ISSN 2078-9181 DOI 10.15622/sp.48

РОССИЙСКАЯ АКАДЕМИЯ НАУК
Отделение нанотехнологий и информационных технологий

САНКТ-ПЕТЕРБУРГСКИЙ
ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РАН

ТРУДЫ СПИИРАН

proceedings.spiiras.nw.ru

ВЫПУСК 5(48)

Санкт-Петербург
2016

18+

Труды СПИИРАН

Выпуск № 5(48), 2016

Научный, научно-образовательный, междисциплинарный журнал с базовой специализацией в области информатики, автоматизации и прикладной математики

Журнал основан в 2002 году

Учредитель и издатель

Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

Адрес редакции

199178, Санкт-Петербург, 14-я линия, д. 39,
e-mail: publ@iias.spb.su, сайт: http://www.proceedings.spiiras.nw.ru/

Подписано к печати 01.10.2016. Формат 60×90 1/16. Усл. печ. л. 14,0. Заказ № 365. Тираж 150 экз., цена свободная
Отпечатано в Редакционно-издательском центре ГУАП, 190000, Санкт-Петербург, Б. Морская, д. 67

Журнал зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций, свидетельство ПИ № ФС77-41695 от 19 августа 2010 г.
Подписной индекс 29393 по каталогу «Почта России»

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук»

SPIIRAS Proceedings

Issue № 5(48), 2016

Scientific, educational, and interdisciplinary journal primarily specialized
in computer science, automation, and applied mathematics

Trudy SPIIRAN ♦ Founded in 2002 ♦ Труды СПИИРАН

Founder and Publisher

Federal State Budget Institution of Science
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences

Editorial Board's address

14-th line VO, 39, SPIIRAS, St. Petersburg, 199178, Russia,
e-mail: publ@iias.spb.su, web: http://www.proceedings.spiiras.nw.ru/

Signed to print 01.10.2016
Printed in Publishing center GUAP, 67, B. Morskaya, St. Petersburg, 190000, Russia

The journal is registered in Russian Federal Agency for Communications and Mass-Media Supervision, certificate ПИ № ФС77-41695 dated August 19, 2010 г.
Subscription Index 29393, Russian Post Catalog

СОДЕРЖАНИЕ

Информационная безопасность

Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В.
КОМБИНИРОВАННАЯ МЕТОДИКА ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ВСТРОЕННЫХ УСТРОЙСТВ НА ПРИМЕРЕ СИСТЕМЫ ОХРАНЫ ПЕРИМЕТРА 5

Новикова Е.С., Котенко И.В.
ВЫЯВЛЕНИЕ АНОМАЛЬНОЙ АКТИВНОСТИ В СЕРВИСАХ МОБИЛЬНЫХ ДЕНЕЖНЫХ ПЕРЕВОДОВ С ПОМОЩЬЮ RADVIZ-ВИЗУАЛИЗАЦИИ 32

Лившиц И.И.
МЕТОДИКА ОПТИМИЗАЦИИ ПРОГРАММЫ АУДИТА ИНТЕГРИРОВАННЫХ СИСТЕМ МЕНЕДЖМЕНТА 52

Воробьев В.И., Евневич Е.Л., Левоневский Д.К., Фаткиева Р.Р., Федорченко Л.Н.
ИССЛЕДОВАНИЕ И ВЫБОР КРИПТОГРАФИЧЕСКИХ СТАНДАРТОВ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДОКУМЕНТОВ 69

Гаврилов И.В.
АЛГОРИТМ ОЦЕНИВАНИЯ СЛОВЕСНОЙ РАЗБОРЧИВОСТИ РЕЧИ НА ОСНОВЕ ФУНКЦИИ КОГЕРЕНТНОСТИ 88

Методы управления и обработки информации

Каныгин Г.В., Полтинникова М.С.
КОНТЕКСТНО-ОРИЕНТИРОВАННЫЕ ОНТОЛОГИЧЕСКИЕ МЕТОДЫ В СОЦИОЛОГИИ 107

Карасев В.В., Соложенцев Е.Д.
ГИБРИДНЫЕ ЛОГИКО-ВЕРОЯТНОСТНЫЕ МОДЕЛИ ДЛЯ УПРАВЛЕНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ 125

Карсаев О.В.
ОБЗОР ТРАДИЦИОННЫХ И ИННОВАЦИОННЫХ СИСТЕМ ПЛАНИРОВАНИЯ МИССИЙ КОСМИЧЕСКИХ АППАРАТОВ 151

Соколов Б.В., Минаков Е.П.
ИССЛЕДОВАНИЯ ХАРАКТЕРИСТИК РАЗМЕЩЕНИЯ И ВАРИАНТОВ ПРИМЕНЕНИЯ МОНОБЛОЧНЫХ СТАЦИОНАРНЫХ НАЗЕМНЫХ СРЕДСТВ ПОРАЖЕНИЯ АСТЕРОИДОВ 182

Алгоритмы и программные средства

Воевода А.А., Романников Д.О.
АСИНХРОННЫЙ АЛГОРИТМ СОРТИРОВКИ МАССИВА ЧИСЕЛ С ИСПОЛЬЗОВАНИЕМ ИНГИБИТОРНЫХ СЕТЕЙ ПЕТРИ 198

Каплин А.Ю., Коротин А.А., Назаров А.В., Якимов В.Л.
АЛГОРИТМ КЛАССИФИКАЦИИ ГРУППОВЫХ ТОЧЕЧНЫХ ОБЪЕКТОВ С НЕУПОРЯДОЧЕННЫМИ ЭЛЕМЕНТАМИ НА ОСНОВЕ ВЕРОЯТНОСТНОЙ МЕРЫ БЛИЗОСТИ 214

CONTENTS

Information Security

Desnitsky V.A., Chechulin A.A., Kotenko I.V., Levshun D.S., Kolomeec M.V.
COMBINED DESIGN TECHNIQUE FOR SECURE EMBEDDED DEVICES EXEMPLIFIED BY A PERIMETER PROTECTION SYSTEM 5

Novikova E.S., Kotenko I.V.
DETECTION OF ANOMALOUS ACTIVITY IN MOBILE MONEY TRANSFER SERVICES USING RADVIZ-VISUALIZATION 32

Livshitz I.I.
A METHOD FOR OPTIMIZING THE INTEGRATED MANAGEMENT SYSTEM AUDIT PROGRAM 52

Vorobiev V.I., Evnevich E.L., Levonevskiy D.K., Fatkieva R.R., Fedorchenko L.N.
A STUDY AND SELECTION OF CRYPTOGRAPHIC STANDARDS ON THE BASIS OF TEXT MINING 69

Gavrilov I.V.
AN ALGORITHM FOR ASSESSING VERBAL SPEECH RECOGNITION BASED ON THE COHERENCE FUNCTION 88

Methods of Information Processing and Management

Kanygin G.V., Poltinnikova M.S.
CONTEXT-ORIENTED ONTOLOGICAL METHODS IN SOCIOLOGY 107

Karasev V.V., Solozhentsev E.D.
HYBRID LOGICAL AND PROBABILISTIC MODELS FOR RISK MANAGEMENT OF SYSTEMS 125

Karsaev O.V.
A REVIEW OF CONVENTIONAL AND INNOVATIVE SATELLITE MISSION PLANNING SYSTEMS 151

Sokolov B.S., Minakov E.P.
INVESTIGATION OF ALLOCATION CHARACTERISTICS AND DEPLOYMENT VARIANTS OF GROUND-BASED MISSILES FOR ASTEROID DESTRUCTION 182

Algorithms and Software

Voevoda A.A., Romannikov D.O.
ASYNCHRONOUS SORTING ALGORITHM FOR ARRAY OF NUMBERS WITH THE USE OF INHIBITORY PETRI NETS 198

Kaplin A.Yu., Korotin A.A., Nazarov A.V., Yakimov V.L.
CLASSIFICATION ALGORITHM OF GROUP POINT OBJECTS WITH UNORDERED ELEMENTS BASED ON CLOSENESS PROBABILITY MEASURE 214

УДК 004.056.53 **DOI** 10.15622/sp.48.1

В.А. Десницкий, А.А. Чечулин, И.В. Котенко, Д.С. Левшун, М.В. Коломеец

КОМБИНИРОВАННАЯ МЕТОДИКА ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ВСТРОЕННЫХ УСТРОЙСТВ НА ПРИМЕРЕ СИСТЕМЫ ОХРАНЫ ПЕРИМЕТРА

Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.М., Коломеец М.В. **Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра.**

Аннотация. С точки зрения информационной безопасности встроенные устройства представляют собой элементы сложных киберфизических систем, работающих в потенциально враждебном окружении. Поэтому разработка таких устройств является сложной задачей, часто требующей экспертных решений. Сложность задачи разработки защищенных встроенных устройств обуславливается различными типами угроз и атак, которым может быть подвержено устройство, а также тем, что на практике вопросы безопасности встроенных устройств обычно рассматриваются на финальной стадии процесса разработки в виде добавления дополнительных функций защиты. В статье предлагается методика проектирования, применение которой будет способствовать разработке безопасных и энергоэффективных киберфизических и встроенных устройств. Данная методика организует поиск наилучших комбинаций компонентов защиты на основе решения оптимизационной задачи. Работоспособность предлагаемой методики демонстрируется на основе разработки прототипа защищенной системы охраны периметра помещения.

Ключевые слова: встроенные устройства, киберфизические системы, охрана периметра, проектирование защищенных киберфизических систем.

1. Введение. В настоящее время встроенные устройства получают все большее распространение в самых разных областях приложения — в системах управления и контроля на транспорте, в системах управления производственным процессом, системах, предоставляющих телекоммуникационные сервисы потребителям, в системах имплантируемых медицинских устройств для контроля жизненно важных показаний организма человека, в электроэнергетике, в системах обеспечения физической безопасности помещений, прикладных системах распознавания речи и др. Критически важный характер таких систем, а также высокая степень взаимодействия встроенного устройства с другими элементами программно-аппаратного окружения и пользователями системы обуславливает важность разработки механизмов защиты таких устройств от угроз информационной безопасности.

Под встроенным устройством понимается электронное устройство, функциональность которого определяется прежде всего его аппаратной и программной частями. Аппаратная составляющая определяет его вычислительные и коммуникационные возможности, интерфейсы взаимодействия с источниками данных (сенсорами) и различными сило-

выми приводами, производительность, энергоэффективность, автономность, мобильность и другие возможные характеристики устройств. Программная же часть реализует бизнес-логику устройства с использованием драйверов и библиотек для связи с периферийными аппаратными модулями, базами данных, веб-сервисами и др. Ключевым признаком встроенного устройства является его узкоспециализированное назначение, причем, как правило, такие устройства имеют следующие особенности: 1) жесткие ограничения на аппаратные возможности устройств и энергоресурсы, обуславливаемые, в частности, использованием одноплатных компьютеров; 2) изменчивость киберфизического окружения встроенных устройств, и как следствие, их подверженность специфичным наборам атак; 3) компонентно-ориентированная структура с возможными скрытыми конфликтами между отдельными компонентами или их побочным влиянием друг на друга.

Приведенные выше особенности встроенных устройств обуславливают потребность в разработке специализированных подходов и методов проектирования, которые позволили бы повысить защищенность конечных продуктов и сервисов [1].

Данная работа сфокусирована на решении вопросов проектирования безопасных систем в части комбинирования отдельных компонентов встроенных устройств в единый, согласованно работающий программно-аппаратный комплекс. Такое комбинирование осуществляется на основе установленных требований к защите с учетом ограничений устройств и связей между компонентами. Данная статья является логическим продолжением работ, опубликованных ранее по проектированию и верификации систем со встроенными устройствами. В [2, 3] были предложены общие рекомендации по комбинированию компонентов защиты систем со встроенными устройствами с учетом показателей их ресурсопотребления (конфигурированию) с привлечением оптимизационного подхода для комбинаторного перебора имеющихся альтернатив компонентов защиты и эвристического подхода для определения порядка учета показателей ресурсопотребления.

В рамках данной статьи предложена методика проектирования защищенных встроенных устройств на основе комбинирования компонентов защиты в виде структурированной последовательности действий, которые разработчик должен выполнить для формирования эффективной реализации защищенного устройства. Помимо этого, вкладом данной статьи является также подтверждение выполнимости предложенной методики путем ее практического применения при проектировании защищенной системы охраны периметра помещения (в части реализации функций контроля доступа) с использованием одно-

платных компьютеров. При этом практический результат применения методики — набор выбранных программных и программно-аппаратных компонентов из списков имеющихся альтернатив, применение которых позволило построить защищенную систему с учетом улучшения ее целевых показателей, в том числе цены и некоторых показателей ресурсопотребления.

Новизна данной статьи заключается в (1) разработке методики проектирования защищенных встроенных устройств путем комбинирования компонентов защиты с использованием правил их выбора с учетом семантики защитного функционала и имеющихся нефункциональных ограничений, а также (2) подтверждение корректности этой методики путем ее практического применения для создания системы контроля доступа в помещение с использованием программируемых микроконтроллеров.

Данная статья имеет следующую структуру. В разделе 2 приведен обзор работ в предметной области. В разделе 3 представлено описание предлагаемой методики проектирования защищенных встроенных устройств на основе комбинирования компонентов защиты. Разделы 4-6 сфокусированы на проверке корректности предложенной методики: в разделе 4 сформулированы требования к разрабатываемой системе охраны периметра; раздел 5 содержит описание процесса выбора программно-аппаратных средств, при помощи которых может быть реализована система, соответствующая требованиям, определенным в разделе 4; в разделе 6 приведено описание разработанной системы. Раздел 7 включает анализ полученных результатов. Завершает статью заключение, содержащее основные выводы.

2. Работы в предметной области. В соответствии с [4], встроенные устройства определяются как программно-аппаратные устройства, вычислительный процесс которых тесно связан с реакцией на процессы физического окружения и выполняется в рамках некоторой физической платформы, которая, помимо непосредственно вычислительных модулей, включает также модули, взаимодействующие с киберфизическими объектами окружения. К таким объектам относятся разнообразные сенсоры, силовые приводы, сканеры текстовых, звуковых и других данных, устройства отображения информации, разнообразные коммуникационные и навигационные устройства, бытовые и промышленные устройства нагревания, вентиляции, насосные станции, устройства мониторинга и диагностики и др.

Как следствие, связи между программной частью устройства, с одной стороны, и аппаратно-техническим окружением — с другой,

обуславливают наличие дополнительных ограничений, влияющих существенным образом на процесс проектирования таких устройств.

В настоящее время широкое применение на практике получил компонентный подход к проектированию встроенных устройств [5], реализованный в рамках платформ Arduino, Raspberry Pi, Beagle board и операционной системы Android. Фактически, в силу специфики встроенных устройств, завязанных в своей работе непосредственно на обеспечение установленных требований защиты, встроенное устройство представляется в виде множества взаимодействующих программных и программно-аппаратных компонентов. Далее в статье компоненты встроенных устройств, выбор которых во многом определяет выполнимость требований защиты, будем обобщенно называть — компоненты защиты.

На практике при разработке встроенных устройств зачастую выбор тех или иных компонентов защиты осуществляется экспертно, в силу заранее предопределенных субъективных предпочтений разработчиков и уже известных им решений. При этом в процессе комбинирования таких компонентов в единый механизм недостаточное внимание уделяется индивидуальным особенностям компонентов защиты, возможным неявным связям и скрытым конфликтам между компонентами в силу отсутствия их априорной согласованности между собой и ограничениям программно-аппаратной платформы.

Для встроенных устройств, которым присущи как вычисления, так и физические ограничения в [6] также обосновывается важность достижения компромиссов между защищенностью и нефункциональными характеристиками встроенных устройств, в том числе с применением оптимизационных подходов и комбинирования встроенных устройств из отдельных компонент в соответствии с их свойствами и требованиями. При этом учитываются вопросы их корректного взаимодействия в виде последовательного и параллельного функционирования компонентов, что характерно для программных и аппаратных систем, образующих конкретное встроенное устройство.

В [7] обосновывается необходимость и важность исследования вопросов разработки защищенных встроенных устройств на основе использования высокоуровневых средств защиты с приемлемыми энергетическими и вычислительными расходами. Помимо вопросов предоставления устройству и его сервисам необходимых аппаратных и энергоресурсов, особый интерес представляют атаки, направленные на истощение энергоресурсов устройства [8]. При этом подобные атакующие воздействия не обнаружимы посредством традиционно применяемых решений, но обуславливают неконтролируемый расход ресур-

сов со стороны наиболее энергозатратных аппаратных модулей устройства, таких как интерфейсные модули Wi-Fi, Bluetooth и дисплей, и тем самым делая невозможным на некоторое время дальнейшее функционирование устройства. Поэтому комплексная система защиты встроенного устройства должна включать программные и программно-аппаратные модули, направленные против релевантных угроз безопасности с учетом возможных неявных связей между модулями, несогласованностей между ними и побочными эффектами.

В качестве пути достижения компромисса между защищенностью устройства и его ресурсопотреблением в [9] предлагается использование «реконфигурируемых примитивов безопасности» на основе динамической адаптации архитектуры устройства в зависимости от состояния устройства и его окружения. Предлагаемая адаптация основывается, во-первых, на возможности динамического переключения между несколькими механизмами, встроенными в устройство, и во-вторых, на возможности обновления элементов этих механизмов.

В специальной литературе существует достаточно много примеров решения задачи построения системы охраны периметра на основе использования встроенных устройств, объединяемых в единую сеть для обеспечения возможности централизованного управления. Так, например, в работе [10] представлена архитектура, анализ и результаты тестирования распределенной системы контроля доступа. В работе [11] представлена информация о возможных потребителях и отличительных особенностях распределенных систем контроля периметра. Однако в этих работах архитектура разработанных решений основана на экспертном методе.

Методика, представленная в настоящей работе, позволяет выбирать основные решения для построения подобной системы без обязательного вовлечения эксперта в области компонентов защиты встроенных устройств с возможностью автоматизации ее отдельных стадий в части перебора и сравнения большого количества функциональных требований защиты и альтернатив компонентов защиты.

3. Методика проектирования защищенных встроенных устройств. В данном разделе представлена предлагаемая методика проектирования защищенных встроенных устройств на основе комбинирования компонентов защиты. Отличительной особенностью методики является учет функциональных и нефункциональных характеристик компонентов защиты, ограничений устройства и связей между компонентами с использованием оптимизационного подхода.

Под конфигурацией защиты понимается набор компонентов защиты с определенными функциональными и нефункциональными ха-

рактеристиками. Цель методики — определить наиболее эффективную с точки зрения заданных нефункциональных показателей (оптимальную) конфигурацию защиты на основе входных данных об особенностях устройства и возможных компонентах защиты (таблица 1).

Таблица 1. Представление методики проектирования защищенных встроенных устройств

№	Стадии методики
1	Определение функциональных требований к защите
2	Определение нефункциональных ограничений, существенных для проектируемого данного устройства
3	Выявление множества альтернатив компонентов защиты, которые его реализуют, для каждого функционального требования защиты
4	Определение правил выбора компонентов защиты, исходя из связей между ними
5	Вычисление значений нефункциональных показателей для заданных компонентов
6	Упорядочивание альтернатив компонентов по степени ухудшения значений установленных нефункциональных ограничений
7	Определение порядка учета рассматриваемых нефункциональных показателей
8	Исследование альтернатив компонентов защиты и вычисление суммарных значений нефункциональных показателей наборов компонентов защиты, а также выбор оптимальной конфигурации

Фактически, в рамках методики решается задача дискретной оптимизации на множестве конфигураций с целевой функцией, выражаемой при помощи нефункциональных показателей и ограничений на заданные как функциональные, так и нефункциональные показатели [3]. В качестве целевой функции решаемой оптимизационной задачи рассматривается упорядоченный набор из нескольких нефункциональных показателей, каждый из которых подвергается либо минимизации, либо максимизации, в зависимости от семантики нефункциональной характеристики, лежащей в основе рассматриваемого нефункционального показателя *(p1→min/max, p2→min/max, p3→min/max,…)*. Порядок показателей определяется на основе эвристического подхода.

Первая стадия включает определение функциональных требований защиты, которые нужно реализовать в процессе разработки комбинированного механизма защиты. Данные требования основываются на анализе спецификации целевого устройства с использованием методов аналитического моделирования действий нарушителя [12–14]. В качестве примера можно привести следующее функциональное требование защиты: «секретность бизнес-данных устройства должна осу-

ществляться с использованием симметричного шифрования с ключами не менее 128 бит».

Стадия 2 включает действия по определению нефункциональных ограничений, существенных для проектируемого данного устройства. Источником возможных нефункциональных ограничений является методология MARTE [5], где релевантные нефункциональные показатели, характерные для встроенных устройств, специфицированы с использованием UML. В частности, в рамках методики используются нефункциональные ограничения, построенные на основе следующих классов доменов знаний: HW_Physical, HW_PowerSupply, HW_StorageManager, HW_Computing, HW_Communication [5].

На стадии 3 для каждого функционального требования защиты осуществляется определение множества альтернатив компонентов защиты, которые его реализуют. Например, для требования секретности бизнес-данных определяется набор криптографических алгоритмов симметричного блочного шифрования заданной стойкостью с установленной длиной ключа, таких как AES/128/192/256, IDEA и др.

На стадии 4 осуществляется определение правил выбора компонентов защиты, исходя из связей между ними и учитывая семантику компонентов защиты, установленных требований защиты и сценариев использования. Каждое такое правило представляется в виде формальной четверки, имеющей следующие элементы *(req, Alts, reason, justif)*, где *req* — формулировка функционального требования защиты; *Alts* — набор альтернатив компонентов, каждый из которых реализует данное требование; *reason* — причинно-следственная связь в определении предпочтительности компонентов из *Alts,* в зависимости от рассматриваемых для данного требования нефункциональных показателей (т.е. формулировка критерия выбора); и *justif* — фактическое обоснование предлагаемого порядка предпочтительности компонентов из *Alts* для данного функционального требования защиты.

