{\mathbf{x}_\mu\}_{\mu\neq v}$. *Тогда КР ковариационного оператора* $\mathbf{K}^{\mathbf{X}}$ *соответствует КР случайной величины* $\mathbf{X}$.

Полученные результаты для действительных случайных величин легко обобщаются на случай банаховых пространств под полем комплексных чисел путем замены симметричного билинейного на эрмитовый билинейный функционал.

- Статья посвящена развитию инструментального программного обеспечения анализа линейных нестационарных дифференциальных систем на основе теории вейвлетов в среде MATLAB. Получены вейвлет алгоритмы аналитического моделирования векторов математических ожиданий, ковариационных матриц и матриц ковариационных функций.

  Использование вейвлет канонических разложений для систем высокой доступности и алгоритмов разряженных матриц [13, 14] позволяет существенно сократить объем вычислений даже при применении последовательных алгоритмов декорреляции.

  Приведены тестовые примеры, обобщающие полученные результаты.

  В качестве первого обобщения изложенных алгоритмов для линейных нестационарных СтС можно рассмотреть линейные СтС со случайными параметрическими шумами. Вторым важным обобщением могут служить алгоритмы, основанные на статистической линеаризации нелинейных преобразований с последующим использованием методов теории линейных систем.

ПРИЛОЖЕНИЕ 1

Рассмотрим одномерную стационарную линейную СтС [3, 4]

$$\dot{Y} = \beta Y + \sqrt{2\alpha\beta}V, \quad Y(0) = Y_0, \quad t \in [0,1], \tag{П.1}$$

где V – одномерный белый шум единичной интенсивности $v = 1$.

Уравнения (2.5), (2.6), (2.8) в этом случае принимают вид

$$\dot{m} = -\alpha m, \quad m(0) = m_0, \tag{П.2}$$

$$\dot{D} = -2\alpha D + 2\alpha\beta, \quad D(0) = D_0, \tag{П.3}$$

$$\frac{\partial K(t_1, t_2)}{\partial t_2} = -\alpha K(t_1, t_2) + 2\alpha\beta, \quad K(t_1, t_1) = D(t_1). \tag{П.4}$$

В соответствии с теоремой 4.1 решение (П.2) дается формулой

$$m(t) = \sum_{i=1}^{2L} c_i\, p_i(t) + m_0, \tag{П.5}$$

где коэффициенты c_i определяются из системы линейных алгебраических уравнений

$$c_1 = -\alpha \sum_{i=1}^{2L} c_i u_1^i - \alpha m_0, \quad c_s = -\alpha \sum_{i=1}^{2L} c_i u_s^i, \quad s = \overline{2, 2L}. \tag{П.6}$$

Коэффициенты u_j^i для $i, j = \overline{1, 2L}$ являются коэффициентами разложения функций (4.12) по системе вейвлетов Хаара (4.8)–(4.10) при заданном J, $L = 2^J$:

$$p_i(t) = \sum_{j=1}^{2L} u_j^i w_j(t), \quad u_{js}^i = \int_0^1 p_i(\tau) w_j(\tau) d\tau. \tag{П.7}$$

В соответствии с теоремой 5.1 решение (П.3) принимает вид

$$D(t) = \sum_{i=1}^{2L} c_i^{11} p_i(t) + D_0. \qquad (П.8)$$

Здесь коэффициенты c_i^{11} определяются из системы линейных алгебраических уравнений

$$c_1^{11} = -2\alpha \sum_{i=1}^{2L} c_i^{11} u_1^i - 2\alpha D_0 + 2\alpha\beta, \quad c_s^{11} = -2\alpha \sum_{i=1}^{2L} c_i^{11} u_s^i, \qquad (П.9)$$

где u_j^i находятся из (П.3) с помощью MATLAB.

Наконец, в соответствии с теоремой 6.1 получаем, что решение уравнения (П.4) имеет вид

$$K(t_1, t_2) = \sum_{i_1=1}^{2L} \sum_{i_2=1}^{2L} d_{i_1 i_2} w_{i_1}(t_1) p_{i_2}(t_2) + D(t_1), \qquad (П.10)$$

где

$$\begin{aligned} &d_{11} = -\alpha \sum_{j=1}^{2L} (d_{1i} + c_i^{11}) u_1^i + \alpha D_0; \quad d_{1s_1} = -\alpha \sum_{j=1}^{2L} d_{1i} u_{s_1}^i, \quad s_1 = \overline{2,2L}; \\ &d_{s_2 1} = -\alpha \sum_{j=1}^{2L} (d_{s_2 i} + c_i^{11}) u_{s_2}^i, \quad s_2 = \overline{2,2L}; \quad d_{s_2 s_1} = -\alpha \sum_{j=1}^{2L} d_{s_2} u_{s_1}^i, \quad s_1, s_2 = \overline{2,2L}; \end{aligned} \qquad (П.11)$$

u_j^i определяются из (П.6); c_i^{11} являются решением уравнений (П.7).