На стадии 5 производится определение значений нефункциональных ограничений для заданных компонентов защиты следующими способами: путем сбора данных от конкретных производителей используемых программно-аппаратных модулей; эмпирически — на основе программного моделирования компонентов защиты (когда это возможно); экспертно — с учетом предыдущего опыта работы с такими или сходными компонентами. Так, например, для каждого из имеющихся альтернативных алгоритмов удаленной аттестации критических бизнес-данных встроенного устройства определяется величина необходимой оперативной памяти (КБ), которое устройство должно предоставить, и объем коммуникационного ресурса, расходуемого на

передачу аттестующих подписей доверенному серверу в единицу времени (Мбит/сек).

Стадия 6 включает упорядочивание альтернатив компонентов защиты по степени ухудшения значений их нефункциональных ограничений. Фактически, для каждого нефункционального показателя осуществляется сортировка компонентов защиты. Например, для учета энергопотребления имеющихся разновидностей некоторого программно-аппаратного компонента защиты возможные альтернативы упорядочиваются в соответствии с уменьшением величины потребляемого ими тока (измеряемого в миллиамперах).

На стадии 7 определяется порядок учета рассматриваемых нефункциональных ограничений в зависимости от относительной важности каждого из них с использованием эвристики, предложенной в [3]. Данная эвристика задает общий алгоритм приоритезации нефункциональных ограничений встроенного устройства. По существу, для каждого нефункционального ограничения выделяется набор специфичных функциональных и нефункциональных признаков встроенного устройства, таких как «наличие постоянного источника питания», «возможность замены устройства или аккумулятора без ущерба для предоставляемых им сервисов», «степень зависимости достижения бизнес-целей устройства от энергоресурсов» и др. Для каждого такого признака предопределено значение ранга (например, с заданием значений от 1 до 3, где 1 — низкая важность, 3 — высокая важность) в зависимости от критичности данного признака для выполнимости заданного нефункционального ограничения (например, ограничения на ресурс энергопотребления). В результате спецификация целевого встроенного устройства анализируется на предмет наличия у него обозначенных признаков. Для каждого нефункционального ограничения выбирается максимальное значение ранга по всем выявленным у разрабатываемого устройства признакам, в соответствии с которыми происходит упорядочивание уже собственно нефункциональных ограничений. При этом ограничения, получившие одинаковые результирующие значения ранга, упорядочиваются между собой согласно порядку, предопределенному экспертно [3].

На стадии 8 осуществляются комбинаторный перебор альтернатив компонентов защиты и вычисление суммарных значений нефункциональных показателей наборов компонентов защиты (конфигураций). Стадия включает также выбор оптимальной конфигурации на основе полученных значений. В частности, в случае большого числа рассматриваемых функциональных требований защиты и имеющихся альтернатив компонентов защиты на данной стадии целесообразно

применять разработанное программное средство Конфигуратор, позволяющее автоматизировать процесс перебора и вычисления.

В случае если в рамках установленных ограничений решений оптимизационной задачи не существует, на стадии 8 предлагается ряд конфигураций, которые смогут быть реализованными при ослаблении определенных ограничений (в частности, увеличения объемов аппаратных ресурсов устройства, выделяемых на работу компонент).

Отметим, что в общем случае выбор компонентов — итеративный процесс. При каком-либо изменении спецификации системы или особенностей ее реализации итоговый набор компонентов может изменяться вследствие изменений условий, которые учитывались в процессе выбора компонентов.

4. Требования к разрабатываемому прототипу системы охраны периметра. Для демонстрации работоспособности предложенной методики проектирования и разработанных программных средств была выбрана задача построения прототипа системы охраны периметра. Данная система должна осуществлять управление физическим доступом в определенном здании (кого пускать, в какое время пускать и в какое помещение пускать), включая ограничение доступа в заданное помещение и идентификацию лица, имеющего доступ в заданное помещение. Кроме того, система должна контролировать информационный доступ (разрешать или запрещать доступ к информации, расположенной на персональных компьютерах). Каждый пользователь, контролируемый системой, может находиться в четырех состояниях: S_1 — пользователь вошел в помещение; S_2 — пользователь авторизовался на рабочем месте (начало сеанса работы с операционной системой); S_3 — пользователь завершил сеанс работы с операционной системой; S_4 — пользователь покинул помещение.

Вход пользователя в помещение или выход пользователя из помещения идентифицируется приложением бесконтактной карты к считывателю, который подсоединен к подсистеме контроля доступа в помещении. В ситуациях, когда пользователь не приложил карту, открытие двери идентифицируется переходом кнопки из нажатого состояния в свободное и/или инфракрасным датчиком движения. Как только установлено, что человек вошел в помещение (или вышел из него), запускается обратный отсчет — время, за которое пользователю необходимо авторизоваться в системе при помощи карты. На основе уникальных данных карты формируется специальный запрос к центральному серверу управления доступом для получения информации о наличии или отсутствии доступа к помещению у пользователя карты. Подсистема контроля доступа в помещение, получив ответ от цен-

трального сервера управления доступом, начинает обработку полученной информации. Результат проверки карты пользователя сопровождается открытием замка, выводом текстовой информации на экран, световым и звуковым сигналом. Результаты проверки карт вместе с информацией о состоянии сеансов работы пользователей с операционной системой направляются на сервер журналирования.

Таким образом, для реализации защищенной системы охраны периметра в целом необходимо реализовать надежную и защищенную подсистему контроля доступа в помещение. Данная подсистема представляет собой встроенное устройство (ВУ), расположенное в дверях между помещениями и подключенное к механизму управления замком.

Рассмотрим основные функциональные требования к данному устройству более подробно.

ВУ должно осуществлять работу в локальной сети системы по беспроводному каналу передачи данных. Это необходимо для защиты от физического воздействия на канал передачи данных между микроконтроллером и центральным сервером управления (например, повреждение Ethernet-кабеля), а также для существенного снижения стоимости установки системы.

ВУ должно поддерживать интерфейс для взаимодействия с удаленным сервером приложений для удобства интеграции в общую систему контроля и управления доступом. Взаимодействие с сервером приложений может осуществляется по HTTP, HTTPS, SOAP. Данные, передаваемые по HTTP и SOAP, должны быть предварительно зашифрованы.

Для взаимодействия с центральным сервером управления доступом ВУ должно поддерживать запуск приложений, разработанных на одном из высокоуровневых языков программирования.

Разрабатываемое ВУ должно поддерживать аварийный режим работы, в случае, если обмен данными между ВУ и центральным сервером управления доступом перестает быть возможным (отсутствие соединения с сервером, отказ в обслуживании на стороне сервера и т.п.). В аварийном режиме работы решение о предоставлении пользователю доступа в помещение принимается на основе локальной базы данных, расположенной на ВУ. Локальная база данных представляет собой резервную копию сетевой базы данных доступа и содержит информацию об администраторах системы. Таким образом, при аварийном режиме работы, доступ в помещение может получить только сотрудник с правами администратора. При этом разрабатываемое ВУ должно обладать объемом памяти, достаточным для хранения и поддержки локальной базы данных.

ВУ должно предоставлять веб-интерфейс для управления ВУ при локальном Ethernet подключении. Данный веб-интерфейс должен содержать внутренний журнал ВУ и обеспечить инициализацию ре-

зервного копирования сетевой базы данных доступа. Таким образом, функциональные требования могут быть сведены в общее представление (таблица 2).

Таблица 2. Функциональные требования к разрабатываемому ВУ

Функциональные требования	№	Описание
К аппаратному обеспечению	1	Обеспечение взаимодействия с внешними электронными компонентами: механическими замками, сканерами бесконтактных RFID-карт, инфракрасными датчиками движения, устройствами вывода текстовой и звуковой информации, звуковых и световых сигналов.
	2	Обеспечение беспроводного канала передачи данных.
	3	Обеспечение передачи данных через Ethernet.
К программному обеспечению	4	Обеспечение обмена данными по HTTP, HTTPS, SOAP.
	5	Обеспечение запуска приложений, написанных на JAVA, Python, C++.
	6	Обеспечение хранения локальной резервной копии базы данных.
	7	Обеспечение шифрования данных, передаваемых по каналам передачи данных.
	8	Обеспечение управления ВУ через веб-интерфейс при локальном Ethernet подключении.

В случае выхода из строя электрической цепи, к которой подсоединено ВУ, обеспечение энергией выполняет источник резервного питания. В подобной ситуации функционирование ВУ не нарушается, но максимально возможное время работы ВУ зависит от ёмкости источника и количества потребляемой им энергии. Стоимость ВУ рассчитывается комплексно, учитывается микроконтроллер со всем множеством компонент. Таким образом, предпочтение следует отдавать ВУ, которое удовлетворяет всем функциональным требованиям и при этом оптимально по соотношению итоговая стоимость / энергоэффективность.

Предполагается, что устройство будет располагаться в непосредственной близости от входа в помещение. ВУ должно обладать соответствующими размерами, позволяющими разместить его на малой площади. Наименьшей поверхностью в данной ситуации обладает дверь. Таким образом, при встраивании в дверь ВУ должно быть не толще трех сантиметров, при условии, что наиболее распространенная толщина двери четыре сантиметра. Отметим, что толщиной менее трех сантиметров обладает большая часть популярных микроконтроллеров.

Таким образом, нефункциональные требования могут быть сведены в единую таблицу (таблица 3).

Таблица 3. Нефункциональные требования к разрабатываемому ВУ

Нефункциональные требования	Описание
К энергоэффективности	Обеспечение функционирования ВУ в условиях выхода из строя электрической цепи, к которой подсоединено ВУ, за счет энергии резервного источника питания.
К стоимости	Минимизация стоимости микроконтроллера, расширений микроконтроллера, сенсоров и периферии, необходимых для соответствия функциональным требованиям.
К занимаемому пространству	Минимизация размеров микроконтроллера, расширений микроконтроллера, сенсоров и периферии, таким образом, чтобы толщина ВУ не превышала толщины двери.

5. Применение методики для выбора компонентов прототипа системы охраны периметра. В соответствии с функциональными требованиями (таблица 2), каждая из рассматриваемых альтернатив должна поддерживать взаимодействие с внешними электронными компонентами: механическими замками, сканерами бесконтактных карт технологии RFID, инфракрасными датчиками движения, устройствами вывода текстовой, звуковой информации, звуковых и световых сигналов. Набор внешних электронных компонент с их показателями по цене и потреблению электроэнергии сведен в единую таблицу (таблица 4).

Таблица 4. Набор внешних электронных компонентов

Внешний электронный компонент	Выбранное физическое устройство	Потребление (мАм/час)	Стоимость (руб.)
Механический замок	TowerPro SG90	550 [15] (в момент открытия двери)	792
Сканер бесконтактных карт технологии RFID	Grove 125KHz RFID Reader	50 [16]	1296
Инфракрасный датчик движения	**PIR Motion Sensor HC-SR501**	0,05 [17]	216
Устройство вывода текстовой информации	DC 5V Character LCD 16x2	100 [18] (при поднесении бесконтактной карты к сканеру)	1080
Устройство вывода звуковых сигналов	DC 12mA 5V 12mm Piezo Alarm Buzzer	12 [17] (в момент подачи сигнала)	216
Устройство вывода световых сигналов	RGB Light-emitting Diode	20 [19]	7.2
Итого		70,05 – 732,05 (среднее – 200)	2880

Примем, что набор внешних электронных компонент будет единым, поэтому в методике проектирования (раздел 2) не будет осуществляться поиск альтернатив для каждого из внешних электронных компонентов. Влияние набора (таблица 4) внешних электронных компонентов на нефункциональные требования (таблица 3) будет учтено при принятии оптимального с точки зрения нефункциональных требований решения. С учетом функциональных требований, на выходе методики были сформированы альтернативы, представленные в таблице 5.

Таблица 5. Альтернативы, выбранные при помощи методики проектирования безопасных ВУ

№	Набор компонентов защиты (альтернатива)	Описание
1	Arduino Yun, microSD 512 MB	Внутренняя память Arduino Yun ограничена 8 MB, чего недостаточно для соответствия функциональным требованиям к программному обеспечению. Внутреннюю память Arduino Yun можно расширить с помощью microSD.
2	Raspberry Pi B+, Wi-Pi модуль	Raspberry Pi B+ не поддерживает передачу данных по беспроводному каналу передачи данных, а потому не соответствует одному из функциональных требований к аппаратному обеспечению. Wi-Pi модуль разработан специально для Raspberry Pi, чтобы нивелировать данный недостаток.
3	Beaglebone Black, Compact USB Wi-Fi Adapter	Beaglebone Black не поддерживает передачу данных по беспроводному каналу передачи данных, а потому не соответствует одному из функциональных требований к аппаратному обеспечению. Compact USB Wi-Fi Adapter разработан специально для Beaglebone Black, чтобы нивелировать данный недостаток.
4	Intel Galileo Gen 2P Board, Intel Galileo Wi-Fi Kit	Intel Galileo Gen 2P Board не поддерживает передачу данных по беспроводному каналу передачи данных, а потому не соответствует одному из функциональных требований к аппаратному обеспечению. Intel Galileo Wi-Fi Kit разработан специально для Intel Galileo Gen 2P Board, чтобы нивелировать данный недостаток.

В процессе выполнения методики проектирования в выходной набор альтернатив не прошли: микроконтроллер Arduino Mega из-за отсутствия поддержки запуска приложений, написанных на JAVA, Python, C++; Raspberry Pi A+ из-за отсутствия поддержки передачи

данных через Ethernet. Кроме того, Raspberry Pi 2 не был включен в перечень микроконтроллеров, подаваемых на вход методике, так как Raspberry Pi 2 является более дорогим аналогом Raspberry Pi B+, а потому хуже по нефункциональным требованиям.

При анализе энергоэффективности отдельных компонентов и устройств использовались как источники из сети Интернет, так и эксперименты с реальным оборудованием.

Потребление электроэнергии альтернативы 1 включает энергопотребление Arduino Yun и набора внешних электронных компонент. Энергопотребление микроконтроллера Arduino Yun, в свою очередь, зависит от степени нагрузки процессора и может варьироваться между 200 и 300 мАч [21]. Таким образом, потребление электроэнергии альтернативы 1 составляет 400-500 мАч.

Потребление электроэнергии альтернативы 2 включает энергопотребление Raspberry Pi B+, Wi-Pi модуля и набора внешних электронных компонент. Минимальное энергопотребление Raspberry Pi B+ без подключенных внешних устройств составляет 600 мАч [21]. Потребление Wi-Pi модуля составляет 450 мАч [22]. Таким образом, потребление электроэнергии альтернативы 2 составляет 1250 мАч.

Потребление электроэнергии альтернативы 3 включает энергопотребление Beaglebone Black, Compact USB Wi-Fi Adapter и набора внешних электронных компонент. Энергопотребление Beaglebone Black составляет 210-460 мАч [23]. Потребление Compact USB Wi-Fi Adapter составляет 120 мАч (получено экспериментально). Таким образом, потребление электроэнергии альтернативы 3 составляет 780 мАч.

Потребление электроэнергии альтернативы 4 включает энергопотребление Intel Galileo Gen 2P Board, Intel Galileo Wi-Fi Kit и набора внешних электронных компонент. Минимальное энергопотребление Intel Galileo Gen 2P Board без подключенных внешних устройств составляет 800 мАч [24]. Потребление Intel Galileo Wi-Fi Kit составляет около 400мАч [17]. Следовательно, потребление электроэнергии альтернативы 4 составляет 1400 мАч.

Стоимости микроконтроллеров и специфичных для них элементов сформированы исходя из официальных предложений разработчиков и их дистрибьюторов. Более дешевые аналоги (реплики) не рассматривались, так как невозможно гарантировать их совместимость с общим набором внешних компонент. Стоимость неспецифичных компонент сформирована исходя из предложений электронного магазина Amazon [20]. Стоимость внешних компонентов, включая механический замок, сканер бесконтактных карт на технологии RFID, инфра-

красный датчик движения, устройства вывода текстовой информации, звуковых и световых сигналов, составляет 2880 руб. (таблица 6).

Рассмотрим особенности предлагаемых альтернатив, которые также влияют на общую цену:

– В стоимость альтернативы 1 входят: Arduino Yun — 3744 руб. [14], Micro SD карта — 144 руб. [17]. Итоговая стоимость с учтом внешних электронных компонент — 6768 руб.

– В стоимость альтернативы 2 входят: Raspberry Pi B+ — 656 руб. [25], Wi-Pi модуль — 792 руб. [17]. Итоговая стоимость с учетом внешних электронных компонент — 5328 руб.

– В стоимость альтернативы 3 входят: Beaglebone Black — 3600 руб. [26], Compact USB Wi-Fi Adapter — 792 руб. [17]. Итоговая стоимость с учетом внешних электронных компонент — 7272 руб.

– В стоимость альтернативы 4 входят: Intel Galileo Gen 2P Board — 4464 руб. [27], Intel Galileo Wi-Fi Kit — 3240 руб. [17]. Итоговая стоимость с учетом внешних электронных компонент — 10584 руб.

Таблица 6. Сравнение альтернатив по нефункциональным требованиям

Набор компонентов защиты	Потребление энергии (мАч)	Стоимость (₽)	Размер (мм)
Arduino Yun, microSD 512 MB	500	6768	73*53*8
Raspberry Pi B+, Wi-Pi модуль	1250	5328	60*36*7
Beaglebone Black, Compact USB Wi-Fi Adapter	780	7272	86*53*7
Intel Galileo Gen 2P Board, Intel Galileo Wi-Fi Kit	1400	10584	123*72*9

Размеры ВУ напрямую зависят от размера их самой большой части микроконтроллеров. Толщина всех микроконтроллеров соответствует ограничению в 3 сантиметра (при непосредственном размещении в двери). Исходя из нефункциональных требований, были получены результаты, представленные в таблице 6.

Альтернатива 1 показывает лучшую энергоэффективность при средней стоимости. Альтернатива 2 имеет малую энергоэффективность, однако ее стоимость значительно ниже приведенных аналогов, что дает основания для рассмотрения и этого варианта. Альтернатива 3 имеет энергоэффективность и стоимость, близкую к альтернативе 1, но все же несколько уступает ей. Таким образом, альтернативу 3 можно

далее не рассматривать. Альтернатива 4 является наиболее дорогим и наименее энергоэффективным решением в сравнении с остальными наборами компонентов защиты. Дальнейшее рассмотрение альтернативы 4 нецелесообразно.

Требование энергоэффективности подразумевает, что ВУ способно поддерживать функционирование в условиях выхода из строя электрической цепи, к которой подсоединено ВУ, за счет энергии резервного источника питания. Время работы от резервного источника питания для различных альтернатив зависит и от емкости источника резервного питания. Для работы альтернатив 1 и 2 на протяжении 24 часов необходимы аккумуляторы со следующими емкостями: альтернатива 1 — 12000 mAh, альтернатива 2 — 30000 mAh. Необходимая емкость была рассчитана на основе полученных ранее значений среднего энергопотребления.

В качестве источников резервного питания рассматриваются power bank, так как их размер соответствует нефункциональным требованиям. Стоимость power bank зависит от ёмкости и количества поддерживаемых циклов перезарядки и равна 1280 руб. и 2560 руб. для ёмкостей в 12000 mAh и 30000 mAh. Таким образом, итоговая стоимость эксплуатации альтернативы 2 составляет 7888 руб., если учитывать стоимость источника резервного питания. Это значительно выше, чем итоговая стоимость альтернативы 1, которая составляет 8048 руб.

С учетом вышесказанного, оптимальным набором компонентов защиты является альтернатива 1. Итоговый набор компонент защиты: Arduino Yun, microSD 512 MB, TowerPro SG90, Grove 125KHz RFID Reader, PIR Motion Sensor HC-SR501, DC 5V Character LCD 16x2, DC 12mA 5V 12mm Piezo Alarm Buzzer, RGB Light-emitting Diode, power bank 12000 mAh; стоимостью 6768 руб. и энергопотреблением 500mAh.

6. Описание прототипа спроектированной системы охраны периметра. Архитектура системы представлена на рисунке 1:

(1) микроконтроллер Arduino Yun состоит из двух частей:

– процессор ATmega 32U4 (выполняет требования 2, 3 из табл. II), управляющий через sketch [28] сервоприводом, сканнером бесконтактных карт технологии RFID, текстовым экраном, инфракрасным датчиком движения, компонентами вывода световых и звуковых сигналов;

– процессор AR9331 под управлением Linux (выполняет требования 5, 6 из табл. II), содержащий Arduino_Client (выполняет требования 4, 7 из табл. II), который выполняет роль посредника между ATmega 32U4 и Access_App_Server, а также журналирует вход и выход пользователей из помещения;

(2) Access_App_Server предоставляет удаленный доступ к Access_DB_Server для Arduino_Client и для Admin_Client, а также журналирует действия Admin_Client;

(3) база данных Access_DB_Server содержит информацию о пользователях системы, бесконтактных картах, ролях пользователей, устройствах и правах доступа к помещениям для каждой из ролей;

(4) Admin_Client осуществляет управление информацией, хранящейся в базе данных Access_DB_Server, а также журналирование действий администратора;

(5) User_Client журналирует начало и завершение сеанса пользователя с операционной системой;

(6) Syslog_App_Server предоставляет удаленный доступ к Syslog_DB_Server, а также осуществляет генерацию инцидентов безопасности на основе корреляции журналов;

(7) база данных Syslog_DB_Server содержит информацию о событиях и инцидентах безопасности, происходящих в системе.

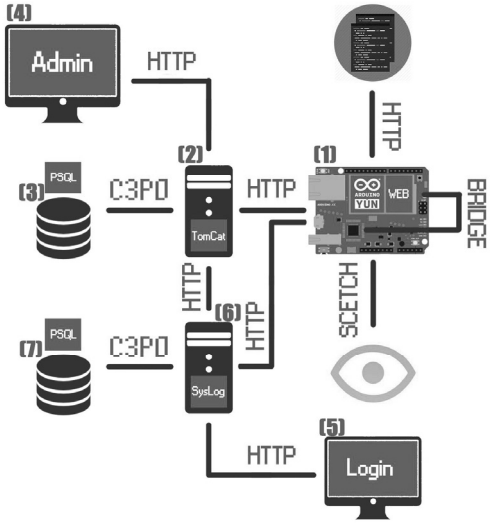


Рис. 1. Архитектура системы

В процессор ATmega 32U4 (1) загружается код, который называется sketch [28]. Любой sketch можно условно разделить на три части: блок инициализации, блок прошивки, блок исполнения. В блоке инициализации подключаются необходимые для работы sketch-библиотеки, объявляются глобальные переменные, задаются специальные обозначения для цифровых или аналоговых PIN. В блоке про-

шивки (setup(){}) осуществляется настройка Arduino, ее подготовка для выполнения функционала, необходимого в блоке исполнения. Блок исполнения (loop(){}) циклически выполняет записанный в нем код, представляя собой алгоритмическое ядро sketch.

Взаимосвязь между ATmega 32U4 и AR9331 Linux-процессорами Arduino Yun осуществляется при помощи библиотек Bridge.h и FileIO.h [28]. Библиотека Bridge.h позволяет запускать shell-команды прямо из sketch, а FileIO.h дает возможность считывать и записывать файлы, принадлежащие файловой системе Linux.

Запуск Arduino_Client осуществляется из sketch благодаря библиотеке Bridge.h посредством выполнения асинхронной (без ожидания завершения) shell-команды. Дальнейшее взаимодействие между sketch и Arduino_Client строится на обработке (чтение/запись) специальных текстовых (.txt) файлов. Это происходит относительно быстро благодаря использованию библиотеки FileIO.h. Запись осуществляется в специальном формате, напоминающем HTTP.

Arduino_Client представлен jar-приложением [29]. Работу jar-приложения клиента можно разделить на два этапа: инициализация и функционирование. При инициализации происходит проверка доступности сервера (2), настройка параметров взаимодействия между AR9331 и ATmega, а также репликация данных администраторов из Access_DB_Server в локальную базу данных и из нее в кэш. Локальная база данных хранит реплицированные данные администраторов. Она необходима на случай, если Access_App_Server станет недоступен. На этапе функционирования предусмотрено разбиение главного потока на прикладные. Каждый поток обрабатывает запросы, приходящие от Arduino, с некоторой периодичностью. В данный момент реализовано четыре потока: первый обрабатывает запросы на получение доступа в помещение, второй проверяет соединение с сервером, третий обеспечивает журналирование, четвертый обновляет локальную БД с некоторой периодичностью или по запросу от ATmega.

При помощи sketch также реализована Arduino_Web_Pannel веб-страница, позволяющая просматривать локальные журналы устройства и инициировать обновления локальной базы данных. Для получения доступа к веб-странице необходимо прямое подключение к микроконтроллеру через Ethernet-кабель, а также прохождение процедуры аутентификации.

Серверная часть (2) и (6) представлена каталогом сервлетов Tomcat [30], на котором развернуто war-приложение. War-приложение разрабатывается в рамках фреймворка Spring [31], который уже имеет готовые решения в области доступа к базе данных (пакет DAO

Support) и реализации базовых требований к безопасности (пакет Spring Security).

Посредником между war-приложением и базами данных (3) и (7) является пул соединений C3P0 [32], который основан на JDBC [29]. C3P0 обеспечивает большую гибкость соединения: он позволяет распределять подключения к базе данных для разных пользователей с разными правами, а также реализует механизмы управления нагрузкой.

База данных Access_DB_Server (3) содержит информацию о пользователях системы, бесконтактных картах, ролях пользователей, устройствах и правах доступа на эти устройства для каждой из ролей.

Клиентская часть администратора (4) представлена jar-приложением, запуск которого осуществляет администратор, предварительно пройдя процедуру аутентификации путем ввода логина и пароля.

Клиентская часть, расположенная на пользовательском компьютере (5), представлена jar-приложением, запуск которого осуществляет операционная система при успешной попытке входа/выхода в/из системы. При запуске клиент (5) отправляет сообщение на Syslog_App_Server (6) с информацией о параметрах входа в систему. При отсутствии сети (как правило, сеть появляется через несколько секунд после входа в систему) клиент пытается отправить сообщение с определенным интервалом вплоть до успешной отправки или выхода из системы.

База данных Syslog_DB_Server (7) содержит информацию о событиях и инцидентах безопасности, происходящих в системе.

Взаимодействие компонентов системы осуществляется в рамках сетевого соединения при помощи HTTP-сообщений, так как сообщения обладают большей надежностью, легко поддаются регулированию, поддерживают асинхронное взаимодействие и обеспечивают легкую интеграцию. Сообщения формируются по принципу построения GET-запросов, так как подобная структура устойчива к ошибкам и обеспечивает легкость интеграции компонентов.

Скорость отклика системы контроля доступа в помещение зависит от скорости работы отдельных компонент ВУ. Так, скорость работы ATmega 32U4 зависит от скорости чтения бесконтактных карт технологии RFID и скорости вывода текстовой информации, составляя 30,1 мс. Скорость взаимодействия между ATmega 32U4 и AR9331 зависит от скорости чтения текстовых файлов и записи в них, составляя в среднем 316,2 мс. Скорость обработки запросов и ответов Access_App_Server составляет 47,1 мс и также может варьироваться в зависимости от степени загруженности сервера или канала связи. Таким образом, среднее время между моментом считывания RFID карты и выводом устройством информации составляет 393,4 мс.

7. Анализ. Методика проектирования защищенных встроенных устройств определяет оптимальную конфигурацию защиты, которая соответствует функциональным требованиям на основе нефункциональных требований. Множество альтернатив компонентов защиты задается в специальной базе данных, которая также содержит информацию о совместимости (наличии или отсутствии возможных конфликтов) между компонентами защиты. Оптимальное решение, получаемое на основе работы методики, напрямую зависит от содержимого специальной базы данных, а также от заданных функциональных и нефункциональных требований. Таким образом, качество предоставляемого методикой набора зависит от полноты и актуальности специальной базы данных и корректности заданных требований. Поэтому в общем случае методика проектирования защищенных встроенных устройств не является полноценной заменой экспертного мнения.

Эксперт в области компонентов защиты встроенных устройств, обладая знаниями о специализированных решениях, с большой долей вероятности подберет достаточно эффективный набор компонентов защиты. Но результат работы методики способен принести пользу в случае значительного числа функциональных требований защиты и рассматриваемых альтернатив компонентов защиты в условиях использования программного средства Конфигуратор. Данное средство позволяет автоматизировать стадии 6 и 8 методики, ручное выполнение которых затруднительно. Конфигуратор также может предложить альтернативы субъективным предпочтениям и известным решениям эксперта.

К особенностям предложенной методики можно отнести и то, что она предоставляет возможность заменить собой функции эксперта, определяющего выбор необходимых компонентов защиты, базируясь на заложенных экспертных знаниях, позволяя разработчикам системы сфокусироваться непосредственно на разработке системы защиты и тем самым упростить сложность процесса разработки.

В соответствии с [33] предлагаемая методика относится к категории технических процессов и позволяет реализовывать организационные и проектные функции для оптимизации пользы и снижения рисков, являющихся следствием технических решений и действий [33]. В отличие от [33] предлагаемая методика определяет процесс проектирования защищенных встроенных устройств в части анализа системных требований, проектирования архитектуры системы, процесса реализации с учетом нефункциональных характеристик, входящих в состав компонентов защиты с решением поставленной оптимизационной задачи и с использованием предложенной эвристики.

Отметим также, что оптимальность получаемого в результате применения методики решения понимается в терминах достижения наилучших значений заданных нефункциональных показателей при фиксированных ограничениях на параметры защищенности. Поэтому задача проверки выполнимости критериев оценки информационной безопасности [34] выходит за рамки настоящей статьи. Тогда как точность решения задачи дискретной оптимизации на множестве конфигураций защиты определяется точностью исходных значений нефункциональных показателей компонентов защиты.

В соответствии с [35] предложенную методику можно отнести к следующим стадиям и этапам создания автоматизированных систем в защищенном исполнении [35]: формирование требований к системе защиты информации, разработка (проектирование) системы защиты информации. В соответствии с [36] проектируемую систему охраны периметра можно отнести в качестве интегрированной системы безопасности – подсистемы комплексной системы безопасности в части реализации функций охранной и пожарной сигнализации [36] с учетом требований к энергоэффективности, стоимости и физическим параметрам отдельных компонентов защиты.

На примере разработанного прототипа системы охраны периметра помещения представлена предлагаемая методика, ее основные стадии, а также способы отбора и оценки возможных компонентов защиты на предмет получения оптимального решения. При этом отметим, что задача разработки полнофункционального программно-технического решения по организации системы охраны периметра и контроля доступа коммерческого или ведомственного уровня с учетом всех актуальных требований и критериев из приведенных выше стандартов в предметной области выходит за рамки проведенного исследования. При этом такие требования и критерии, будучи специфицированы в терминах входных данных методики, могут быть реализованы посредством применения методики путем задания соответствующих функциональных требований к защите.

8. Заключение. В работе предложена методика проектирования защищенных встроенных устройств на основе комбинирования компонентов защиты. Особенностью методики является использование правил выбора компонентов защиты с учетом функциональных и нефункциональных характеристик компонентов защиты, ограничений устройства и связей между компонентами с использованием оптимизационного подхода. Для проверки методики была выбрана задача проектирования защищенной системы охраны периметра в части реализации функций контроля доступа в помещение. Данная система

представляет собой встроенное устройство, расположенное в дверях между помещениями и подключенное к механизму управления замком. С помощью разработанной методики был осуществлен выбор наиболее подходящего для решения данной задачи микроконтроллера и дополнительных компонент.

Литература

1. *Vasilevskaya M.* Designing Security-enhanced Embedded Systems: Bridging Two Islands of Expertise // PhD thesis. Linkoping Studies in Science and Technology. Sweden. 2013.
2. *Desnitsky V., Kotenko I., Chechulin A.* Configuration-based approach to embedded device security // Springer-Verlag. 2012. LNCS. 7531. pp. 270–285.
3. *Desnitsky V., Kotenko I.* Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices // Springer-Verlag. 2014. LNCS 8708. pp. 194–210.
4. *Henzinger T., Sifakis J.* The Embedded Systems Design Challenge // Springer-Verlag. LNCS 4085. 2006. pp.1–15.
5. Object Management Group. The UML Profile for MARTE: Modeling and Analysis of Real-Time and Embedded Systems. version 1.1. 2011.
6. *Hwang D., Schaumont P., Tiri K., Verbauwhede I.* Securing Embedded Systems // IEEE Security and Privacy. 2006. vol. 4. no. 2. pp. 40–49.
7. *Knezevic M., Rozic V., Verbauwhede I.* Design Methods for Embedded Security // Telfor Journal. 2009. vol. 1. no. 2. pp. 69–72.
8. *Moyers B., Dunning J., Marchany R., Tron J.* Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices // Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS'10). IEEE Computer Society. 2010. pp.1–9.
9. *Gogniat G., Wolf T., Burleson W.* Reconfigurable Security Primitive for Embedded Systems // Proceedings of International Symposium on In System-on-Chip. 2005. pp. 23–28.
10. *Norman J.* Open Source Physical Security. URL: www.layerone.org/wp-content/uploads/2012/07/LayerOne2012-John_Norman-DIY_Access_Control.pdf (дата обращения 29.09.2016).
11. *Nojmol I.* How can Access Control Systems Improve Security and Reduce Costs? // Public Sector Estates Management, September. 2014. 8 p. URL: http://www.assaabloy.co.uk/Other/ASSA/ASSA%20ABLOY/White%20Papers/ASSA_Smartair_Whitepaper%20V3.pdf (дата обращения 29.09.2016).
12. *Ruiz J., Harjani R., Maña A., Desnitsky V., Kotenko I., Chechulin A.* A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // Proceedings of the 20th Euromicro International Conference on Parallel, Distributed and Network-Based Computing (PDP2012). Munich. Germany. 2012. pp. 261–268.
13. *Rae A., Wildman L.* A Taxonomy of Attacks on Secure Devices // Australian Information Warfare and IT Security. 2003. pp. 251–264.
14. *Abraham D., Dolan G., Double G., Stevens J.* Transaction security system // IBM Systems Journal. 1991. pp. 206–228.
15. Intel Galileo distributor shop. URL: http://newegg.com/ (дата обращения: 20.05.2015).
16. Electronic shop. URL: http://nettigo.pl/ (дата обращения: 20.05.2015).
17. Intel Galileo distributor shop. URL: http://mouser.com/ (дата обращения: 20.05.2015).

18. Electronic shop. URL: http://seeedstudio.com/ (дата обращения: 20.05.2015).
19. Energy efficiency of DC 5V Character LCD 16x2. URL: http://melt.com/ (дата обращения: 20.05.2015).
20. Amazon. URL:http://www.amazon.com (дата обращения: 20.05.2015).
21. Arduino forum. URL: http://forum.arduino.cc/ (дата обращения: 20.05.2015).
22. News portal. URL: http://linuxgizmos.com/ (дата обращения: 20.05.2015).
23. Mark VandeWettering`s blog. URL: http://brainwagon.org/ (дата обращения: 20.05.2015).
24. Beaglebone distributor shop. URL: http://digikey.com/ (дата обращения: 20.05.2015).
25. Arduino shop. URL:http://store.arduino.cc/ (дата обращения: 20.05.2015).
26. Raspberry-pi distributor shop. URL: http://alliedelec.com/ (дата обращения: 20.05.2015).
27. Beaglebone distributor shop. URL: https://adafruit.com/ (дата обращения: 20.05.2015).
28. Ebay. URL: http://ebay.com/ (дата обращения: 20.05.2015).
29. C3p0 pooling. URL: http://mchange.com/projects/c3p0/ (дата обращения: 20.05.2015).
30. Arduino references. URL: http://arduino.cc/en/Reference/ (дата обращения: 20.05.2015).
31. Apache Tomcat. URL: http://tomcat.apache.org/ (дата обращения: 20.05.2015).
32. Spring Framework. URL: http://projects.spring.io/spring-framework/ (дата обращения: 20.05.2015).
33. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств // М.: Госстандарт России. 2010.
34. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий // М.: Госстандарт России. 2008.
35. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения // М.: Госстандарт России. 2014.
36. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования // М.: Госстандарт России. 2009.

Десницкий Василий Алексеевич — к-т техн. наук, старший научный сотрудник лаборатории проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: интернет вещей, безопасность встроенных устройств, защита ПО, методы формальной верификации. Число научных публикаций — 90. vasily.desnitsky@mail.ru, http://comsec.spb.ru/desnitsky; 14-я линия В.О., 39, ком. 205, Санкт-Петербург, 199178; р.т.: +7(812)328-71-81.

Чечулин Андрей Алексеевич — к-т техн. наук, старший научный сотрудник лаборатории проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, обнаружение вторжений, анализ сетевого трафика, анализ уязвимостей. Число научных публикаций — 150. andreych@bk.ru, http://comsec.spb.ru/ru/staff/chechulin; 14-я линия В.О., 39, ком. 205, Санкт-Петербург, 199178; р.т.: +7(812)328-71-81.

Котенко Игорь Витальевич — д-р техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — 450. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7-(812)-328-71-81, Факс: +7(812)328–4450.

Левшун Дмитрий Сергеевич — программист лаборатории проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), студент, Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина). Область научных интересов: компьютерная безопасность, защита встроенных устройств, системы киберфизической безопасности, безопасность распределённых систем, корреляция событий безопасности. Число научных публикаций — 5. levshun@comsec.spb.ru, http://comsec.spb.ru/levshun; 14-я линия В.О., 39, ком. 205, Санкт-Петербург, 199178; р.т.: +7-(812)-328-71-81.

Коломеец Максим Вадимович — программист лаборатории проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), студент, Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В.И. Ульянова (Ленина). Область научных интересов: безопасность распределенных систем, визуализация данных. Число научных публикаций — 10. guardeecwalker@gmail.com; 14-я линия В.О., д. 39, ком. 205, Санкт-Петербург, 199178; р.т.: +7(812)328-71-81.

Поддержка исследований. Работа выполнена при частичной финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м, 16-37-50035), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

V.A. DESNITSKY, A.A. CHECHULIN, I.V. KOTENKO, D.S. LEVSHUN, M.V. KOLOMEEC

COMBINED DESIGN TECHNIQUE FOR SECURE EMBEDDED DEVICES EXEMPLIFIED BY A PERIMETER PROTECTION SYSTEM

Desnitsky V.A., Chechulin A.A., Kotenko I.V., Levshun D.S., Kolomeec M.V. **Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protection System.**

Abstract. In terms of information security, embedded devices are elements of complex cyber-physical systems, systems of the Internet of Things, working in a potentially hostile environment. Therefore, the development of such devices is a challenging problem, often requiring expert solutions. The complexity of developing secure embedded devices is due to different types of potential threats and attacks to the device, as well as the fact that in practice security of embedded devices is usually considered in the final stages of the development process in the form of adding additional security features. In the paper, we propose a design technique aimed at the development of safe and energy-efficient cyber-physical and embedded devices. This technique organizes a search for the best combination of security components on the basis of solving an optimization problem. The efficiency of the proposed technique is demonstrated through the development of a secure system to protect a room perimeter.

Keywords: Embedded devices, cyber-physical systems, perimeter control, design of secure cyber-physical systems.

Desnitsky Vasily Alekseevich — Ph.D., senior researcher of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science (SPIIRAS). Research interests: Internet of Things, embedded security, software protection, methods of formal verification. The number of publications — 90. vasily.desnitsky@mail.ru, http://comsec.spb.ru/desnitsky; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-71-81.

Chechulin Andrey Alexeevich — Ph.D., senior researcher of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science (SPIIRAS). Research interests: computer network security, intrusion detection, analysis of the network traffic, vulnerability analysis. The number of publications — 150. andreych@bk.ru, http://comsec.spb.ru/ru/staff/chechulin; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-71-81.

Kotenko Igor Vitalievich — Ph.D., Dr. Sci., professor, head of computer security problems Laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — 450. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-(812)-328-71-81, Fax: +7(812)328–4450.

Levshun Dmitry Sergeevich — software developer of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science (SPIIRAS), student, Saint Petersburg Electrotechnical University "LETI". Research interests:

distributed system security, embedded devices, event correlation, cyber-physical security systems. The number of publications — 5. levshun@comsec.spb.ru, http://comsec.spb.ru/levshun; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-(812)-328-71-81.

Kolomeec Maxim Vadimovich — developer of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS), student, Saint Petersburg Electrotechnical University "LETI". Research interests: distributed system security, security visualization. The number of publications — 10. guard-eecwalker@gmail.com; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-71-81.

Acknowledgements. This research was partially financially supported by grants of RFBR (projects No. 14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 ofi_m, 16-37-50035), by the budget (projects No. 0073-2015-0004 and 0073-2015-0007) as well as by Grant of Russian Science Foundation No. 15-11-30029 in SPIIRAS.

References

1. Vasilevskaya M. Designing Security-enhanced Embedded Systems: Bridging Two Islands of Expertise. PhD thesis. Linkoping Studies in Science and Technology. Sweden. 2013.
2. Desnitsky V., Kotenko I., Chechulin A. Configuration-based approach to embedded device security. Springer-Verlag. 2012. LNCS 7531. pp. 270–285.
3. Desnitsky V., Kotenko I. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices. Springer-Verlag. LNCS 8708. 2014. pp. 194–210.
4. Henzinger T., Sifakis J. The Embedded Systems Design Challenge. Springer-Verlag. 2006. LNCS 4085. pp.1–15.
5. Object Management Group. The UML Profile for MARTE: Modeling and Analysis of Real-Time and Embedded Systems. version 1.1. 2011.
6. Hwang D., Schaumont P., Tiri K., Verbauwhede I. Securing Embedded Systems. *IEEE Security and Privacy*. 2006. vol. 4. no. 2. pp.40–49.
7. Knezevic M., Rozic V., Verbauwhede I. Design Methods for Embedded Security. *Telfor Journal*. 2009. vol. 1. no. 2. pp. 69–72.
8. Moyers B., Dunning J., Marchany R., Tron J. Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices. Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS'10). IEEE Computer Society. 2010. pp. 1–9.
9. Gogniat G., Wolf T., Burleson W. *Reconfigurable Security Primitive for Embedded Systems*. Proceedings of International Symposium on In System-on-Chip. 2005. pp. 23–28.
10. Norman J. Open Source Physical Security. July 2012. URL: www.layerone.org/wp-content/uploads/2012/07/LayerOne2012-John_Norman-DIY_Access_Control.pdf (accessed 29.09.2016).
11. Nojmol I. How can Access Control Systems Improve Security and Reduce Costs? Public Sector Estates Management, September. 2014. 8 p. URL: http://www.assaabloy.co.uk/Other/ASSA/ASSA%20ABLOY/White%20Papers/ASSA_Smartair_Whitepaper%20V3.pdf (accessed 29.09.2016).
12. Ruiz J., Harjani R., Maña A., Desnitsky V., Kotenko I., Chechulin A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. Proceedings of the 20th Euromicro International Conference on Parallel, Distributed and Network-Based Computing (PDP2012). Munich. Germany. 2012. pp. 261–268.