ПРИЛОЖЕНИЕ 2

Пусть задана линейная двумерная стационарная СтС [3, 4]

$$\dot{Y}_1 = Y_2 + \beta_1 V, \quad \dot{Y}_2 - \omega^2 Y_1 - 2\varepsilon\omega Y_2 + \beta_2 V, \quad Y_1(0) = Y_{01}, \quad Y_2(0) = Y_{02}, \quad t \in [0,1], \qquad (П.12)$$

где V – скалярный белый шум интенсивности $v = 1$.

Уравнения для первых двух вероятностных моментов (2.5), (2.6), (2.8) имеют вид

$$\dot{m} = \begin{bmatrix} \dot{m}_1 \\ \dot{m}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -\omega^2 & -2\varepsilon\omega \end{bmatrix}, \quad m(0) = \begin{bmatrix} m_{01} \\ m_{02} \end{bmatrix}, \qquad (П.13)$$

$$\dot{K} = \begin{bmatrix} 0 & 1 \\ -\omega^2 & -2\varepsilon\omega \end{bmatrix} K + K \begin{bmatrix} 0 & -\omega^2 \\ 1 & -2\varepsilon\omega \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix} [\beta_1 \beta_2], \quad K(0) = [K_{0ij}], \qquad (П.14)$$

$$\frac{\partial K(t_1, t_2)}{\partial t_2} = K(t_1, t_2) \begin{bmatrix} 0 & -\omega^2 \\ 1 & -2\varepsilon\omega \end{bmatrix}, \quad K(t_1, t_1) = K(t_1). \qquad (П.15)$$

В соответствии с теоремой 4.1 имеем следующие соотношения для аналитического моделирования математических ожиданий:

$$m_1(t) = \sum_{i=1}^{2L} c_{1i} p_i(t) + m_{01}, \quad m_2(t) = \sum_{i=1}^{2L} c_{2i} p_i(t) + m_{02}, \qquad (П.16)$$

где коэффициенты c_{1i} и c_{2i} определяются из системы линейных алгебраических уравнений

$$c_{1s} = \sum_{i=1}^{2L} c_{1i} (g_s^{11i} + g_s^{12i}) + m_{01}(g_s^{11} + g_s^{12}), \quad c_{2s} = \sum_{i=1}^{2L} c_{2i} (g_s^{21i} + g_s^{22i}) + m_{02}(g_s^{21} + g_s^{22}), \quad s = \overline{1,2L}, \qquad (П.17)$$

где

$$g_j^{11i} = 0; \quad g_j^{12i} = u_j^i; \quad g_j^{21i} = -\omega^2 u_j^i; \quad g_j^{22i} = -2\varepsilon\omega u_j^i; \qquad (П.18)$$

$$q_j^{11}=0,\quad j=\overline{1,2l};\quad q_1^{12}=1;\quad q_s^{12}=0,\quad s=\overline{2,2L};\quad q_1^{21}=-\omega^2;$$
$$q_s^{21}=0,\quad s=\overline{2,2L};\quad q_1^{22}=-2\varphi\omega;\quad q_s^{22}=0,\quad s=\overline{2,2L}. \tag{П.19}$$

Уравнения (П.17) с учетом (П.18) и (П.19) принимают следующий окончательный вид:

$$c_{11}=\sum_{i=1}^{2L}c_{1i}u_1^i+m_{01},\quad c_{1s}=\sum_{i=1}^{2L}c_{1i}u_s^i,\quad s=\overline{2,2L},\quad c_{21}=-2\omega(\omega+\varepsilon)\sum_{i=1}^{2L}c_{2i}u_1^i-m_{02}\omega(\omega+2\varepsilon),$$
$$c_{2s}=-2\omega(\omega+\varepsilon)\sum_{i=1}^{2L}c_{2i}u_s^i,\quad s=\overline{2,2L}. \tag{П.20}$$