13. Rae A., Wildman L. A Taxonomy of Attacks on Secure Devices. Australian Information Warfare and IT Security. 2003. pp.251–264.
14. Abraham D., Dolan G., Double G., Stevens J. Transaction security system // *IBM Systems Journal*. 1991. pp.206–228.
15. Intel Galileo distributor shop. Available at: http://newegg.com/ (accessed 20.05.2015).
16. Electronic shop. Available at: http://nettigo.pl/ (accessed 20.05.2015).
17. Intel Galileo distributor shop. Available at: http://mouser.com/ (accessed 20.05.2015).
18. Electronic shop. Available at: http://seeedstudio.com/ (accessed 20.05.2015).
19. Energy efficiency of DC 5V Character LCD 16x2. Available at: http://melt.com/ (accessed 20.05.2015).
20. Amazon Available at: http://www.amazon.com (accessed 20.05.2015).
21. Arduino forum. Available at: http://forum.arduino.cc/ (accessed 20.05.2015).
22. News portal. Available at: http://linuxgizmos.com/ (accessed 20.05.2015).
23. Mark VandeWettering`s blog. Available at: http://brainwagon.org/ (accessed 20.05.2015).
24. Beaglebone distributor shop. Available at: http://digikey.com/ (accessed 20.05.2015).
25. Arduino shop. Available at: http://store.arduino.cc/ (accessed 20.05.2015).
26. Raspberry-pi distributor shop. Available at: http://alliedelec.com/ (accessed 20.05.2015).
27. Beaglebone distributor shop. Available at: https://adafruit.com/ (accessed 20.05.2015).
28. Ebay. Available at: http://ebay.com/ (accessed 20.05.2015).
29. C3p0 pooling. Available at: http://mchange.com/projects/c3p0/ (accessed 20.05.2015).
30. Arduino references. Available at: http://arduino.cc/en/Reference/ (accessed 20.05.2015).
31. Apache Tomcat. Available at: http://tomcat.apache.org/ (accessed 20.05.2015).
32. Spring Framework. Available at: http://projects.spring.io/spring-framework/ (accessed 20.05.2015).
33. GOST R ISO/MJK 12207-2010. [Information technology. System and software engineering. The processes of software life cycle]. M.: Gosstandart Rossii. 2010. (In Russ.).
34. GOST R ISO/MJK 15408-1-2008. [Information technology. Methods and security features. Criteria for Information Technology Security Evaluation]. M.: Gosstandart Rossii. 2008. (In Russ.).
35. GOST R 51583-2014. [Data protection. The order of creation of automated systems in the protected design. General provisions]. M.: Gosstandart Rossii. 2014. (In Russ.).
36. GOST R 53704-2009. [Security systems complex and integrated. General specifications]. 2009. (In Russ.).

УДК 004.056.5 **DOI** 10.15622/sp.48.2

Е.С. Новикова, И.В. Котенко

ВЫЯВЛЕНИЕ АНОМАЛЬНОЙ АКТИВНОСТИ В СЕРВИСАХ МОБИЛЬНЫХ ДЕНЕЖНЫХ ПЕРЕВОДОВ С ПОМОЩЬЮ RADVIZ-ВИЗУАЛИЗАЦИИ

Новикова Е.С., Котенко И.В. **Выявление аномальной активности в сервисах мобильных денежных переводов с помощью RADViz-визуализации.**

Аннотация. Сети мобильной связи представляют собой удобную инфраструктуру для предоставления финансовых сервисов, поскольку они обладают рядом достоинств, связанных с широким распространением и достаточно низкой себестоимостью финансовых транзакций. В настоящей работе рассматривается сценарий мобильных денежных переводов, в которых оператор сотовой связи не только предоставляет инфраструктуру, но и выпускает виртуальные денежные средства.

В работе авторы предлагают новый подход к анализу транзакций, основанный на использовании группы взаимосвязанных интерактивных моделей визуализации данных, характеризующих действия пользователей в системе денежных переводов. В его основе лежит графическое представление пользователей с помощью методики визуализации RadViz. Она позволяет выделить группы пользователей, обладающих схожим поведением, и абонентов, своим поведением отличающихся от основной массы, и при этом обладает низкой вычислительной сложностью. Анализ научных работ показал, что авторы первыми предложили использовать данную методику визуализации для исследования денежных переводов. RadViz-визуализация пользователей сервиса мобильных денежных переводов поддерживается графом их контактов. Граф контактов является наиболее распространенной методикой графического представление операций в финансовых системах, поскольку он позволяет изучить структурные свойства связей между пользователями, выявив мосты и клики графа.

Разработанная методика визуального анализа была апробирована на тестовых данных, содержащих различные сценарии мошеннической деятельности в СМДП. Анализ применения RadViz-визуализации пользователей системы на различных тестовых данных показал, что она полезна при обнаружении мошеннических сценариев, которые предполагают использование пользователей-мулов, чье поведение существенно отличается от поведения других абонентов СМДП. Таким образом, она позволяет выявить финансовые правонарушения, которые связаны с длительными, возможно, незначительными изменениями в поведении пользователей, однако имеющих кумулятивный эффект, и поэтому могут быть раскрыты при выборе достаточно длительного периода времени. По этой причине данная модель визуализации оказалась эффективна при обнаружении мулов в схеме отмывания денег и мобильной бот-сети.

1. Введение. Сети мобильной связи представляют собой удобную инфраструктуру для предоставления финансовых сервисов, поскольку они обладают рядом достоинств, связанных с широким распространением и достаточно низкой себестоимостью финансовых транзакций. В настоящей работе рассматривается сценарий мобильных денежных переводов, в которых оператор сотовой связи не только предоставляет инфраструктуру, но и выпускает виртуальные денежные

средства. Этот сервис позволяет своим пользователям вносить и снимать деньги, переводить деньги другим пользователям, оплачивать счета, оплачивать сотовую связь. Пользователи таких сервисов могут иметь различные роли в системе, они могут быть розничными агентами оператора мобильной связи, с помощью которых осуществляются операции пополнения мобильного счета и снятия с них денежных средств, поставщиками различных услуг и товаров и обычными пользователями финансовых сервисов.

Рост покрытия сотовых сетей, а также их доступность обеспечивает широкое распространение сервисов мобильных денежных переводов (СМДП), особенно в развивающихся странах, таких как Кения, Индия, Уганда и Филиппины [1, 2]. Особенно эти сервисы востребованы у людей, которые не имеют своего собственного банковского счета и которым намного удобнее и проще использовать мобильный телефон для выполнения платежей и денежных переводов другим пользователям. В последнее время наблюдается рост популярности подобных сервисов и в развитых странах, в которых жители лишились банковского счета в результате распространения финансового кризиса, и провайдеры финансовых сервисов оценивают потенциал новых платежных систем, возникших в развивающихся странах для удовлетворения потребностей пользователей.

Однако по мере роста рынка СМДП повышаются и риски, связанные с их использованием, поскольку они становятся объектом атаки опытных и высоко мотивированных злоумышленников, а большие объемы данных значительно снижают способность механизмов обнаружения вредоносной активности своевременно выявлять нарушения. Как и другие системы денежных переводов, СМДП могут быть использованы в схемах отмывания денежных средств или получения доступа к данным пользователей СМДП для получения финансовой выгоды (кража мобильного устройства или заражение вредоносным программным обеспечением) и т.д.

В настоящей статье авторы предлагают новый подход к анализу транзакций, основанный на использовании группы взаимосвязанных интерактивных моделей визуализации данных, характеризующих действия пользователей СМДП и способствующих обнаружению аномалий и возможных правонарушений. Выбранные модели визуализации позволяют аналитику получить общее представление об активности в системе, а затем сосредоточиться на пользователях, представляющих особый интерес, путем детализации их операций. В основе предложенного подхода лежит графическое представление пользователей с помощью методики визуализации RadViz [3]. Она позволяет выделить группы пользователей, обладающие схожим

поведением, и абонентов, своим поведением отличающихся от основной массы, и при этом обладает низкой вычислительной сложностью.

Статья структурирована следующим образом. В разделе 2 представлены методики визуализации, используемые для обнаружения финансовых махинаций. В разделах 3 и 4 детально описываются исходные данные и предложенный подход, в том числе разработанные модели визуализации и методики взаимодействия с ними. В разделе 5 представлена общая методика работы с предложенными моделями визуализации, а в разделах 6 и 7 представлены результаты ее использования для выявления финансовых мошенничеств различного типа в СМДП. В заключении подводятся итоги исследования и обозначаются дальнейшие направления исследований.

2. Методики визуального анализа для обнаружения аномальной активности в СМДП. Применение автоматических методик анализа для обнаружения любых схем мошенничества предполагает, что данные четко структурированы, полны и корректны, не изменяются с течением времени, и задача четко определена [4]. Реальные данные редко отвечают этим требованиям. Кроме того, эти методики в большинстве случаев воспринимаются конечными пользователям как черные ящики, выдающие конечный результат без его пояснения. Методы визуальной аналитики помогают справиться с огромными объемами разнородных и зашумленных данных. Их можно рассматривать как процесс генерации и проверки гипотезы, который интуитивно понятен и не требует явного применения сложных математических и статистических методов [4-10].

Сложность структуры финансовых данных позволяет применять различные методики визуализации для их анализа — графы на параллельных координатах, матрицы рассеивания, специальные глифы, карты деревьев, представления на основе иконок и пикселей, дендрограммы. В большинстве случаев они предназначены для решения таких задач, как анализ финансового рынка в целом или отдельных сегментов в частности, оценку финансовых показателей компаний, оценку инвестиций за длительное время.

Модели визуализации, применяемые для обнаружения подозрительной активности в финансовых системах, достаточно просты. Большая часть коммерческого программного обеспечения [11-13] использует линейные графики, круговые диаграммы, гистограммы и глифы в виде измерительных приборов для отображения характеристик финансовых потоков, количества зарегистрированных предупреждений, их типа и критичности и т.д. Выбор этих визуальных моделей объясняется простотой их понимания и способностью передавать наиболее важную информацию. Кроме того, они легко

могут быть включены в отчеты любого уровня и назначения. Помимо стандартных визуальных моделей, в системах обнаружения подозрительной финансовой деятельности часто присутствуют географические карты, поскольку они позволяют обнаруживать регионы с высоким уровнем финансовых рисков, а также определять границы ответственности организации.

Выявление скрытых взаимосвязей между пользователями и отслеживание денежных потоков чаще всего осуществляется с помощью графов контактов пользователей [12-15]. Вершинами графа могут быть различные объекты финансовой деятельности: счета, идентификаторы пользователей, телефоны, кредитные карты, адреса, организации и т.д. Ребра между ними указывают на использование или участие соответствующего объекта в финансовых операциях, а толщина линии обозначает частоту сделки транзакций субъектами. Графы позволяют обнаруживать скрытые связи между клиентами финансовых организаций, формировать паттерны денежных потоков, характерные для мошеннических операций.

Интересная графическая метафора KnotLines для представления последовательности электронных транзакций предложена в [16]. В ее основе лежит нотная нотация: линии отображают связи между операциями, а узлы кодируют подробную информацию о сделках. Это представление поддерживается пиксельным-ориентированным представлением, которое отображает меру схожести транзакции заданному логическому выражению. Сочетание этих двух представлений позволяет достаточно быстро идентифицировать представляющие интерес сделки из большого набора данных.

Похожий подход реализован в инструменте WireVis [17], который был разработан в сотрудничестве с Банком Америки. Транзакции отображаются с помощью специального графического представления, названного Strings and Beads (строки и бисер), в котором строки ссылаются на счета или кластера счетов в течение длительного времени, а бусинки относятся к конкретным операциям, выполненным за заданный день. Основной акцент в нем делается на частотный анализ ключевых слов транзакций.

3. Исходные данные СМДП. В общем случае информация о персональных данных пользователей, а также данные по операциям, совершаемых ими в СМДП, является конфиденциальной и, как следствие, закрытой для исследователей. Одним из возможных решений проблемы отсутствия реальных данных, необходимых как для разработки, так и оценки моделей и методик визуального анализа, используются искусственно сгенерированные данные. Этот подход

широко применяется при обучении моделей анализа данных в системах автоматического обнаружения и предотвращения вторжений [18].

Для моделирования платформы мобильных денежных платежей и действий пользователей в работе используется генератор транзакций СМДП [18]. Он позволяет создавать тестовые наборы данных, содержащие различные сценарии аномальной активности. Используемые в генераторе модели легитимного и вредоносного поведения пользователей построены на основе свойств реальных транзакций СМДП. Кроме того, они содержат специальное поле ground proof, определяющее тип транзакции — легитимная или мошенническая, которое может быть использовано для проверки корректности результатов, полученных в процессе анализа.

Генератор транзакций СМДП формирует только логи транзакций, которые содержат следующую информацию: номера телефонов отправителя и получателя, идентификаторы их счетов, роль абонентов в системе (подписчик системы, поставщик услуг, оператор и т.д.), идентификатор транзакции, метка времени, тип транзакции (индивидуальные денежные переводы между физическими лицами, пополнение и снятие денежных средств из мобильного кошелька, и т.д.), сумма денежного перевода, статус транзакции (успешно завершена, ошибка), а также баланс отправителя и приемника до и после операции. Исследование показало, что этих данных достаточно для того, чтобы выявить признаки нелегитимного использования системы мобильных денежных переводов.

Разработанная методика визуального анализа была апробирована на тестовых данных, содержащих различные сценарии мошеннической деятельности в СМДП. Следует отметить, что в сгенерированных сценариях каждый подписчик СМДП имеет только одну учетную запись в системе и роль, связанную с ним (ней), однако это не влияет на точность полученных результатов.

4. Модели визуализации и методики взаимодействия с ними. В основе предлагаемой авторами методики лежит RadViz-визуализация транзакций СМДП. Она позволяет выявить группы пользователей, характеризующих схожим поведением в системе. Под поведением пользователя в системе авторы понимают, какие типы операций обычно совершает пользователь в СМДП, как часто и на какие суммы.

RadViz-визуализация является нелинейной методикой визуализации многомерных данных, которая выполняет отображение n-мерных данных на 2-мерное пространство. Исследуемые признаки объектов представляются в виде координат, размещаемых по окружности. Затем объекты отображаются в виде точек внутри круга,

их положение определяется с помощью метафоры из физики: каждая точка соединяется с помощью *n* пружин к *n* координатным узлам.

Жесткость каждой пружины пропорциональна значению соответствующего атрибута объекта. Таким образом, точка располагается в месте, где силы растяжения пружин находятся в равновесии. Очевидно, что объекты, имеющие более высокое значение определенного атрибута, будут располагаться ближе к соответствующему координатному узлу. Если все *n* атрибутов имеют одинаковые значения, то точка данных находится точно в центре круга. Если объект имеет атрибуты с одинаковыми значениями, а соответствующие координатные узлы располагаются друг напротив друга на окружности, то точка лежит недалеко от центра. В качестве примера рассмотрим рисунок 1.

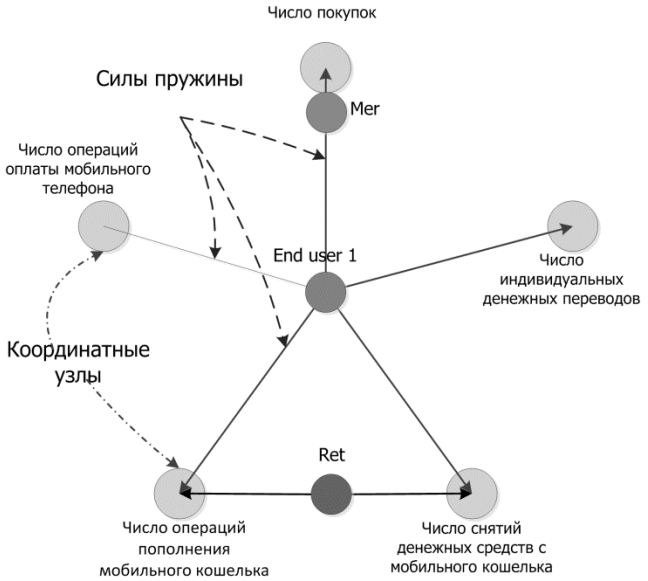


Рис. 1. Схема представления пользователей СМДП с помощью RadViz-визуализации (цвета с учетом схемы)

В соответствии с рисунком 1 пользователь ***Mer*** расположен на оси *Число покупок*, что означает, что он участвует только в операциях предоставления различных розничных услуг и покупок, что, возможно, объясняется его ролью в системе. Пользователь ***Ret*** в равной мере участвует в операциях пополнения мобильного кошелька денежными

средствами и снятием их со счета. Пользователь ***End user 1*** расположен в центре единичного круга, что говорит о том, что одинаково часто пользуется всеми доступными операциями в СМДП: пополнение мобильного кошелька денежными средствами, снятие денег с мобильного кошелька, оплата услуг мобильной связи, покупка товаров и перевод денежных средств другим пользователям системы. Данную методику визуализации можно рассматривать как алгоритм кластеризации, имеющий низкую вычислительную сложность — $O(n)$, где n — число объектов.

Авторы предлагают использовать следующие атрибуты в качестве координатных узлов для описания поведения пользователя в системе мобильных денежных платежей: количество операций различного типа за заданный период времени; средняя сумма денежных переводов с разбиением по типам операций; минимальная или максимальная сумма денежного перевода за заданный период времени с разбиением по типам операций.

Пользователи СМДП отображаются в виде точек разного цвета внутри единичной окружности. Цвет используется для кодирования их роли в СМДП, например, конечные пользователи закрашиваются оранжевым цветом, оператор сотовой связи — желтым, поставщики розничным услуг — пурпурно-красным и т.д. Авторы предполагают, что пользователи, имеющие одинаковую роль в системе, должны формировать группы точек, расположенных рядом, что объясняется схожим поведением в системе. Например, точки, обозначающие поставщиков розничных услуг, должны образовать группу. Расположение конечных пользователей предсказать труднее, поскольку они в общем случае обладают разнообразным поведением в системе, тем не менее они также могут образовывать кластеры точек. Таким образом, следующие особенности расположения точек на графе могут являться признаками потенциального мошенничества:

– пользователь не принадлежит ни к одному кластеру или входит в группу пользователей, имеющих другую роль;

– расположение небольшой группы пользователей существенно отличается от остальных.

Эти аномалии могут стать отправной точкой в анализе действий пользователя в СМДП.

Следует отметить, что расположение точек на плоскости при RadViz-визуализации сильно зависит от выбора координатных узлов и их расположения, т.е. не для каждого набора выбранных атрибутов имеется возможность выявить кластеры и выбросы в данных. Для n

атрибутов существует (n - 1)! / 2 возможных проекций RadViz [19]. Из этого утверждения следует, что при выборе трех атрибутов транзакции в качестве координатных узлов формируется только одна нетривиальная RadViz-проекция объектов, поэтому авторы рекомендуют использовать следующие три атрибута в качестве координат:

– количество индивидуальных переводов за заданный период времени;

– количество операций пополнения мобильного кошелька за заданный период времени;

– количество операций по снятию наличных денег за заданный период времени.

Тем не менее в системе, реализующей предложенную разработанную методику, предусмотрена возможность настройки координат RadViz-визуализации, что позволяет аналитику экспериментировать с исследуемыми данными, выбирая атрибуты из предопределенного списка и задавая их последовательность.

Для исследования контактов пользователей СМДП авторы предлагают использовать граф. Граф контактов является наиболее распространенной методикой графического представления операций в финансовых системах [7, 13, 15, 17]. Основным преимуществом использования графов является возможность изучить структурные свойства связей между пользователями, выявив мосты и клики графа.

В предложенной методике визуального анализа граф используется традиционным образом: его вершины обозначают пользователей системы, а связи между ними — транзакции, связывающие их. Как и в случае RadViz-визуализации, цвет используется для обозначения роли пользователя в СМДП, он также применяется для кодирования типа транзакции. Следует отметить, что все используемые в прототипе цветовые схемы предназначены для отображения категорийных данных, подчеркивают их отличия между собой и созданы с помощью специальной утилиты Color-Brewer [20]. Она позволяет формировать цветовые схемы с учетом типа исходных данных (качественные или количественные), а также характера решаемой задачи (выявление выбросов, сравнение последовательных значений). Кроме того, она позволяет выбрать цвета, которые являются безопасными для людей, страдающих нарушением цветоощущения.

Форма вершины графа зависит от того, является ли пользователь только отправителем транзакций (ромб), получателем (эллипс) или выполняет обе роли (прямоугольник). Эта опция помогает упростить процесс обнаружения абонентов, чьи счета используются только для

снятия наличных или пополнения мобильных кошельков. Если пользователи связаны между собой множеством транзакций одного типа, то они отображаются одной линией, толщина которой определяется мощностью этого множества. Аналитик может управлять размером вершин графа: он может быть определен суммой как принятых, так и отправленных денежных переводов за определенный период времени. Эта опция помогает обнаружить абонентов, которые участвуют в крупных денежных потоках.

Процесс визуального анализа графа поддерживается различными механизмами взаимодействия: фильтрация данных, эффект связывания, управление укладкой вершин графа и получение детальной информации.

Механизм фильтрации позволяет задавать аналитику сложные логические выражения для отображения множества пользователей СМДП или транзакций данных, отвечающих поставленным условиям. Применение эффекта связывания и затемнения позволяет изучить контакты конкретного пользователя: в этом режиме видимыми остаются все входные и выходные ребра выбранного узла, а остальные — скрываются.

Различные способы укладки вершин графа дают возможность аналитику изучить структуру графа. Авторы предлагают использовать два способа укладки графа — радиальный и специальный, в основе которого лежит график рассеивания.

Укладка вершин графа на основе графика рассеивания строится следующим образом. Для каждого узла рассчитываются два параметра — общее число транзакций, совершенных пользователем, и число различных типов транзакций, используемых им. Эти два параметра определяют положение соответствующего узла на плоскости: x-координата определяется общим количеством всех сделок, а y-координата определяется количеством различных типов транзакций (рисунок 2).

Радиальное расположение вершин графа удобно для изучения контактов уже выбранного пользователя. Укладка узлов графа на основе графика рассеивания позволяет быстро разбить пользователей на группы с различным уровнем активности и числом различных типов операций, и поэтому она может быть особенно полезна на начальном этапе изучения логов системы СМДП, поскольку позволяет проверить корректность структурных связей между пользователями.