В соответствии с теоремой 5.1 приходим к соотношениям

$$K_{11}(t)=\sum_{i=1}^{2L}c_i^{11}p_i(t)+K_{01},\quad K_{12}(t)=\sum_{i=1}^{2L}c_i^{12}p_i(t)+K_{012}=K_{21},\quad K_{22}(t)=\sum_{i=1}^{2L}c_i^{22}p_i(t)+K_{022}, \tag{П.21}$$

где коэффициенты $c_i^{11},c_i^{12},c_i^{22}$ находятся из системы линейных алгебраических уравнений

$$c_s^{11}=2\sum_{i=1}^{2L}c_i^{11}g_s^{11i}+2\sum_{i=1}^{2L}c_i^{12}g_s^{12i}+2K_{01}q_s^{11}+2K_{012}q_s^{12}+\rho_s^{11},$$
$$c_s^{12}=\sum_{i=1}^{2L}c_i^{12}\left(g_s^{11i}+g_s^{22i}\right)+\sum_{i=1}^{2L}c_i^{22}g_s^{12i}+\sum_{i=1}^{2L}c_i^{11}g_s^{21i}+K_{012}\left(q_s^{11}+q_s^{22}\right)+K_{022}q_s^{12}+K_{011}q_s^{21}+\rho_s^{12}, \tag{П.22}$$
$$c_s^{22}=2\left[\sum_{i=1}^{2L}c_i^{12}g_s^{21i}+\sum_{i=1}^{2L}c_i^{22}g_s^{22i}+K_{012}q_s^{21}+K_{022}q_s^{22}\right]+\rho_s^{22}.$$

Учитывая соотношения

$$B_{11}=\rho_1^{11}=\beta_1^2,\quad B_{22}=\rho_1^{22}=\beta_2^2,\quad B_{12}=B_{21}=\rho_1^{12}=\rho_1^{21}=\beta_1\beta_2, \tag{П.23}$$

представим (П.22) в следующем окончательно виде:

$$c_1^{11}=2\sum_{i=1}^{2L}c_i^{12}u_1^i+\beta_i^2g_s^{12i}+2K_{012},\quad c_s^{11}=2\sum_{i=1}^{2L}c_i^{12}u_s^i,\quad s=\overline{2,2L},$$
$$c_1^{12}=-2\varepsilon\omega\sum_{i=1}^{2L}c_i^{12}u_1^i+\sum_{i=1}^{2L}c_i^{22}u_1^i-\omega^2\sum_{i=1}^{2L}c_i^{11}u_1^i+K_{022}-\omega^2K_{011}-2\varepsilon\omega K_{012}+\beta_1\beta_2,$$
$$c_s^{12}=-2\varepsilon\omega\sum_{i=1}^{2L}c_i^{12}u_s^i+\sum_{i=1}^{2L}c_i^{22}u_s^i-\omega^2\sum_{i=1}^{2L}c_i^{11}u_s^i, \tag{П.24}$$
$$c_1^{22}=-2\omega^2\sum_{i=1}^{2L}c_i^{12}u_1^i-4\varepsilon\omega\sum_{i=1}^{2L}c_i^{22}u_1^i-2\omega^2K_{012}-4\varepsilon\omega K_{022}+\beta_2^2,$$
$$c_s^{22}=-2\omega^2\sum_{i=1}^{2L}c_i^{12}u_s^i-4\varepsilon\omega\sum_{i=1}^{2L}c_i^{22}u_s^i,\quad s=\overline{2,2L}.$$

В соответствии с теоремой 6.1 решение (П.15) принимает вид

$$K_{11}(t_1,t_2)=\sum_{i_1=1}^{2L}\sum_{i_2=1}^{2L}d_{i_1i_2}^{11}w_{i_1}(t_1)p_{i_2}(t_2)+K_{11}(t_1),\quad K_{12}(t_1,t_2)=\sum_{i_1=1}^{2L}\sum_{i_2=1}^{2L}d_{i_1i_2}^{12}w_{i_1}(t_1)p_{i_2}(t_2)+K_{12}(t_1),$$
$$K_{22}(t_1,t_2)=\sum_{i_1=1}^{2L}\sum_{i_2=1}^{2L}d_{i_1i_2}^{22}w_{i_1}(t_1)p_{i_2}(t_2)+K_{22}(t_1),\quad K_{21}(t_1,t_2)=K_{12}(t_1,t_2), \tag{П.25}$$

где коэффициенты $d^{11}_{i_1 i_2}$, $d^{12}_{i_1 i_2}$ и $d^{22}_{i_1 i_2}$ определяются из системы линейных алгебраических уравнений

$$
\begin{aligned}
&d^{11}_{11} = \sum_{i=1}^{2L} d^{12}_{1i} u^i_1 + \sum_{i=1}^{2L} d^{12}_{1i} u^i_1 + K_{011}, \quad d^{11}_{1s} = \sum_{i=1}^{2L} d^{12}_{1i} u^i_s, \quad s = \overline{2,2L},\\
&d^{12}_{11} = -\omega^2 \sum_{i=1}^{2L} d^{11}_{1i} u^i_1 - 2\varepsilon\omega \sum_{i=1}^{2L} d^{12}_{1i} u^i_1 - \omega^2 \sum_{i=1}^{2L} c^{11}_i (u^i_1)^2 - 2\omega \sum_{i=1}^{2L} c^{12}_i (u^i_1)^2 - K_{012}\omega(\omega + 2\varepsilon),\\
&d^{12}_{1s} = -\omega^2 \sum_{i=1}^{2L} d^{11}_{1i} u^i_s - 2\varepsilon\omega \sum_{i=1}^{2L} d^{12}_{1i} u^i_s, \quad s = \overline{2,2L},\\
&d^{22}_{11} = -\omega^2 \sum_{j=1}^{2L} d^{21}_{1i} u^i_1 - 2\varepsilon\omega \sum_{i=1}^{2L} d^{22}_{1i} u^i_1 - \omega^2 \sum_{i=1}^{2L} c^{21}_i u^i_1 - 2\omega \sum_{i=1}^{2L} c^{22}_i u^i_1 - \omega(\omega + 2\varepsilon) K_{022},\\
&d^{22}_{1s} = -\omega^2 \sum_{i=1}^{2L} d^{21}_{1i} u^i_s - 2\varepsilon\omega \sum_{i=1}^{2L} d^{22}_{1i} u^i_s, \quad s = \overline{2,2L},\\
&d^{11}_{s1} = \sum_{i=1}^{2L} d^{12}_{1i} u^i_s + \sum_{i=1}^{2L} c^{12}_i u^i_s, \quad s = \overline{2,2L}, \qquad d^{11}_{s_2 s_1} = \sum_{i=1}^{2L} d^{12}_{s_2 i} u^i_{s_1}, \quad s_1, s_2 = \overline{2,2L},\\
&d^{12}_{s_1} = -\omega^2 \sum_{i=1}^{2L} d^{11}_{si} u^i_1 - 2\varepsilon\omega \sum_{i=1}^{2L} d^{12}_{si} u^i_1 - \omega^2 \sum_{i=1}^{2L} c^{11}_i u^i_s - 2\varepsilon\omega \sum_{i=1}^{2L} c^{12}_i u^i_s, \quad s = \overline{2,2L},\\
&d^{12}_{s_2 s_1} = -\omega^2 \sum_{i=1}^{2L} d^{11}_{s_2 i} u^i_{s_1} - 2\varepsilon\omega \sum_{i=1}^{2L} d^{12}_{s_2 i} u^i_{s_1}, \quad s_2, s_1 = \overline{2,2L},\\
&d^{22}_{s_1} = -\omega^2 \sum_{i=1}^{2L} d^{21}_{si} u^i_1 - 2\varepsilon\omega \sum_{i=1}^{2L} d^{22}_{si} u^i_1 - \omega^2 \sum_{i=1}^{2L} c^{21}_i u^i_s - 2\varepsilon\omega \sum_{i=1}^{2L} c^{22}_i u^i_s, \quad s = \overline{2,2L},\\
&d^{22}_{s_2 s_1} = -\omega^2 \sum_{i=1}^{2L} d^{21}_{s_2 i} u^i_{s_1} - 2\varepsilon\omega \sum_{i=1}^{2L} d^{212}_{s_2 i} u^i_{s_1}, \quad s_1, s_2 = \overline{2,2L},
\end{aligned}
\tag{П.26}
$$

где u^i_j определяются из (П.6), а c^{11}_i являются решением уравнений (П.7).