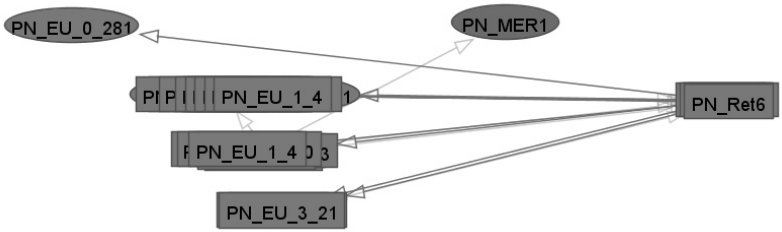


Рис. 2. Расположение вершин графа контактов пользователей СМДП на основе графика рассеивания

Информация о вершинах и ребрах графа доступна в виде всплывающей подсказки и таблицы свойств объектов. Всплывающая подсказка содержит краткую информацию об элементе графа: идентификатор пользователя, количество совершенных операций, тип транзакции, отправитель и получатель денежного перевода. Таблица свойств объекта предоставляет детальную информацию по выбранному объекту. Для вершин графа, представляющих пользователей СМДП, выводятся следующие данные: число выполненных операций с разбивкой по их типам; минимальная, максимальная и средняя суммы денежных переводов с детализацией по типам операций; общая сумма полученных и отправленных денежных переводов. По клику мышки по ребру графа в таблице свойств отображается информация о типе транзакции, ее получатель и отправитель, число транзакций между ними, минимальная и максимальная суммы денежных переводов, статус транзакций.

5. Сценарии использования методики. Любой процесс поиска информации может быть описан следующим образом: общий вид → масштабирование, фокусирование → детали по требованию [21]. Следуя этому принципу, процесс исследования транзакций СМДП может быть описан следующим образом.

На первом этапе аналитик формирует общее понимание об активности всех пользователей в СМДП в рамках выбранного периода времени и выявляет множество пользователей, деятельность которых по каким-либо признакам отличается от остальных. Эта задача может быть выполнена с помощью RadViz-визуализации данных или графа контактов с применением специальной укладки вершин графа.

На следующем этапе аналитик исследует контакты каждого пользователя из определенного ранее множества, и при необходимости

проводит детальный анализ непосредственно транзакций данного пользователя СМДП.

Разработанная методика визуального анализа данных была реализована в программном прототипе MMTViewer, написанном на языке программирования Java. Модели визуализации и механизмы взаимодействия реализованы с использованием графической библиотеки Prefuse Toolkit [22], которая позволяет создавать сложные интерактивные графические представления.

Предлагаемая в работе методика была апробирована на множестве тестовых данных, содержащих следующие сценарии финансовых мошенничеств: отмывание денег, кража мобильного телефона и заражение устройств вредоносным ПО. Все тестовые данных были получены с помощью генератора транзакций СМДП, представленного выше.

6. Выявление схем по отмыванию денежных средств. Существует несколько схем по отмыванию денег [23]. Используемый в работе сценарий финансового правонарушения предполагает использование так называемых пользователей-мулов, с помощью которых обычно скрывается происхождение нелегитимных денег и затрудняется отслеживание финансовых потоков. Мошенники, имеющие определенную сумму денег для отмывания, обычно разделяют ее на несколько частей и отправляют их пользователям-мулам. Позже они выводят эти деньги, используя пользователей, выполняющих роль поставщиков различных услуг и товаров. Последовательности мулов могут состоять из нескольких слоев. В анализируемом сценарии применяется только один слой из нескольких мулов. Тем не менее это условие не ограничивает возможности предлагаемого подхода к обнаружению мошенничества, поскольку задачей предлагаемой методики является выявление аномальной активности в СМДП любого типа, а не конкретной мошеннической финансовой схемы.

При обнаружении аномальной активности с помощью разработанной методики мы использовали следующие исходные предположения: сумма нелегитимных операций меньше, чем средняя сумма обычных, легитимных транзакций; мулы также выполняют законные сделки; внезапное изменение в передаваемых денежных суммах соответствует аномалии.

Эти предположения определили, какие атрибутов транзакций следует использовать в качестве координатных узлов модели визуализации RadViz: количество индивидуальных денежных

переводов, количество операций пополнения мобильного кошелька и количество операций снятия денежных средств из него.

Результат RadViz-визуализации пользователей СМДП представлен на рисунок 3. Видно, что существует группа агентов оператора мобильной связи, обозначенных подписью ***Агенты***, которая расположена обособленно от других абонентов СМДП, это объясняется тем, что они участвуют только в операциях снятия денежных средств с мобильного кошелька и его пополнения. Обычные пользователя СМДП образуют достаточно большую группу точек оранжевого цвета, расположенных достаточно плотно и равномерно вдоль оси Ind. Transfer (num), обозначающей индивидуальные денежные переводы. Это говорит о том, что данный тип финансовых операций преобладает над двумя другими типами. Положение точек на сравнительно равноудаленном расстоянии от координатных узлов Deposit (num) и Withdrawal (num) свидетельствует о том, что пользователи в равном количестве совершают операции пополнения и снятия денежных средств с мобильного кошелька. На рисунке 3 легко можно увидеть двух обычных пользователей системы, которые лежат отдельно от остальных конечных пользователей ***Пользователи 1***. Они отмечены подписью ***Пользователи 2***.

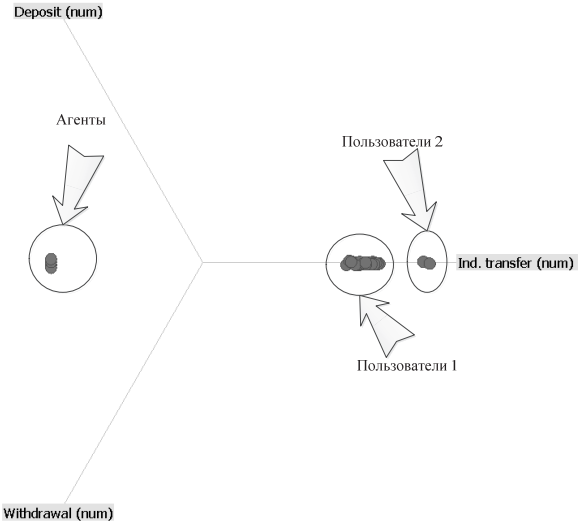


Рис. 3. RadViz-визуализация пользователей СМДП в исследуемом сценарии по отмыванию денег

Их расположение объясняется значительным преобладанием индивидуальных денежных переводов над финансовыми операциями других типов. Граф контактов показал: (1) один из этих пользователей (пользователь PN_FR1) посылает деньги, а другой (пользователь PN_FR2) только получает их; 2) они соединены друг с другом через конечное множество пользователей (рисунок 4). Следовательно, можно сделать вывод, что PN_FR1 и PN_FR2 могут быть потенциальными мошенниками, а подписчики, связанные с ними, — мулы.

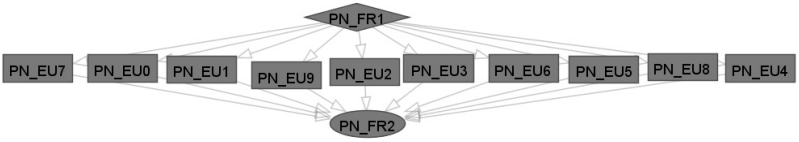


Рис. 4. Структура пользователей-мулов в исследуемом сценарии по отмыванию денег

7. Выявление поведенческих финансовых мошенничеств. Под поведенческим мошенничеством понимаются сценарии незаконной финансовой деятельности, в которых действия мошенника накладываются на легитимные операции обычного пользователя. Примерами такого типа финансовых нарушений являются кража мобильного телефона или заражение мобильного устройства вредоносным программным обеспечением. В этих случаях одно мобильное устройство используется двумя пользователями (легитимным и злоумышленником) одновременно.

Используемые тестовые данные содержали два сценария поведенческого мошенничества. В первом сценарии моделировалось заражение мобильных устройств вредоносным кодом. После заражения вредоносная программа выполняет несколько денежных переводов пользователям-мулам, которые затем снимают деньги с мобильного кошелька в течение 72 часов после их получения. Эта схема мошенничество довольно похожа на схему по отмыванию денег, отличаются лишь суммы денежных переводов, и пользователи-мулы используются здесь для того, чтобы скрыть конечное место перевода украденных денег, а не их происхождение. Вторая схема поведенческого мошенничества соответствует краже мобильного телефона. После кражи мобильного устройства злоумышленник в течение достаточно короткого отрезка времени совершает несколько попыток снять деньги с мобильного кошелька, пытаясь успеть до того момента, как кража телефона будет обнаружена, а телефон отключен.

Очевидно, что поведенческие мошенничества характеризуются изменениями в частоте транзакций и переводимой сумме денег. По этой причине в качестве координатных узлов модели визуализации RadViz были выбраны число индивидуальных переводов, число снятий мобильных денег и пополнения мобильного кошелька, число переводов за покупки и оплата эфирного времени сотовому оператору в единицу времени. На рисунке 5 показаны результаты RadViz-визуализации пользователей СМДП. Видно, что есть группы точек фиолетового и розового цвета, обозначающие поставщиков розничных услуг (***Продавцы***) и агентов оператора мобильной связи (***Агенты***) соответственно, и лежащих обособленно в силу особенностей их роли в СМДП. Большинство конечных пользователей расположены кучно в центре единичного круга, что означает, что они достаточно равномерно используют операции, выбранные в качестве координат RadViz-визуализации. Однако есть группа, состоящая из четырех пользователей, у которых индивидуальные денежные переводы значительно преобладают над транзакциями других типов. На рисунке 5 они помечены как ***Пользователи 1***.

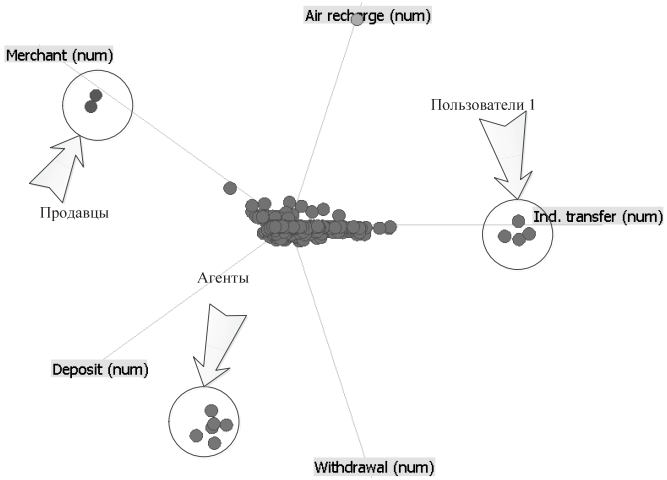


Рис. 5. RadViz-визуализация пользователей СМДП в сценарии поведенческих мошенничеств

Кроме того, анализ контактов этих пользователей выявил, что множества пользователей СМДП, отправляющие им денежные средства, пересекаются. Эти два факта позволяют сделать вывод, что выявленные четыре пользователя являются мулами, чьи учетные

записи используются для получения, а затем снятия мобильных денег с мобильного кошелька.

RadViz-визуализация пользователей СМДП оказалась полезной при выявлении мулов в схеме по отмыванию денег и сценарии заражения мобильных устройств вредоносным кодом, однако выявить случаи кражи мобильных телефонов с ее помощью оказалось невозможно.

8. Заключение. В настоящей работе авторы предложили методику визуального анализа данных, в основе которой лежит метафорическое представление поведения пользователей СМДП на основе RadViz-визуализации. Анализ применения RadViz-визуализации пользователей системы на различных тестовых данных показал, что она полезна при обнаружении мошеннических сценариев, которые предполагают использование пользователей-мулов, чье поведение существенно отличается от поведения других абонентов СМДП. Таким образом, она позволяет выявить финансовые правонарушения, которые связаны с длительными, возможно, незначительными изменениями в поведении пользователей, однако имеющих кумулятивный эффект, и поэтому могут быть раскрыты при выборе достаточно длительного периода времени. По этой причине данная модель визуализации оказалась эффективной при обнаружении мулов в схеме отмывания денег и мобильной бот-сети.

Авторы предлагают использовать данную модель графического представления данных в качестве отправной точки анализа транзакций, который поддерживается также традиционным представлением транзакций пользователя в виде графа. В работе описан сценарий использования предложенной методики визуального анализа транзакций на примере обнаружения схемы отмывания денежных средств и поведенческих мошенничеств.

Дальнейшие исследования будут связаны с реализацией методик взаимодействия, осуществляющих поиск объектов по заданному шаблону, а также проработкой вопросов масштабирования предложенных методик с учетом больших объемов данных.

Литература

1. Mobile Payment System. URL: http://www.vodafone.com/content/index/about/about-us/money_transfer.html (дата обращения 22.05.2016).
2. Infographic: Tanzania's Mobile Money Revolution. URL: http://www.cgap.org/data/infographic-tanzanias-mobile-money-revolution (дата обращения 22.05.2016).
3. *Ankerst M., Berchtold S., Keim D.A.* Similarity Clustering of Dimensions for an Enhanced Visualization of Multidimensional Data // Proc. of 1998 IEEE Symposium on Information Visualization (INFOVIS '98). IEEE Computer Society. 1998. pp. 52–60.

4. *Keim D., Andrienko G., Fekete J.-D., Goerg C., Kohlhammer J., Melancon G.* Visual Analytics: Definition, Process, and Challenges // Information Visualisation. Springer-Verlag, Berlin Heidelberg. 2008. vol. 4950. pp.154–175.
5. *Kotenko I., Novikova E.* VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment // Proc. of the 3rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013). Springer. Heidelberg. 2013. vol. 8128. pp. 345–360.
6. *Novikova E., Kotenko I.* Analytical Visualization Techniques for Security Information and Event Management // Proc. of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). 2013. pp. 519–525.
7. *Novikova E., Kotenko I.* Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services // Lecture Notes in Computer Science. Berlin. Heidelberg: Springer-Verlag. 2014. vol. 8708. pp. 63–78.
8. *Котенко И.В., Новикова Е.С.* Визуальный анализ защищенности компьютерных сетей // Информационно-управляющие системы. Санкт-Петербург. 2013. № 3. С. 56–61.
9. *Котенко И.В., Новикова Е.С.* Методики визуального анализа в системах управления информационной безопасностью компьютерных сетей // Вопросы защиты информации. Москва. 2013. № 3. С. 33–42.
10. *Новикова Е.С., Котенко И.В.* Анализ механизмов визуализации для обеспечения защиты информации в компьютерных сетях // Труды СПИИРАН. 2012. № 4(23). С. 7–30.
11. Financial Crime Risk Management solution. URL: http://www.fiserv.com/risk-compliance/financial-crime-risk-management.htm (дата обращения 22.05.2016).
12. Nice Actimize Integrated Fraud Management. http://www.niceactimize.com/index.aspx?page=solutionsfraud (дата обращения 22.05.2016).
13. SAS Fraud detection solutions. URL: http://www.sas.com/offices/europe/uk/industries/banking/fraud-detection.html (дата обращения 22.05.2016).
14. Delloite. Visual Analytics: Revealing Corruption, Fraud, Waste, and Abuse. Presentation of the Forensic Center. URL: http://www.slideshare.net/DeloitteForensicCenter/visual-analytics-revealing-corruption-fraud-waste-and-abuse-13958016 (дата обращения 22.05.2016).
15. *Westphal C.R.* Patterns for Financial Intelligence Units (FIUs) and Anti-Money Laundering (AML) Operations. URL: http://support.visualanalytics.com/technicalArticles/whitePaper/pdf/VAI%20AML%20FIU%20Patterns%20Presentation.pdf (дата обращения 22.05.2016).
16. *Xie C., Chen W., Huang X., Hu Y., Barlowe S., Yang J.* VAET: A Visual Analytics Approach for E-Transactions Time-Series // IEEE Transactions Visualization and Computer Graphics. 2014. vol. 20(12). pp. 1743–1752.
17. *Chang R. et. al*: Visualization of Categorical, Time-Varying Data From Financial Transactions // Proc. of IEEE Symposium on Visual Analytics Science and Technology (VAST 2007). 2007. pp. 155–162.
18. *Gaber C., Hemery B., Achemlal M., Pasquet M., Urien P.* Synthetic logs generator for fraud detection in mobile transfer services // Proc. of Int. Conference on Collaboration Technologies and Systems (CTS 2013). 2013. pp.174–179.
19. *Di Caro L., Frias-Martinez V., Frias-Martinez E.* Analyzing the Role of Dimension Arrangement for Data Visualization in Radviz // Proc. of Advances in Knowledge Discovery and Data Mining. 2010. LNCS 6119. pp. 125–132.
20. ColorBrew2. URL: http://colorbrewer2.org. (дата обращения 22.05.2016).

21. *Shneiderman B.* Dynamic queries for visual information seeking // The Craft of Information Visualization: Readings and Reflections. Morgan Kaufman Publishers. 2003. pp. 14–21.
22. Prefuse Information Visualization toolkit. URL: http://prefuse.org/ (дата обращения 22.05.2016).
23. Money Laundering using New Payment Methods. URL: http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneyla (дата обращения 22.05.2016).

Новикова Евгения Сергеевна — к-т техн. наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: визуальная аналитика, вредоносное программное обеспечение, двухключевая криптография. Число научных публикаций — 45. evgeshka19@mail.ru, http://www.comsec.spb.ru/en/staff/novikova; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328–2642.

Котенко Игорь Витальевич — д-р техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — 450. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328–2642, Факс: +7(812)328–4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проекты №14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482 офи_м), при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также гранта РНФ 15-11-30029 в СПИИРАН.

E.S. Novikova, I.V.Kotenko

DETECTION OF ANOMALOUS ACTIVITY IN MOBILE MONEY TRANSFER SERVICES USING RADVIZ-VISUALIZATION

Novikova E.S., Kotenko I.V. **Detection of Anomalous Activity in Mobile Money Transfer Services Using RadViz-Visualization.**

Abstract. Nowadays, mobile communication networks represent a key enabling infrastructure for financial service provision, since they offer significant opportunities for increasing the efficiency and pervasiveness of such services by expanding access and lowering transaction costs. In the paper, the authors analyze the use case of mobile money transfer services which are managed by a mobile network operator who not only provides infrastructure to financial services but also emits mobile money.

In this paper, we present an interactive multi-view visualization approach that provides a better insight in the large data sets describing MMTS activity. It is based on a RadViz-related visualization of the MMTS users that helps to determine groups of similarities and outliers among them and is characterized by low computational complexity. To the best of knowledge of the authors, this work is the first to exploit the RadViz-visualization technique to visualize MMTS subscribers. RadViz –based presentation of the MMTS users is supported by interactive graph based visualization of their contacts. The graph of the users' contacts is often used to analyze financial transactions as it allows discovering structural peculiarities such as bridges and cliques.

The proposed visual analytics technique was evaluated on different test data sets containing different fraudulent financial scenarios. Summarizing the results of the efficiency evaluation of the proposed visualization technique for MMTS transaction activity, we can say that RadViz visualization is helpful when detecting fraudulent scenarios which make use of mules users whose behavior significantly differs from the behavior of the other MMTS subscribers. It also allows detecting frauds associated with shifts in user behavior which have cumulative character. Thus these frauds can be revealed when choosing a relatively long period of time (e.g. a month) to explore MMTS transactions. That is why this technique was effective when detecting mules in the money laundering scheme and the mobile botnet.

Novikova Evgenia Sergeevna — Ph.D., senior researcher of the computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: security visual analytics, malware, public key cryptography. The number of publications — 45. evgeshka19@mail.ru, http://www.comsec.spb.ru/en/staff/novikova; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328–2642.

Kotenko Igor Vitalievich — Ph.D., Dr. Sci., professor, head of computer security problems Laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — 450. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328–2642, Fax: +7(812)328–4450.

Acknowledgements. This research is supported by RFBR (projects No. 14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338, 16-29-09482), in part by the budget (projects No. 0073-2015-0004 and 0073-2015-0007) and by the grant of RSF 15-11-30029 in SPIIRAS.

References

1. Mobile Payment System. Available at: http://www.vodafone.com/content/index/about/about-us/money_transfer.html (accessed 22.05.2016).
2. Infographic: Tanzania's Mobile Money Revolution. Available at: http://www.cgap.org/data/infographic-tanzanias-mobile-money-revolution (accessed 22.05.2016).
3. Ankerst M., Berchtold S., Keim D.A. Similarity Clustering of Dimensions for an Enhanced Visualization of Multidimensional Data // Proceedings of 1998 IEEE Symposium on Information Visualization (INFOVIS '98). IEEE Computer Society. 1998. pp. 52–60.
4. Keim D., Andrienko G., Fekete J.-D., Goerg, C., Kohlhammer, J., Melancon, G. Visual Analytics: Definition, Process, and Challenges. *Information Visualisation*. Springer-Verlag, Berlin Heidelberg. 2008. vol. 4950. pp. 154–175.
5. Kotenko I., Novikova E. VisSecAnalyzer: a Visual Analytics Tool for Network Security Assessment. Proceedings of the 3rd IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2013). Springer. Heidelberg. 2013. vol. 8128. pp. 345–360.
6. Novikova, E., Kotenko, I. Analytical Visualization Techniques for Security Information and Event Management. Proceedings of the 21th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2013). 2013. pp. 519–525.
7. Novikova E., Kotenko I. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services. Proceedings of the 4th IFIP International Workshop on Security and Cognitive Informatics for Homeland Defense (SeCIHD 2014). Springer. Heidelberg: Springer-Verlag. 2014. vol. 8708. pp. 63–78.
8. Kotenko I.V., Novikova E.S. [Visual analysis of the security of computer networks]. *Informacionno-upravljajushhie sistemy – Information and Control Systems*. 2013. vol. 3. pp. 56–61. (In Russ.).
9. Kotenko I.V., Novikova E.S. [Methods of visual analysis in control systems for information security of computer networks]. *Voprosy zashhity informacii – Information security issues.* 2013. vol. 3. pp. 33–42. (In Russ.).
10. Novikova E.S., Kotenko I.V. [Analysis of the Visualization Techniques used for Information Security in the Computer Networks]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2012. vol. 4(23). pp.7–30. (In Russ.).
11. Financial Crime Risk Management solution. Available at: http://www.fiserv.com/risk-compliance/financial-crime-risk-management.htm (accessed 22.05.2016).
12. Nice Actimize Integrated Fraud Management. Available at: http://www.niceactimize.com/index.aspx?page=solutionsfraud (accessed 22.05.2016).
13. SAS Fraud detection solutions. Available at: http://www.sas.com/offices/europe/uk/industries/banking/fraud-detection.html (accessed 22.05.2016).
14. Delloite. Visual Analytics: Revealing Corruption, Fraud, Waste, and Abuse. Presentation of the Forensic Center. Available at: http://www.slideshare.net/DeloitteForensicCenter/visual-analytics-revealing-corruption-fraud-waste-and-abuse-13958016 (accessed 22.05.2016).
15. Westphal C.R. Patterns for Financial Intelligence Units (FIUs) and Anti-Money Laundering (AML) Operations Available at: http://support.visualanalytics.com/

technicalArticles/whitePaper/pdf/VAI%20AML%20FIU%20Patterns%20Presentation.pdf (accessed 22.05.2016).
16. Xie C., Chen W., Huang X., Hu Y., Barlowe S., Yang J. VAET: A Visual Analytics Approach for E-Transactions Time-Series. *IEEE Transactions Visualization and Computer Graphics*. 2014. vol. 20(12). pp. 1743–1752.
17. Chang R. et. al. Visualization of Categorical, Time-Varying Data From Financial Transactions. Proceedings of IEEE Symposium on Visual Analytics Science and Technology (VAST 2007). 2007. pp. 155–162.
18. Gaber C., Hemery B., Achemlal M., Pasquet M., Urien P. Synthetic logs generator for fraud detection in mobile transfer services. Proceedings of Int. Conference on Collaboration Technologies and Systems (CTS 2013). 2013. pp.174–179.
19. Di Caro L., Frias-Martinez V., Frias-Martinez E. Analyzing the Role of Dimension Arrangement for Data Visualization in Radviz. Proceedings of Advances in Knowledge Discovery and Data Mining. 2010. LNCS 6119. pp. 125–132.
20. ColorBrew2. Available at: http://colorbrewer2.org. (accessed 22.05.2016).
21. Shneiderman B. Dynamic queries for visual information seeking. *The Craft of Information Visualization: Readings and Reflections*. Morgan Kaufman Publishers. 2003. pp. 14–21.
22. Prefuse Information Visualization toolkit. Available at: http://prefuse.org/ (accessed 22.05.2016).
23. Money Laundering using New Payment Methods. Available at: http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneyla (accessed 22.05.2016).