Литература

1. *Синицын И.Н.*, *Сергеев И.В.*, *Корепанов Э.Р.*, *Конашенкова Т.Д.* Инструментальное программное обеспечение анализа и синтеза стохастических систем высокой доступности (IV) // Системы высокой доступности. 2017. Т. 13. № 3. С. 55−69.
2. *Синицын И.Н.*, *Синицын В.И.*, *Корепанов Э.Р.*, *Белоусов В.В.*, *Конашенкова Т.Д.*, *Сергеев И.В.*, *Семендяев Н.Н.*, *Басилашвили Д.А.* Инструментальное программное обеспечение анализа и синтеза систем высокой доступности (V) // Системы высокой доступности. 2018. Т. 14. № 1. С. 59−70.
3. *Пугачев В.С.*, *Синицын И.Н.* Теория стохастических система. М.: Логос. 2000. 2004. 1000 с.
4. *Синицын И.Н.*, *Синицын В.И.* Лекции по нормальной и эллипсоидальной аппроксимации в стохастических системах. М.: Торус Пресс. 2013. 488 с.
5. *Синицын И.Н.* Канонические представления случайных функций и их применения в задачах компьютерной поддержки научных исследований. М.: Торус Пресс. 2009.
6. *Синицын И.Н.*, *Сергеев И.В.*, *Корепанов Э.Р.*, *Конашенкова Т.Д.* Стохастические канонические вейвлет разложения в задачах моделирования виброударонадежности компьютерного оборудования // XVIII Междунар. научн. конф. «Системы компьютерной математики и их приложения» (СКМП-2017). Смоленск. 19−21 мая 2017 г. Смоленск: изд-во СмолГу. С. 123−124.
7. *Синицын И.Н.*, *Сергеев И.В.*, *Агафонов Е.С.* Применение канонических представлений случайных функций в задачах расчета виброзащитных систем для компьютерного оборудования // Материалы XI Междунар. научн. конф. «Системы компьютерной математики и их приложения», посвященной 70-летию профессора В.П. Дьяконова. Смоленск: изд-во СмолГу. 2010. № 11. С. 239−241.
8. *Синицын И.Н., Сергеев И.В.* Методическое обеспечение измерения, контроля и испытаний вычислительного оборудования в условиях ударных воздействий // Труды конф. «Технические и программные средства систем управления, контроля и измерения» (УКИ-2010). М.: ИПУ РАН. 2010. С. 47−56.
9. *Добеши И.* Десять лекций по вейвлетам. Москва–Ижевск: НИЦ «Регулярная и хаотическая динамика». 2004. 464 с.

10. *Xu J. and Shann W.* Galerkin-wavelet methods for two point value problems // Numer. Math. 1992. № 63. P. 123–144.
11. *Gagnon L. and Lina J.M.* Symmetric Daubechies' wavelets and numerical solutions of NLS2 equations // J. Phys. A: Math. Gen. 1994. № 27. P. 8207–8230.
12. *Lepik U.* Numeral solution of evolution equations by the Haar wavelet metods // Appl. Math. Comput. 2007. № 185. P. 695–704.
13. *Lepik U.* Application of the Haar wavelet transform to solving integral and differential equations // Proc. Estonian Acad. Sci. Phys. Math. 2007. № 56. P. 28–46.
14. *Писсанецки С.* Технология разреженных матриц. М.: Мир. 1988. 412 с.

Поступила ██ ██████ 20██ г.

Software tools for analysis and synthesis of stochastic systems with high availability (VI)

© Authors, 2018
© Radiotekhnika, 2018

I.N. Sinitsyn – Dr.Sc.(Eng.), Professor, Main Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: sinitsin@dol.ru
I.V. Sergeev – Ph.D.(Eng.), Deputy Director, FRC «Computer Science and Control» RAS (Moscow)
E-mail: isergeev@ipiran.ru
E.R. Korepanov – Ph.D.(Eng.), Leading Research Scientist, FRC «Computer Science and Control» RAS (Moscow)
E-mail: ekorepanov@ipiran.ru
T.D. Konashenkova – Leading Programmer, FRC «Computer Science and Control» RAS (Moscow)
E-mail: tkonzshenkova@ipiran.ru

The article proceeds the thematic cycle dedicated to analytical modeling of linear nonstationary stochastic systems (StS) based on wavelet and wavelet canonical expansions. Section 2 contains elements of spectral and correlation theory. Section 3 is devoted to canonical expansions (CE) of stochastic processes. In Sections 4–6 wavelet algorithms for analytical modeling of mathematical expectation, covariance matrix and matrix of covariance functions are described. Sections 7 and 8 is dedicated to applications of wavelet CE for spectral and correlation analytical express modeling algorithms. Test examples (Appendices 1 and 2) and generalizations are given.