УДК 004.94 **DOI** 10.15622/sp.48.3

И.И. Лившиц

МЕТОДИКА ОПТИМИЗАЦИИ ПРОГРАММ АУДИТА ИНТЕГРИРОВАННЫХ СИСТЕМ МЕНЕДЖМЕНТА

Лившиц И.И. **Методика оптимизации программы аудита интегрированных систем менеджмента.**

Аннотация. Применение интегрированных систем менеджмента (ИСМ) в настоящее время привлекает внимание высшего руководства самых разных организаций: нефтеперерабатывающих, приборостроительных, авиационных и оборонных. Однако, на данный момент остается важной проблемой выполнение аудита в ИСМ — реализация в полном объеме комплекса проверок различных стандартов ISO при ограничении или существенном сокращении доступных ресурсов.

В то же время постоянное совершенствование принципов управления, и в частности переход к мышлению, основанному на рисках, обеспечивают повышение интереса к рациональному применению стандартов ISO. В данном исследовании предлагается методика оптимизации программы аудита ИСМ, основанная на принципах непрерывной адаптации при поступлении данных в течение одного микроцикла аудита. Дополнительным преимуществом данной методики является применение численных метрик аудита информационной безопасности, способствующих постоянному повышению уровня обеспечения информационной безопасности организаций.

Ключевые слова: информационная безопасность, интегрированная система менеджмента, стандарт, аудит, система менеджмента информационной безопасности.

1. Введение. В последнее время применение интегрированных систем менеджмента (ИСМ) привлекает внимание высшего руководства (лиц, принимающих решения — ЛПР) различных организаций. Наблюдаются практически единичные случаи, когда современные организации самой разной отраслевой принадлежности (нефтеперерабатывающие, приборостроительные, авиационные и оборонные) внедряют только одну систему менеджмента (СМ), напротив, сейчас, как правило, реализуются именно проекты ИСМ. Рассмотрим несколько крупнейших российских организаций, в которых автору в течение длительного периода 2010–2015 гг. доводилось выполнять аудит ИСМ:

- «КАМАЗ-Дизель» (машиностроение);
- «Теплоком» (приборостроение);
- «Водоканал Санкт-Петербург» (коммунальные услуги);
- «Газпром трансгаз Москва» (транспортировка газа).

В таблице 1 представлены примеры реализации систем менеджмента информационной безопасности (СМИБ).

Однако на данный момент остается важной проблемой обеспечение выполнения программы аудита в ИСМ — реализация в полном объеме комплекса проверок по различным стандартам ISO при

существенном сокращении доступных ресурсов. В большей степени эта проблема характерна для обеспечения программы аудита ИСМ для проверок информационной безопасности (ИБ), поскольку негативные последствия инцидентов ИБ могут привести к существенному ущербу для организации, вплоть до прекращения деятельности.

Таблица 1. Примеры реализации проектов ИСМ

Организация	Стандарты ISO	Национальные стандарты (ГОСТ)	**Источник**
«КАМАЗ-Дизель» (Набережные Челны)	9001 14001 18001 16949 27001	РВ 0015-002-2012	http://www.kamaz.ru/about/policy/labor-protection/; http://www.kamaz.ru/about/quality/system/
«Теплоком» (Санкт-Петербург)	9001 14001 18001 50001	Нет	http://www.teplocom-holding.ru/about/licenses_and_certificates/ http://www.teplocom-holding.ru/about/our_policy/
«Водоканал Санкт-Петербург» (Санкт-Петербург)	9001 14001 18001 50001 27001	Нет	http://www.vodokanal.spb.ru/o_kompanii/ohrana_okruzhayuwej_sredy/ http://www.regcon.ru/index.php/konsalting/ohsas-18001
«Газпром трансгаз Москва» (Москва)	9001 14001 18001 50001 27001	ГОСТ Р ИСО/МЭК 27001-2006	http://moskva-tr.gazprom.ru/ecology/ http://www.rusregister.ru/press-center/association-news/?ELEMENT_ID=15701

В то же время постоянное совершенствование принципов управления, и в частности, переход к мышлению, основанному на рисках, обеспечивают повышение интереса к рациональному применению современных риск-ориентированных стандартов [1-5]. Соответственно, представляет определенный интерес изучение существующих проблем при выполнении аудита ИСМ, а также поиск способов оптимизации программы аудита ИСМ, основанных на принципах непрерывной адаптации при поступлении данных в течение одного микроцикла PDCA (Plan-Do-Check-Act), т.е. одного элементарного цикла аудита. На основании практики выполнения аудитов ИСМ предлагается новая методика оптимизации программы аудита, которая позволит обеспечить более рациональное принятие решений для ЛПР в современной сложной экономической обстановке [6–8].

2. Общие аспекты управления аудитом. Как отмечалось ранее, для обеспечения стабильного развития современных организаций в условиях наличия рисков различного происхождения, представляется целесообразным применение риск-ориентированных стандартов и внедрение ИСМ [9-11, 12-17]. С точки зрения управления аудитом ИСМ в предлагаемой методике отметим необходимость решения следующих важных практических задач (в скобках указаны пункты стандарта аудита СМ — ИСО 19011 [18]):

1. Задача выделения ресурсов для программы аудита:
   - — разработка программы аудита (5.1);
   - — идентификация и оценка рисков программы аудита (5.3.4);
   - — идентификация ресурсов для программы аудита (5.3.6).
2. Задача учета факторов, влияющих на глубину программы аудита утечки, инциденты, проявление криминальных действий, выявленные ранее несоответствия, а следовательно — определение объема программы аудита (5.3.3).
3. Задача сбора верифицируемой информации (6.4.6).
4. Задача обеспечения специальных знаний и навыков аудиторов (7.2.3.3), либо привлечение технических экспертов по следующим областям:
   - — осуществляемые виды деятельности;
   - — требования заинтересованных сторон;
   - — знание процессов обеспечения ИБ;
   - — знание технических средств и мер обеспечения ИБ.

Дополнительно отметим, что в ИСМ должны быть приняты к сведению и рекомендации PAS-99 [5], что позволяет учесть специфические требования выполнения комбинированных аудитов, учета рисков, гибкого управления объемом программы аудита ИСМ с учетом предшествующих результатов и важности процессов [19-21].

3. Принципы организации гибких аудитов. Предлагаемая методика оптимизации программы аудита ИСМ основана на следующих основных принципах:

1. Вводится понятие интегральной оценки (ИО) ИБ, которая включает определенный групповой показатель оценки всех вынесенных на аудит ИБ процессов — R_{ISMS}. Этот групповой показатель определяется с помощью взвешенной суммы частных показателей, в которой весовые коэффициенты определяют важность процесса R_{PR} в организации ИБ для конкретного объекта оценки (ОО).
2. После проведения начального (первичного) аудита ИБ по каждому проверяемому процессу оценивается его состояние на

предмет соответствия требованиям критериев аудита (стандартам ISO, ГОСТ, СТО Газпром СОИБ и пр.), а также его влияние на ИО уровня ИБ для конкретного ОО.

3. Последующие аудиты ИБ проводятся по предложенной методике, использующей гибкий подход: наиболее детально и тщательно подвергаются проверке те процессы, по которым на предыдущем аудите выявлены существенные несоответствия (например, в нотации ISO 17021 — “major” [22]) и которые имеют наибольший приоритет в ИО для конкретного ОО.

4. Частота и детальность, которая должна быть дифференцирована для различных проверяемых процессов, также увязывается с ИО. Например, определенные группы процессов, которые в ИО имеют приоритетное значение (например, в зависимости от модели актуальных угроз ИБ) подвергаются аудитам более детально и чаще. Процессы, имеющие более низкий приоритет в ИО для конкретного ОО, проверяются реже и менее детально.

5. Глубина проверки и частота аудитов каждый раз для k-ого аудита в микроцикле PDCA определяется в зависимости от приближения функции ИО для конкретного ОО к некоему установленному целевому показателю — Rtar (в пределе, очевидно, равным 1) для комплексной оценки защищенности конкретного ОО.

Дополнительно отметим важность внедрения нового стандарта ISO 55000 [2-4], т.к. многие активы не управляются должным образом (например, в силу применения устаревших внутренних процедур СТО Газпром СОИБ в принципе не оперирует такими активами, как персонал, здания, сооружения). Соответственно, применение требований уже внедренного стандарта (например, ISO 27001) значительно облегчает решение «типовых» задач безопасности, которые решаются параллельно (учет и защита активов, управление рисками, оценка компетенции и пр.), рекомендуется к параллельной проверке в рамках совместных аудитов всех СМ [22-24].

4. Математическая постановка задачи. Для оценки степени соответствия системы обеспечения ИБ при аудите ИСМ предъявляемым требованиям ИБ используются частные и групповые показатели ИБ. Например, для целей проведения аудита ИСМ в аспекте обеспечения ИБ предлагается применять показатель результативности СМИБ R_{ISMS}, вычисляемый в каждом цикле k-го аудита по аддитивной формуле (весовой коэффициент *i*-го процесса обозначим как α_i и показатель результативности *i*-го процесса ИБ обозначим как R_{PRi}:

$$R_{ISMS} = \sum_{i=1}^{n} \alpha_i \cdot R_{\Pr i}, \quad (1)$$

при этом сумма весовых коэффициентов α_i нормируется:

$$\sum_{i=1}^{n} \alpha_i = 1.$$

Показатель результативности конкретного *i*-го процесса ИБ R_{PRi}, в свою очередь, вычисляется также по аддитивной свертке метрик ИБ (*j*-ю метрику ИБ для *i*-го процесса ИБ обозначим как K_{KPIij}, а весовой коэффициент — как β_{ij}). В формуле (2) допускается ситуация, когда количество метрик m не будет одинаковым для разных циклов, соответственно, необходимо говорить об m_i:

$$R_{\Pr_i} = \sum_{j=1}^{m_i} \beta_{ji} \cdot K_{PKIji}, \quad (2)$$

при этом сумма весовых коэффициентов β_{ij} нормируется:

$$\sum_{j=1}^{m_i} \beta_{ij} = 1.$$

Сумма весовых коэффициентов частных показателей ИБ, используемых при вычислении группового показателя ИБ, должна быть равной 1, что обеспечивает нормирование всех показателей в аддитивных формулах (1) и (2). Показатель результативности СМИБ R_{ISMS} должен быть в пределе равен 1.

В процессе аудита ИСМ постоянное измерение «невязки» текущего для k-го аудита R_{ISMS} измеряется как рассогласование с целевым показателем $R_{ISMStar}$, и крайне важно обеспечить его минимум. Следовательно, задача оптимизации может быть отнесена к типу задач статической оптимизации для процессов управления, протекающих в установившемся режиме. Необходимо реализовать оптимизационную модель для процесса аудита ИСМ в условиях детерминированных ограничений и условной оптимизации (минимальной «невязки»):

$$F(y) \to \min, \quad (3)$$

где: $F(y) \in R^m$, $f(y) \in R^1$. $f(y)$ — целевая функция m-мерного векторного аргумента ***y***, такого что: $y = (y_1, y_2, \ldots y_m)$. Область допустимых значений $y \in D \subset R^m$. Таким образом, рассматривается вид задачи условной оптимизации. Установленные ограничения (II-го рода, в виде неравенства):

$$g_i(y) \geq 0; i = \overline{1, N}.$$

Параметры m-мерного векторного аргумента ***y*** могут быть, например, следующими:

- T — период аудитов ИБ;
- S — плановая стоимость аудитов ИБ;
- V — объем аудитов ИБ (количество подразделений);
- F — перечень функциональных вопросов аудитов ИБ;
- O — перечень посещаемых объектов аудитов ИБ.

По итогам оценки всех процессов аудитов, выполняемых в строгом соответствии с программой аудита ИСМ, заполняется следующая матрица (таблица 2).

Таблица 2. Схема размещения результатов аудита процессов ИБ

Аудит / Процесс	1	2	…	k
PR_1	PKI_{11}	PKI_{12}		PKI_{1k}
PR_2	PKI_{21}	PKI_{22}		PKI_{2k}
…	…	…	…	…
PR_i	PKI_{i1}	PKI_{i2}		PKI_{ik}

5. Базовый оптимизационный цикл программы аудита ИСМ. На основании имеющихся стандартов аудита (в частности [18]), отраслевых методик (СТО ИББС БР, СТО Газпром СОИБ и пр.), предложим метод многошаговой оптимизации процесса аудита ИСМ для сложных промышленных объектов (СлПО), который позволяет обеспечить систему координации, распределения ресурсов и оперативного доведения результатов аудитов ИСМ до ЛПР. Предложенный метод обеспечивает целенаправленное оперативное функционирование подсистемы ИБ в составе ИСМ и отличается от существующих методов проведением циклической непрерывной оценки результативности R_{ISMS} на основе оптимальной системы

численных показателей (метрик) ИБ { PKI_{ik} }. Предложенный метод состоит из 2-х связанных циклов оптимизации программы аудита ИСМ, отличающихся наличием новых блоков:

1. Базового оптимизационного цикла, который характеризует эффективное выполнение аудита ИСМ в терминах оценки результативности для каждого PR_i-процесса ИБ и каждой PKI_j– метрики ИБ, а также определяет параметры циклов оптимизации ресурсов в программе аудита: глубину ("*scope*"), размер аудиторской выборки, количество привлекаемых аудиторов (экспертов) и пр.

2. Быстрого блока оценки результативности мер коррекции и корректирующих действий в текущем k-м аудите, затрагивающие изменения как следующего процесса ИБ, так и следующего в программе (k+1)-го аудита. Также обеспечивается быстрый переход к оценке показателей результативности ИСМ RISMS в k-м аудите и (k+1)-го аудите для постоянной и оперативной оптимизации всей программы аудита ИСМ.

Рассмотрим базовый оптимизационный цикл программы аудита ИСМ, построенный с учетом формальных требований стандартов ISO по аудиту, стандартов ISAGO, стандартов СТО Газпром и СТО БР ИББС и дополненных новыми компонентами (рисунок 1):

– Формирование оценок результативности по каждому k-му аудиту.

– Формирование быстрой оценки результативности коррекции (корректирующих действий).

– Формирование быстрой обратной связи в текущем цикле аудита.

– Формирование реакции системы — «устрожения» и (или) «смягчения» в зависимости от ИО в текущем цикле аудита.

– Формирование ИО защищенности ИСМ.

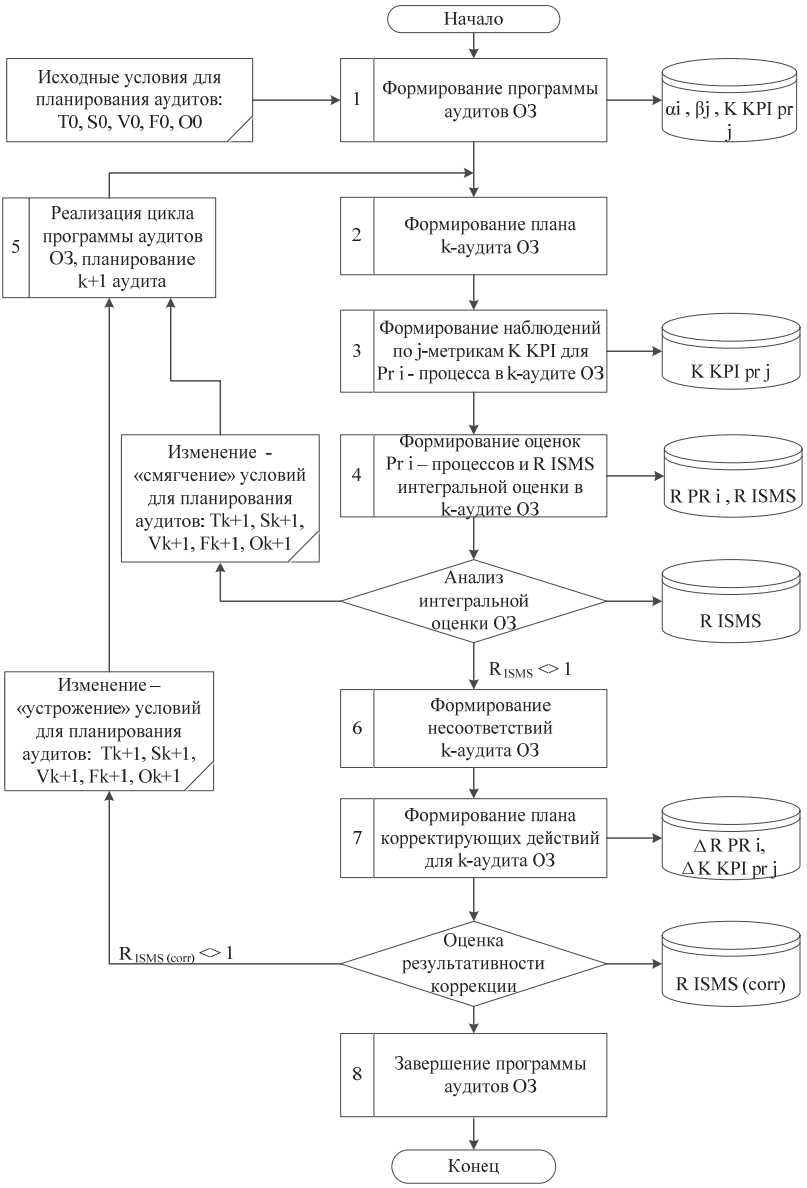


Рис. 1. Базовый оптимизационный цикл программы аудита ИСМ

Определены предусловия (входные данные) для старта базового оптимизационного цикла программы аудита:

- T_0 — базовый период аудитов ИБ.
- S_0 — базовая (плановая) стоимость аудитов ИБ.
- V_0 — базовый объем аудитов ИБ (количество подразделений);
- F_0 — базовый перечень функциональных вопросов аудитов ИБ;
- O_0 — базовый перечень посещаемых объектов аудитов ИБ.

Описание базового оптимизационного цикла программы аудита ИСМ представлено далее по основным шагам.

Шаг 1. Формирование программы аудита, оценивается $R_{ISMS} \geq R_{ISMS\ tar}$ (в соответствии с (1) и (2)). В результате определяются:

- α — весовой коэффициент для групповой метрики процесса ИБ;
- β — весовой коэффициент для частной метрики процесса ИБ;
- k — количество аудитов ИБ в программе аудита;
- R_{ISMS} — текущая ИО результативности СМИБ;
- $R_{ISMS\ tar}$ — целевая ИО результативности СМИБ;
- γ — количество аудитов в программе аудита;
- Δ — допустимая «невязка» показателя $R_{\mathbf{ISMS\ tar}}$;
- $K_{PR\ i}$ — целевой показатель результативности *i*-процесса;
- $K_{KPI\ j}$ — целевой показатель результативности *j*-метрики для *i*-процесса.

Шаг 2. Формирование плана k-го аудита. В результате утверждается план k-го аудита.

Шаг 3. Выполнение k-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 4. Выполняется сбор наблюдений по итогам k-го аудита, соответственно $K_{PR\ i}$ и $K_{KPI\ j}$. В результате заполняется база данных аудита показателями $K_{PR\ i}$ и $K_{KPI\ j.}$

Шаг 5. Выполняется формирование оценки R_{ISMS} — интегральной оценки на k-м аудите. В результате заполняется база данных аудита показателем R_{ISMS} для k-го аудита.

Шаг 6. Выполняется оценка степени достижения R_{ISMS} по итогам k-го аудита целевого показателя $R_{ISMS\ tar}$. В результате заполняется база данных аудита показателем R_{ISMS} для k-го аудита.

Шаг 7. В случае, если $R_{ISMS} \geq R_{ISMS\ tar}$, т.е. достигается установленный показатель результативности, выполняется информирование руководителя программы аудита о возможном «смягчении» условий планирования (k+1)-го аудита. В частности, могут быть снижены частота или объем программы аудита, что, соответственно, снизит и затраты на выполнение аудитов. Далее переход на шаг 13 к реализации (продолжению) программы аудита,

выполнению (k+1)-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 8. В случае, если $R_{ISMS} < R_{ISMS\ tar}$, т.е. не достигает установленный показатель результативности, выполняется формирование перечня несоответствий на k-м аудите. Выполнение далее (k+1)-го аудита может быть приостановлено по решению руководителя программы аудита с целью снижения расходов. В результате формируется отчет по итогам k-го аудита.