References

1. *Siniczy'n I.N.*, *Sergeev I.V.*, *Korepanov E'.R.*, *Konashenkova T.D.* Instrumental'noe programmnoe obespechenie analiza i sinteza stoxasticheskix sistem vy'sokoj dostupnosti (IV) // Sistemy' vy'sokoj dostupnosti. 2017. T. 13. № 3. S. 55–69.
2. *Siniczy'n I.N.*, *Siniczy'n V.I.*, *Korepanov E'.R.*, *Belousov V.V.*, *Konashenkova T.D.*, *Sergeev I.V.*, *Semendyaev N.N.*, *Basilashvili D.A.* Instrumental'noe programmnoe obespechenie analiza i sinteza sistem vy'sokoj dostupnosti (V) // Sistemy' vy'sokoj dostupnosti. 2018. T. 14. № 1. S. 59–70.
3. *Pugachev V.S.*, *Siniczy'n I.N.* Stochastic Systems Theory and Applications. Singapore: World Scientific. 2001. 908 p.
4. *Siniczy'n I.N.*, *Siniczy'n V.I.* Lekczii po normal'noj i e'llipsoidal'noj approksimaczii v stoxasticheskix sistemax. M.: Torus Press. 2013. 488 s.
5. *Siniczy'n I.N.* Kanonicheskie predstavleniya sluchajny'x funkczij i ix primeneniya v zadachax komp'yuternoj podderzhki nauchny'x issledovanij. M.: Torus Press. 2009.
6. *Siniczy'n I.N.*, *Sergeev I.V.*, *Korepanov E'.R.*, *Konashenkova T.D.* Stoxasticheskie kanonicheskie vejvlet razlozheniya v zadachax modelirovaniya vibroudaronadezhnosti komp'yuternogo oborudovaniya // XVIII Mezhdunar. nauchn. konf. «Sistemy' komp'yuternoj matematiki i ix prilozheniya» (SKMP-2017). Smolensk. 19–21 maya 2017 g. Smolensk: izd-vo SmolGu. S. 123–124.
7. *Siniczy'n I.N.*, *Sergeev I.V.*, *Agafonov E.S.* Primenenie kanonicheskix predstavlenij sluchajny'x funkczij v zadachax rascheta vibrozashhitny'x sistem dlya komp'yuternogo oborudovaniya // Materialy' XI Mezhdunar. nauchn. konf. «Sistemy' komp'yuternoj matematiki i ix prilozheniya», posvyashhennoj 70-letiyu professora V.P. D'yakonova. Smolensk: izd-vo SmolGu. 2010. № 11. S. 239–241.
8. *Siniczy'n I.N., Sergeev I.V.* Metodicheskoe obespechenie izmereniya, kontrolya i ispy'tanij vy'chislitel'nogo oborudovaniya v usloviyax udarny'x vozdejstvij // Trudy' konf. «Texnicheskie i programmny'e sredstva sistem upravleniya, kontrolya i izmereniya» (UKI-2010). M.: IPU RAN. 2010. S. 47–56.
9. *Dobeshi I.* Desyat' lekczij po vejvletam. Moskva–Izhevsk: NICz «Regulyarnaya i xaoticheskaya dinamika». 2004. 464 s.
10. *Xu J. and Shann W.* Galerkin-wavelet methods for two point value problems // Numer. Math. 1992. № 63. P. 123–144.
11. *Gagnon L. and Lina J.M.* Symmetric Daubechies' wavelets and numerical solutions of NLS2 equations // J. Phys. A: Math. Gen. 1994. № 27. P. 8207–8230.
12. *Lepik U.* Numeral solution of evolution equations by the Haar wavelet metods // Appl. Math. Comput. 2007. № 185. P. 695–704.
13. *Lepik U.* Application of the Haar wavelet transform to solving integral and differential equations // Proc. Estonian Acad. Sci. Phys. Math. 2007. № 56. P. 28–46.
14. *Pissaneczki S.* Texnologiya razrezhenny'x matricz. M.: Mir. 1988. 412 s.