Шаг 9. На основании сформированного перечня несоответствий на предыдущем шаге формируется план коррекции и корректирующих действий для выявленных несоответствий на k-м аудите. В результате выполняется заполнение базы данных аудита показателями, соответственно, ΔK_{PRi} и ΔK_{KPIj} для k-го аудита, который характеризует степени отклонения, соответственно, по целевому показателю PR_i-процесса ИБ в целом и $K_{KPI\ j}$ по отдельным (частным показателям).

Шаг 10. Выполняется оценка результативности коррекции и корректирующих действий по несоответствиям, выявленным по итогам k-го аудита. В результате выполняется заполнение базы данных аудита показателем R_{ISMS} (corr) для k-го аудита.

Шаг 11. В случае, если $R_{ISMS\ (corr)} \geq R_{ISMS\ tar}$, т.е. достигается полностью установленный показатель результативности корректирующих мер для всех выявленных несоответствий по итогам k-го аудита, выполняется информирование руководителя программы аудита и в случае отсутствия иных несоответствий за период реализации корректирующих мер — завершение программы аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 12. В случае, если $R_{ISMS\ (corr)} < R_{ISMS\ tar}$, т.е. не достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий по итогам k-го аудита, выполняется информирование руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности, могут быть увеличены частота или объем программы аудита для тех PR *i*-процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудитов в дальнейшем. Далее переход на шаг 13 к реализации (продолжению) программы аудита, выполнению (k+1)-го аудита. В результате формируется отчет по итогам k-го аудита.

Шаг 13. В случае, если подтверждена результативность корректирующих мер для всех выявленных несоответствий на k-го аудите, выполняется переход к дальнейшей реализации (продолжении) программы аудита и выполнению (k+1)-го аудита.

6. Быстрый блок оценки результативности программы аудита ИСМ. Быстрый блок оценки результативности мер коррекции и корректирующих действий в текущем k-м аудите, определяющий изменения как следующего процесса, так и следующего в

программе (k+1)-го аудита, а также же быстрый переход к оценке показателей результативности СМИБ представлены на рисунке 2.

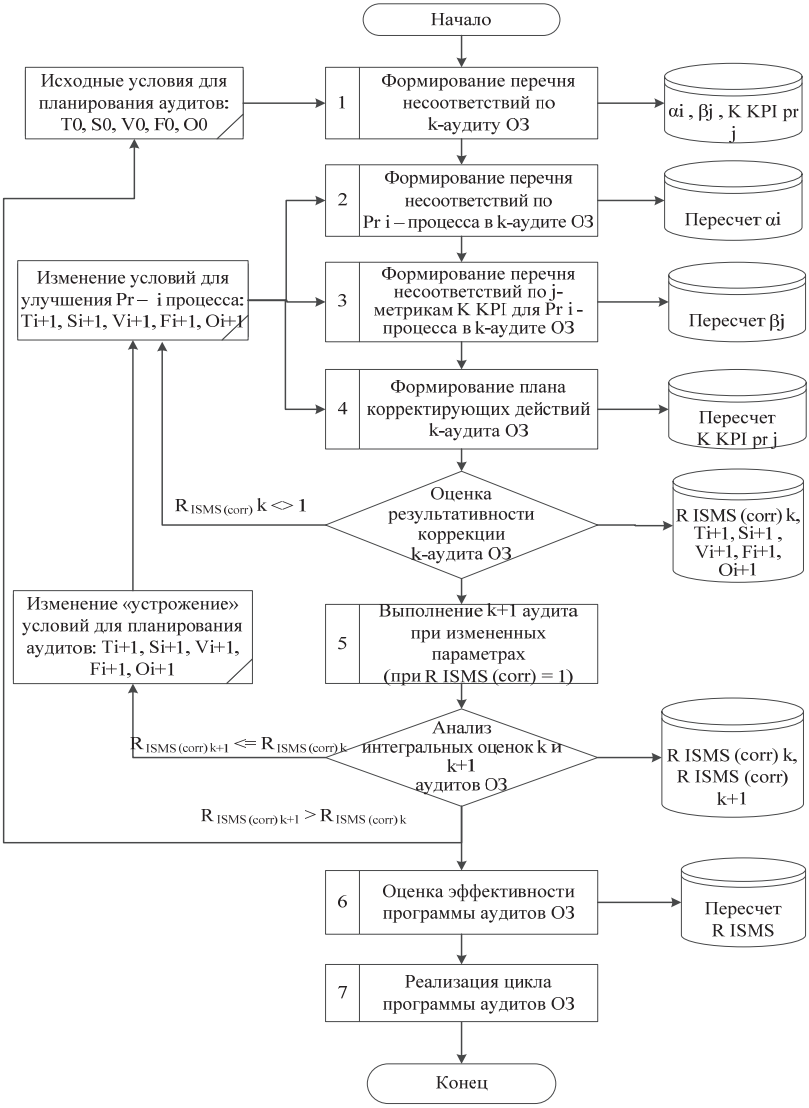


Рис. 2. Быстрый блок оценки результативности программы аудита ИСМ

Описание быстрого блока оценки результативности программы аудита ИСМ представлено далее по основным шагам.

Шаг 1. Формирование программы аудита. В результате определяются:

- α — весовой коэффициент для групповой метрики процесса ИБ;
- β — весовой коэффициент для частной метрики процесса ИБ;
- k — количество аудитов ИБ в программе аудита ОЗ;
- RISMS — текущая ИО результативности СМИБ;
- RISMS tar — целевая ИО результативности СМИБ;
- γ — количество аудитов в программе аудитов;
- Δ — допустимая «невязка» показателя RISMS tar;
- KPR i — целевой показатель результативности j-процесса;
- $K_{KPI\,j}$ — целевой показатель результативности *i*-метрики для *j*-процесса.

Шаг 2. В случае выявленных несоответствий по установленным (базовым) критериям аудита, формируется перечень несоответствий k-го аудита. В результате формируется перечень несоответствий k-го аудита.

Шаг 3. Каждое выявленное несоответствие последовательно соотносится с определенным PR*i*-процессом ИБ. В результате выполняется пересчет весовых коэффициентов (групповых) α PR *i*-процессов ИБ. Заполнение базы данных аудита новым показателем α.

Шаг 4. Каждое выявленное несоответствие последовательно соотносится с j-метрикой и показателем K_{PRi} по определенному PR*i*-процессу ИБ. В результате выполняется пересчет весовых коэффициентов (частных) β для метрик PR*i*-процессов ИБ. Заполнение базы данных аудита новым показателем β.

Шаг 5. Выполняется формирование плана корректирующих действий по k-му аудиту. В результате выполняется пересчет PR*i*– целевого показатель результативности *i* –го процесса. Заполнение базы данных аудита новым показателем $K_{PR\,i.}$

Шаг 6. Выполняется оценка результативности коррекции и корректирующих действий по несоответствиям, выявленным по итогам k-го аудита. В результате выполняется заполнение базы данных аудита показателем R_{ISMS} (corr) для k-аудита и новыми значениями T_j , S_j , V_j , F_j , O_j.

Шаг 7. В случае, если $R_{ISMS\ (corr)} < R_{\ ISMS\ tar}$, т.е. для k-аудита не достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий, выполняется информирование руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности,

могут быть увеличены частота или объем программы аудита для тех PR_j-процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудитов в дальнейшем. Далее переход на шаг 5 к формированию плана корректирующих действий для k-го аудита и пересмотра групповых (α) и частных (β) коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 8. В случае если $R_{ISMS\ (corr)} \geq R_{\ ISMS\ tar}$, т.е. для k-го аудита достигается установленный показатель результативности корректирующих мер для всех выявленных несоответствий, выполняется реализация следующего по программе аудитов: (k+1)-го аудита с учетом новых измененных параметров по итогам успешной реализации корректирующих действий по предыдущему k-му аудиту. В результате формируется отчет по итогам k-го аудита.

Шаг 9. Выполняется анализ интегральных оценок для k и (k+1) аудитов соответственно: $R_{ISMS\ (corr)\ k}$, и $R_{ISMS\ (corr)\ k+1}$. В результате заполняется база данных аудита показателем R_{ISMS} (corr) k для k-го аудита и R_{ISMS} (corr) k+1 для (k+1)-го аудита.

Шаг 10. В случае если $R_{ISMS\ (corr)\ k+1} <= R_{ISMS\ (corr)\ k,}$ выполняется информирование руководителя программы аудита о возможном «устрожении» условий планирования аудита. В частности, могут быть увеличены частота или объем программы аудита для тех PR_j-процессов ИБ, по которым были выявлены несоответствия. Очевидно, это увеличит затраты на выполнение аудитов в дальнейшем. Далее переход на шаг 5 к формированию плана корректирующих действий для k-го аудита и пересмотра групповых (α) и частных (β) коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 11. В случае если $R_{ISMS\ (corr)\ k+1} > R_{ISMS\ (corr)\ k}$, выполняется информирование руководителя программы аудита о возможном возврате к базовым условиям планирования аудита. Далее переход на шаг 5 к формированию плана корректирующих действий для (k+1)-го аудита и пересмотра групповых (α) и частных (β) коэффициентов для каждого несоответствия. В результате формируется отчет по итогам k-го аудита.

Шаг 12. В случае повышения уровня результативности программы $R_{ISMS\ (corr)\ k+1} > R_{ISMS\ (corr)k}$ выполняется оценка программы аудита в целом, в том числе в экономическом аспекте (минимизация S-параметра). В результате формируется отчет по итогам k-го аудита.

7. Заключение. Предложенная методика оптимизации программы аудита ИСМ основана на современных риск-ориентированных стандартах и позволяет обеспечить постоянную

оптимизацию процесса выполнения проверок (аудитов) ИБ на основе гибких связанных адаптивных алгоритмов. Экспериментальная проверка предложенной методики проведена в период 2014–2016 гг. при выполнении проектов ООО «Газинформсервис» (имеется акт внедрения). Применение указанных конкретных блоков оптимизации в методике для иных ИСМ может, вероятно, потребовать иных параметров (например, при выборе в качестве критериев иных отраслевых стандартов или иного количества и состава векторного аргумента оптимизации).

Литература

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems // Requirements, International Organization for Standardization. 2013. 23 p.
2. ISO 55000:2014 Asset management – Overview, principles and terminology // International Organization for Standardization. 2014. 19 p.
3. ISO 55001:2014 Asset management – Management systems – Requirements // International Organization for Standardization. 2014. 14 p.
4. ISO 55002:2014 Asset management – Management systems – Guidelines for the application of ISO 55001 // International Organization for Standardization. 2014. 32 p.
5. PAS-99:2012 «Specification of common management system requirements as a framework for integration» // International Organization for Standardization. 2012. 36 p.
6. *Шишкин В.М., Юсупов Р.М.* Доктрина информационной безопасности Российской Федерации — опыт количественного моделирования // Труды СПИИРАН. 2002. Вып. 1. №. 1. С. 65–78.
7. *Юсупов Р. М., Шишкин В. М.* О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. 2008. Вып. 6. С. 39–59.
8. *Котенко И.В., Саенко И.Б., Юсупов Р.М.* Аналитический обзор докладов Международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010) // Труды СПИИРАН. 2010. Вып. 2. С. 226–248.
9. *Лившиц И.И., Полещук А.В.* Практическая оценка результативности СМИБ в соответствии с требованиями различных систем стандартизации: ИСО 27001 и СТО Газпром // Труды СПИИРАН. 2015. № 3. С. 33–44.
10. *Лившиц И.И.* Практические применимые методы оценки систем менеджмента информационной безопасности // Менеджмент качества. 2013. Вып. 1. С. 22–34.
11. *Лившиц И.И.* Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. 2014. Вып. 6. С. 72–94.
12. *Арзамазов М.А., Серов Г.П.* Консолидация общих требований стандартов к отдельным системам менеджмента и инновации при разработке интегрированных систем менеджмента // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. 2012. № 1. С. 52–55.
13. *Малышева Е.Ю., Бобровский С.М.* Архитектура информационной системы оценки интегрированных систем менеджмента // Вектор науки Тольяттинского государственного университета. 2012. № 1. С. 64–67.
14. *Ajam M., Alshawi M., Mezher T.* Augmented process model for e-tendering: toward integrating object models with document management systems // Automation in Construction. 2010. vol. 19. no. 6. pp. 762–778.

15. *Шеверда В.В.* Подходы к разработке интегрированных систем менеджмента на предприятиях электронной промышленности // Вопросы современной науки и практики. Университет им. В.И. Вернадского. 2012. № 3. С. 250–254.
16. *Mengersen K., Whittle P.J.L., et al.* Beyond compliance: Project on an Integrated system approach for PEST risl management in South East Asia // EPPO Bulletin. 2012. vol. 42. no. 1. pp. 109–116.
17. *Портянко Т.М.* Тенденции создания интегрированных систем менеджмента на предприятиях промышленного комплекса // Восточно-Европейский журнал передовых технологий. 2010. Т. 2. № 8 (44). С. 40–43.
18. ГОСТ Р ИСО 19011:2011. Руководящие указания по проведению аудитов систем менеджмента // Стандартинформ. 2013. 35 с.
19. *Griffith A.* Management systems for sustainable construction: Integrating Environmental, Quality and Safety management systems // International Journal of Environmental Technology & Management. 2002. vol. 2. no 1–3. pp. 114.
20. RAROC and risk management: Quantifying the risks of business // Bankers Trust New York Corporation. 1995.
21. *Smith G.E.* Auditing statistical methods for ISO 9001 // Transactions of 46th Annual Quality Congress. Milwaukee. WI. 1992. vol. 46. no. 0. QICID: 9905. pp. 849–54.
22. ГОСТ Р ИСО/МЭК 17021:2011. Оценка соответствия. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента // Стандартинформ. 2013. 37 с.
23. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems // Overview and vocabulary, International Organization for Standardization. 2014. 31 p.
24. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems // Measurement, International Organization for Standardization. 2009. 55 p.

Лившиц Илья Иосифович — к-т техн. наук, ведущий аналитик, ООО "Газинформсервис". Область научных интересов: системный анализ, защита информации, риск-менеджмент. Число научных публикаций — 50. Livshitz.il@yandex.ru; 198188, Санкт-Петербург, а/я 35; р.т.: +7(812) 677-20-50, Факс: +7(812) 677-20-51.

I.I. LIVSHITS

THE OPTIMIZATION METHOD OF THE INTEGRATED MANAGEMENT SYSTEM AUDIT PROGRAM

Livshits I.I. **A Method for Optimizing the Integrated Management System Audit Program.**

Abstract. The application of Integrated Management Systems (IMS) is now attracting the attention of senior management of a variety of organizations: refineries, instrument-making enterprises, aviation enterprises, defense organizations, etc. However, performing ISM audits as a verification of conformance to different ISO standards with a substantial reduction or limitation of available resources remains a major problem.

At the same time, continuous improvement of management principles and, in particular, transition to risk-based thinking provide a greater interest in the rational use of ISO standards. In this article we suggest a technique of optimization of IMS audit program based on principles of continuous adaptation when collecting data during a single audit micro-cycle. An additional advantage of the proposed technique is the use of numerical metrics of IT-security audit, contributing to continuous improvement of the level of IT security in organizations.

Keywords: Information security, Integrated Management System, standard, audit, IT security Management System.

Livshitz Ilya Iosifovich — Ph.D., lead analyst, LLC "Gasinformservice". Research interests: system analyses, IT-security, risk-management. The number of publications — 50. Livshitz.il@yandex.ru; 198188, Saint-Petersburg, a/ja 35; office phone: +7(812) 677-20-50, Fax: +7(812) 677-20-51.

References

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization. 2013. 23 p.
2. ISO 55000:2014 Asset management – Overview, principles and terminology. International Organization for Standardization. 2014. 19 p.
3. ISO 55001:2014 Asset management – Management systems – Requirements. International Organization for Standardization. 2014. 14 p.
4. ISO 55002:2014 Asset management – Management systems – Guidelines for the application of ISO 55001. International Organization for Standardization. 2014. 32 p.
5. PAS-99:2012 «Specification of common management system requirements as a framework for integration». International Organization for Standardization. 2012. 36 p.
6. Shishkin V., Yusupov R.M. ["The Doctrine of information security of Russian Federation" — an experience of quantitative modeling]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2002. vol. 1. no.1. pp. 65–78. (In Russ).
7. Yusupov R.M., Shishkin V. [About some contradictions in the decision of information security problems]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2008. vol. 6. pp. 39–59. (In Russ).
8. Kotenko I.V., Saenko I.B., Yusupov R.M. [Analytical review of the reports of the International Workshop «Scientific Analysis and Policy Support for Cyber Security» (SA&PS4CS 2010)]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2010, vol. 2(13). pp. 226–248. (In Russ).
9. Livshits I., Poleshuk A. [Practical Assessment of the ISMS Effectiveness in Accordance with the Requirements of the Various Standardization Systems both ISO 27001 and STO Gazprom.]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2015. vol. 3(40). pp. 33–44. (In Russ).

10. Livshitz I. [Practical purpose methods for ISMS evaluation]. *Menedzhment kachestva – Quality Management*. 2013. vol. 1. pp. 22–34. (In Russ).
11. Livshitz I. [Approaches to the application of the integrated management system model for carrying out audits for complex industrial facilities – airport complexes]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2014. vol. 6, pp. 72–94. (In Russ).
12. Arzamazov M.A., Serov G.P. [Consolidation of the general requirements of standards to individual management systems and innovation in the development of integrated management systems]. *Nauka I technologii truboprovodnogo transporta nefti I nefteproduktov – Science and Technologies oil and oil products pipeline transportation*. 2012. vol. 1. pp. 52–55. (In Russ).
13. Malysheva E.Y., Bobrovski' S.M. [The architecture of the information system of integrated management systems assessment]. *Vektor nauki Tol'atti Universitet – Vector Science Togliatti State University*. 2012. vol. 1. pp. 64–67. (In Russ).
14. Ajam M., Alshawi M., Mezher T. Augmented process model for e-tendering: toward integrating object models with document management systems. Automation in Construction. 2010. vol. 19. no 6. pp. 762–778.
15. Sheverda V.V. [Approaches to the development of integrated management systems for the electronics industry companies]. *Voprosy sovremennoy nauki i praktiki – Questions of modern science and practice*. 2012. vol. 3. pp. 250–254. (In Russ).
16. Mengersen K., Whittle P.J.L., et al. Beyond compliance: Project on an Integrated system approach for PEST risl management in South East Asia. EPPO Bulletin. 2012. vol. 42. no 1. pp. 109–116.
17. Portyanko T.M. [Trends in development of integrated management systems at the enterprises of the industrial complex]. *Vostochno-Evrope'ski' zhurnal peredovyh technologi'– Eastern European advanced technology magazine*. 2010. vol. 8 (44). pp. 40–43. (In Russ).
18. GOST 19011:2011. [Guidelines for auditing management systems]. Standartinform. 2013. 35 p. (In Russ).
19. Griffith A. Management systems for sustainable construction: Integrating Environmental, Quality and Safety management systems. International Journal of Environmental Technology & Management. 2002. vol. 2. no 1–3. pp. 114.
20. RAROC and risk management: Quantifying the risks of business. Bankers Trust New York Corporation. 1995.
21. Smith G.E. Auditing statistical methods for ISO 9001 // Transactions of 46th Annual Quality Congress. Milwaukee. WI. 1992. vol. 46. no. 0. QICID: 9905. pp. 849–54.
22. GOST R 17021:2011. [Conformity assessment -Requirements for bodies providing audit and certification of management systems]. Standartinform. 2013. 37 p. (In Russ).
23. ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary, International Organization for Standardization. 2014. 31 p.
24. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management systems. Measurement, International Organization for Standardization. 2009. 55 p.

УДК 004.056.55, 004.82 **DOI** 10.15622/sp.48.4

В.И. Воробьёв, Е.Л. Евневич, Д.К. Левоневский, Р.Р. Фаткиева, Л.Н. Федорченко

ИССЛЕДОВАНИЕ И ВЫБОР КРИПТОГРАФИЧЕСКИХ СТАНДАРТОВ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДОКУМЕНТОВ

Воробьёв В.И., Евневич Е.Л., Левоневский Д.К., Фаткиева Р.Р., Федорченко Л.Н. **Исследование и выбор криптографических стандартов на основе интеллектуального анализа документов.**

Аннотация. В данной статье исследуются проблемы применимости и выбора криптографических стандартов с учетом предпочтений и требований потенциального пользователя. Профили пользователя формируются с помощью онтологических методов. На основе профилей пользователей и характеристик документов формируется набор документов, которые могут подойти конкретному пользователю, и элементы этого набора ранжируются по вероятности соответствия его требованиям. При формировании набора документов используются различные методы фильтрации: коллаборативная фильтрация, анализ и фильтрация контента, а также гибридные методы, совмещающие оба подхода. Таким образом, создается рекомендующая система выбора криптографических стандартов и алгоритмов. При наличии нескольких пользовательских критериев выбора объекта целесообразно использовать интегральный показатель соответствия объекта, который вычисляется в виде взвешенной суммы показателей.

Ключевые слова: криптография, стандарты, рекомендующая система, алгоритмы коллаборативной фильтрации, гибридные методы, онтологии

1. Введение. Современная ситуация в области обеспечения безопасности информационных технологий (ИТ) характеризуется значительной лингвистической неоднородностью стандартов, регламентов, нормативных документов, политик и профилей безопасности, и как следствие, их слабой сбалансированностью и интегрируемостью [1, 2]. Причина прежде всего в том, что объекты защиты представляют собой сложные многоуровневые нелинейные системы с большим числом степеней свободы [3, 4].

Еще более острая проблема заключается в отображении требований каждого стандарта на общее множество требований информационной безопасности, так как некоторые из них повторяются от одного стандарта к другому или взаимно исключают друг друга. При этом встает вопрос о применимости стандартов и конкретных требований к организации в зависимости от формы собственности, сферы деятельности, использования тех или иных видов информации, наличия рисков и т.п. Так, согласно требованиям международного стандарта ISO/IEC 15408-1:2009 [5], требуется как формирование заданий по безопасности, так и построение профиля безопасности. При этом нередко возникают трудности при выборе средств обеспечения криптографической защиты ин-

формации. В частности, трудности могут возникнуть из-за ограничений, связанных с требованиями государственных стандартов при различных формах собственности защищаемого объекта. В связи с этим целесообразно построение *рекомендующей системы выбора криптографических решений*, позволяющей сформировать перечень угроз и произвести выбор на основе опроса пользователей.

2. Основные проблемы. Анализ текстов стандартов на основе онтологических моделей подтверждает их противоречивость и неполноту, что проявляется в несогласованности трактовок базовых концептов стандартов в криптографии, а также в неопределенности некоторых первичных понятий и в вытекающей отсюда неполноте или несогласованности отдельных положений и рекомендаций [1].

Представленные на рынке программные продукты (ПП), используемые для проверки соответствия политики информационной безопасности требованиям стандарта ISO 17799 – Cobra (C & A SystemsSecurityLtd,); CRAMM (CCTA Risk Analysis and Management Method); КОНДОР+ (DigitalSecurity); RiskWatch; ГРИФ 2006 (Digital Security Office); Авангард; Callio Secura(Callio Technologies); Ezrisk (Echelon Consulting); ISRAC (Infosecure Group); PTA (Practical Threat Analysis); RSAM (Relational Security); vsRisk™ (Vigilantsoftware) и др. имеют свои недостатки, например, отсутствие возможности установить весовой коэффициент каждого требования, необходимость специальной подготовки аудитора, высокая стоимость лицензии и ряд других [6, 7].

Высокая значимость обеспечения информационной безопасности, глобальный характер этой деятельности, неоднородность стандартов защиты информации обусловливают необходимость разработки средств, учитывающих особенности пользователей и организаций, сталкивающихся с потребностью в защите информации.

При выборе средств обеспечения информационной безопасности обычно принимаются во внимание следующие аспекты: аппаратная и программная платформа, на которой будет работать средство; сфера согласованности стандартов; масштабируемость; импортно-экспортные возможности; адаптируемость к структуре организации; модель лицензии; простота использования; цена.

Такая постановка задачи основана на анализе документов без учета особенностей пользователей стандартов. Эти особенности связаны с родом деятельности пользователей — физических и юридических лиц, их правовым статусом и ограничениями. Без учета пользовательского аспекта постановка задачи будет неконструктивной.

Требуется согласованная техническая политика для обеспечения определенности и однозначности понятийного аппарата и, в частности,

разработки средств формализации и соответствующей автоматизации этого процесса.

Поэтому предлагается подход на основе построения онтологической модели, описывающей отношения элементов как минимум двух множеств: субъектов (пользователей стандартов, агентов) и объектов (которые в конкретных случаях могут быть стандартами, материалами, документами, сервисами).

Подобный подход позволяет выполнить выбор того или иного документа и оценить механизмы принятия решения. Групповая оценка продукта (информационной системы) позволяет осуществить категорирование или построение рейтинговой шкалы, что облегчает работу пользователя при выборе сервиса. Фактически, пользователь осуществляет свой выбор с учетом информации, предоставленной рекомендующей системой, а эта информация, в свою очередь, зависит от требований конкретного пользователя. Рекомендующие системы также могут приводить аргументы в пользу рекомендуемых объектов, так как пользователи склонны более доверять обоснованным предложениям [8]. Рассмотрим постановку задачи более подробно.

3. Постановка задачи. Пусть существует m пользователей системы $X_1, X_2, \ldots, X_m$ и n документов $Y_1, Y_2, \ldots, Y_n$, созданы профили пользователей, документов и ограничения поиска. Необходимо для пользователя X_i сформировать множество документов, адекватных требованиям пользователя, и ранжировать их по степени релевантности [9].

В рекомендующих системах используются различные методы принятия решения — методы коллаборативной фильтрации [10, 11], гибридные методы, синтаксические методы обработки текстов.

Для сопоставления пользователей определяют метрику сходства. В коллаборативных алгоритмах используется информация о поведении субъекта в прошлом, например, об использовании конкретных ресурсов, взаимодействии с другими субъектами и об оценках рисков [12]. В этом случае не имеет значения тип объектов, но могут учитываться скрытые факторы, которые сложно было бы учесть при создании профиля. В данных методах профиль пользователя определяется множеством сервисов, которым был присвоен рейтинг этим пользователем.

Контекстно-зависимые рекомендующие системы [13] характеризуются также тем, что учитывают знания об интересах пользователя и контекст конкретной задачи выработки рекомендаций. Это выражается, в частности, в том, что такие системы учитывают атрибуты времени, места, социальный контекст, работают с группами пользователей, используют теги для уточнения свойств пользователей и сервисов.

Развитием этого подхода является гибридный метод, который использует как метрики сходства, так и статистические методы и позволяет добиться более точных и обоснованных предположений.

4. Гибридный метод фильтрации как основа рекомендующей системы. Подход базируется на преимуществах фильтрации контента и коллаборативной фильтрации.

В случае коллаборативной фильтрации предполагается, что похожим пользователям нравятся похожие образцы. При поступлении запроса от пользователя U_i вычисляются метрики сходства u_{ij} для всех $j \neq i$ и формируется множество из k пользователей, наиболее сходных с U_i. Далее формируется множество документов, подходящих этим пользователям, и из него исключаются документы, уже известные U_i. Здесь используется только профиль пользователя. Метрики сходства двух пользователей можно рассчитать, используя пересечения множеств понравившихся документов и интересов пользователей. При этом менее популярным документам можно присваивать более высокий весовой коэффициент. Для принятия решения используется симметричная матрица отношений «пользователь-пользователь»:

$$U = \begin{pmatrix} u_{11} \ldots u_{1m} \\ \ldots\ldots\ldots\ldots \\ u_{m1} \ldots u_{mm} \end{pmatrix}.$$

Фильтрация контента используется для оценки сходства документов. Этот подход предполагает, что если пользователю U_i нравится документ D_j, который похож на документ D_k, то пользователю U_i понравится и D_k. В этом случае, напротив, используется профиль документа. Метрики сходства двух документов d_{ij} можно рассчитать, используя пересечения множеств ключевых слов этих документов и пользователей, выставивших документам близкие оценки. Матрица отношений имеет вид:

$$D = \begin{pmatrix} d_{11} \ldots d_{1n} \\ \ldots\ldots\ldots\ldots \\ d_{n1} \ldots d_{nn} \end{pmatrix}.$$

Гибридный подход предполагает построение матрицы «пользователь-документ», содержащей оценки r_{ij}, данные пользователями с индексами $i = 1 \ldots m$ документам с индексами $j = 1 \ldots n$:

$$R = \begin{pmatrix} r_{11} \ldots r_{1n} \\ \ldots\ldots\ldots \\ r_{m1} \ldots r_{mn} \end{pmatrix}.$$

Если учитываются только непосредственные связи между пользователями и документами, матрица R будет очень разреженной, так как пользователь не имеет возможности оценить все или хотя бы значительную часть документов. Неопределенные элементы матрицы можно заполнить, рассчитав псевдорейтинг — величину, которая является предполагаемой оценкой пользователем U_i документа D_j с учетом похожести документов:

$$r_{ij} = \sum_{k=1}^{n} r_{ik} d_{ij},$$

где r_{ik} — известные значения матрицы «пользователь-документ», d_{ij} — метрики сходства документов D_i и D_j.

Сходство пользователей можно определить, используя корреляционную меру, основанную на скалярном произведении векторов:

$$w = \frac{\vec{v}_i \vec{v}_j}{|\, v_i \,||\, v_j \,|},$$

где w представляет собой косинус угла между векторами предпочтений v_i и v_j пользователей u_i и u_j и лежит в пределах от -1 до 1, где -1 соответствует полной противоположности (противонаправленность векторов), 1 — полному сходству (сонаправленность), 0 — отсутствию корреляции (ортогональность).

Предпочтения пользователя u_{ij} можно определить как:

$$u_{ij} = \frac{\sum_{k=1}^{n} (r_{ik} - \overline{r}_i)(r_{jk} - \overline{r}_j)}{\sqrt{\sum_{k=1}^{n} (r_{ik} - \overline{r}_i)^2 \sum_{k=1}^{n} (r_{jk} - \overline{r}_j)^2}},$$

где

$$\overline{r}_i = \frac{1}{n} \sum_{j=1}^{n} r_{ij}.$$

Здесь метрика сходства u_{ij} определяется как корреляция предпочтений пользователей U_i и U_j и является нормированным скалярным произведением векторов предпочтений U_i и U_j в n-мерном пространстве, где каждое измерение соответствует документу, а соответствующая координата вектора — отношению пользователя к этому документу.

Предположение об отношении пользователя U_i к документу D_j выражается величиной:

$$p_{ij} = r_i + \frac{\sum_{k=1}^{m}(r_{kj} - \overline{r}_k)u_{ik}}{\sum_{k=1}^{m}(r_{kj} - \overline{r}_k)}.$$

Для инициализации предполагается определение начальных значений всех элементов матрицы D и по возможности большего количества элементов матрицы R.

Сходство документов d_{ij} предлагается определять путем сопоставления профилей документов. Для этого документам присваиваются атрибуты A_i, определяемые исходя из метаданных, ключевых слов, содержания документа и статистической информации. Каждый атрибут имеет идентификатор (уникальное число или строка). В простейшем случае атрибут может иметь два значения: 1 (true, присвоен) и 0 (false, не присвоен, значение по умолчанию). Тогда наличие атрибута соответствует характеризующему документ утверждению, например:

– документ относится к предметной области пользователя X;

– в документе упоминается X;

– документ положительно/отрицательно оценен пользователем X.

Профиль документа можно определить как множество присвоенных ему атрибутов и их значений, а расстояние между профилями:

$$d(D_i, D_j) = \sum_{k=1}^{l} \alpha(A_k) d(A_k(D_i), A_k(D_j)),$$

где $\alpha(A_k)$ — весовой коэффициент атрибута.

На практике нет необходимости обрабатывать сильно отдаленные документы, поэтому расчет $d(D_i, D_j)$ целесообразно производить для ограниченного числа имеющих наибольший вес атрибутов с расчетом, чтобы выполнялось неравенство:

$$\sum_{k=1}^{l} \alpha(A_k) \le N,$$

где N — константа, ограничивающая точность оценки. В этом случае коэффициент сходства документов можно определить как:

$$d_{ij} = \frac{N}{d(D_i, D_j)}.$$

Применение методов фильтрации позволяет генерировать рекомендации на основании сходства пользователей и документов и с учетом интересов пользователей и их оценок. Следующим этапом развития системы является использование методов контекстного анализа в процессе выработки предложений.

5. Методы учета контекста. Большинство рекомендующих систем опираются на предложение наиболее релевантных образцов конкретным пользователям, при этом контекст, в котором находятся пользователи и сервисы, не принимается во внимание. Такой подход не является достаточным для поставленной задачи.

В рекомендующих системах первого поколения используется оценка функции рейтинга: $R : User \times Item \rightarrow Rating$.

Подобные системы называются также традиционными или двумерными [14], так как учитывают только два измерения — домены пользователей (User) и сервисов (Item). Учет контекста предполагает ввод дополнительных измерений в формулу рейтинга. Это означает, что оценка релевантности сервиса раскладывается по оценкам этого же сервиса в различных контекстах:

$$p_{ij} = \sum_{c=1}^{N_C} p_{ijc}.$$

Рассмотрим применение контекста к решаемой задаче. Пусть имеются отношения:

– *Пользователь* (ID, Имя, Расположение, Организация, Интересы, Профессия);

– *Документ* (ID, Название, Автор, Область, Тип, Время публикации).

Контекст может состоять из нескольких типов, каждый из которых определяет один аспект контекста — временное или пространственное расположение, социальную вовлеченность, цель использования. Для данной задачи можно ввести следующие *типы контекста:*

1. Время — интервал актуальности документа или этап жизненного цикла проекта.

2. Место — атрибут может включать следующие компоненты: *организация* (адрес); *район; населенный пункт*; *область; государство*.

3. Цель — принимает следующие значения*: образовательная; академическая; коммерческая; профессиональная*.

Контекст может иметь сложную и разнообразную структуру. К примеру, информация о пространственном расположении может пред-

ставляться в виде иерархии: *адрес → район → населенный пункт → область → государство.*

Временные атрибуты организуются в иерархии вида: *подэтап жизненного цикла → этап жизненного цикла → степень реализации* или *число → месяц → квартал → год.*

Применительно к построению структуры атрибутов контекста можно выделить два подхода:

– *предметный,* когда множество допустимых значений атрибута и отношений между ними предопределено и не испытывает значительных изменений во времени;

– *интерактивный,* когда предполагается двунаправленное взаимодействие между активностью пользователя и структурой атрибута: контекст влияет на рекомендации, а действия пользователя влияют на структуру контекста.

Для каждого типа контекстных данных определяется одно измерение C_i, каждое измерение характеризуется множеством допустимых значений, упорядоченных в k уровней. Меньшие значения уровня соответствуют меньшей точности и большей общности контекстной информации, а большие значения, близкие к k, определяют контекст наиболее конкретно. Тогда функция рейтинга имеет вид: $R: D_1 \times D_2 \times ... \times D_N \rightarrow Rating$. В этом случае рейтинг представляет собой целую или вещественную функцию, определенную на N-мерном пространстве дискретных значений. Два измерения соответствуют пользователям и сервисам, оставшиеся — типам контекста. Рисунок 1 иллюстрирует функцию рейтинга как гиперкуб.

В этом случае хранилище данных для значений рейтинга удобно организовать с помощью технологии OLAP (Online Analytical Processing) [15]. Рабочие данные представляются в структуре, называемой «OLAP-куб», и аналогичной рисунку 1. OLAP-куб содержит базовые данные и информацию об измерениях (агрегаты). Куб может содержать всю информацию, которая необходима для ответов на любые запросы. При большом количестве агрегатов полный расчет зачастую происходит только для отдельных измерений, для остальных расчет выполняется по требованию.

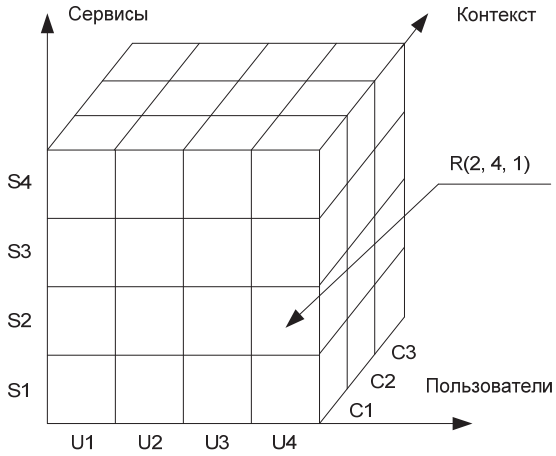


Рис. 1. Иллюстрация функции контекста

Для описания предметной области и формирования структуры контекста применяется инженерия онтологий [16, 17].

6. Инженерия онтологий. Определяется как совокупность процесса разработки онтологий; жизненного цикла онтологий; методов и методологий построения онтологий; набора инструментов и языков для построения и документирования онтологий, импорта и экспорта онтологий разных форматов и языков, поддержки графического редактирования, управления библиотеками онтологий и т.д.

Процесс онтологического моделирования можно разделить на выделение классов (концептов) и их свойств (отношений-слотов). Классы разрабатываемой онтологии описывают понятия предметной области. Каждый из них может иметь свой подкласс, который изображает более подробное описание, чем его надкласс. Задача слота — описать свойства класса и экземпляра. Свойства дают возможность, утверждать общие факты о членах классов. Свойство — это бинарное отношение. Различают два типа свойств:

1. Свойства-значения, отношения между представителями классов и типами данных.
2. Свойства-объекты, отношения между представителями двух классов.

При разработке профиля пользователя предлагается использовать анкетные данные и сведения о его активности. Анкетные данные — круг интересов пользователя, сведения о его образовании, навыках, профессиональной деятельности. Сведения об активности пользователя осно-

вываются на таких его действиях в информационной системе, как: просмотр документа, включая частоту доступа, полноту просмотра и время нахождения на странице; оценку документа; добавление документа в избранное; комментирование документа; создание документа.

Процедуру построения профиля пользователя можно разделить на три этапа:

Этап I. Сбор первоначальной информации о конкретном пользователе. На данном этапе осуществляется сбор информации, поступающей при заполнении анкеты пользователя. Это позволяет осуществить статистическую обработку атрибутов профилей пользователя, а также сформировать группы пользователей по интересам или другим атрибутам, входящим в профиль.

Этап II. Анализ запрашиваемой пользователем информации. Данные о запросах пользователя сохраняются для дальнейшего анализа. Это позволяет осуществить группировку часто встречающихся запросов, осуществить кластеризацию запросов, а также спрогнозировать вероятные запросы пользователя. Использование кластеризации данных позволяет осуществить категорирование пользователей, в том числе, разделение на «новичков в предметной области», специалистов и экспертов.

Такой подход, в свою очередь, позволяет осуществлять адресацию вопросов от новичков к экспертам, выполнять поиск необходимого пользователя, группировать пользователей по командам.

Этап III. Построение онтологии предметной области.

Для построения профиля пользователя была разработана анкета пользователя, а также выделены и описаны основные атрибуты, которые прослеживаются в поведении пользователей на инновационном портале. К базовым атрибутам, не зависящим от особенностей ресурсов информационной системы, относятся: длительность посещения ресурса; длительность посещения страницы; частота посещения ресурса; частота отправления запроса.

7. Синтаксический аспект онтологического моделирования. Переход от текстов стандарта к формализованному онтологическому описанию состоит в определении онтологической тройки:

– множество концепций (терминов);

– множество отношений между концепциями;

– правила логического вывода в сети концепций и отношений (например, правило транзитивности, симметричности, антисимметричности, рефлексивности).

При онтологическом моделировании не обойтись без инструментальной поддержки, обеспечивающей пользователей и лиц, принимающих решения, средствами работы с данными и системами

компьютерной поддержки доказательства утверждений, позволяющими создавать унифицированные программы проверки свойств и проверки доказательств того, что программа соответствует своей спецификации.

В качестве перспективной формальной базы для использования таких систем в СПИИРАН разрабатывается подход, основанный на использовании грамматик и синтаксических методов для представления схем логических выводов и вычислительных схем.

Современные системы компьютерной поддержки доказательства утверждений используют расширяемые системы правил, состоящие из двух частей. Одна часть содержит некоторое постоянное логическое ядро, другая — состоит из правил, задаваемых пользователем. Поскольку набор и состав этих правил может изменяться, необходимы программные средства, позволяющие быстро настраиваться на вводимые изменения и дополнения в схемы правил.

Процесс логического вывода удается разбить на два этапа, при этом первый этап (вывод схем правил и схем выводов) приводит к регулярным выражениям, что допускает эффективное использование специального инструментального средства, упрощающего схемы правил и схемы выводов (например, удаление тупиковых и циклических выводов). Второй этап требует использования грамматик, содержащих контекстно-зависимые правила с атрибутами в виде семантик и предикатов, которые также могут быть проанализированы инструментальной системой. При реализации прототипа системы с атрибутами на платформе .NET в качестве основы взят код инструментального комплекса SynGT, разработанного в СПИИРАН [21].

8. Методика выбора алгоритмов. В условиях многокритериального выбора целесообразно применить метод свертки взвешенных показателей (взвешенного среднего арифметического). Применение этого метода для сравнения криптографических решений предложено в работе [18]. Преимущество этого метода в том, что более высокие оценки получают те решения, которые имеют больше критериев с максимальной степенью соответствия. В качестве критериев рассмотрены безопасность, скорость и стоимость, весовые коэффициенты полагаются одинаковыми и равными 1/3.

Затем применяется метод взвешенной метрики. Вычисляется отклонение (дисперсия) решений по отношению к идеальному.

В отличие от данного подхода, в [19, 20] показано, что при выборе функции распределения, описывающей сложные критические объекты, применяется степенная функция распределения. Предлагается следующий способ моделирования неопределенности задания нормирующей функции:

$$F(z,t)=\begin{cases}0, z \le z_{-}\\ \left(\dfrac{z-z_{-}}{z_{+}-z_{-}}\right)^{t}, z_{-} < z \le z_{+}\\ 1, z_{+} < z\end{cases}.$$

В результате появляется возможность построения вектора показателей качества объекта в виде $q=(q_1,...,q_n)$, i=1, …, l для вектора исходных характеристик $x = (x_1, …, x_n)$. Например, для оценки качества применяется набор показателей q в зависимости от характеристик x. После получения набора отдельных показателей выбирается синтезирующая функция $Q(q)=Q(q;w)$, где $w = (w_1, …, w_l)$, $w_1+…+w_l=1$, интерпретируются как весовые коэффициенты, задающие степень влияния отдельных показателей на сводную оценку — в нашем примере усредненное значение показателя качества документа.

При практическом использовании сводных показателей зачастую имеет место дефицит информации, выражающийся в том, что имеется неопределенность выбора функций q, Q и вектора w. Данная неопределенность усугубляется еще тем, что доступная информация не имеет числового характера, то есть квалиметрическая шкала имеет более бедную структуру, чем обычная числовая шкала. Например, показатели качества объекта защиты в зависимости от его месторасположения. В этом случае задача оцифровки состоит в выборе отображения $\varphi(b)$, где b — качественная характеристика (например, баллы).

9. Реализация рекомендующей системы. Рекомендующая система строится на основе информационной системы, оперирующей объектами как самодостаточными сущностями. Классы, определяющие объекты, упорядочены в иерархическую структуру (рисунок 2).

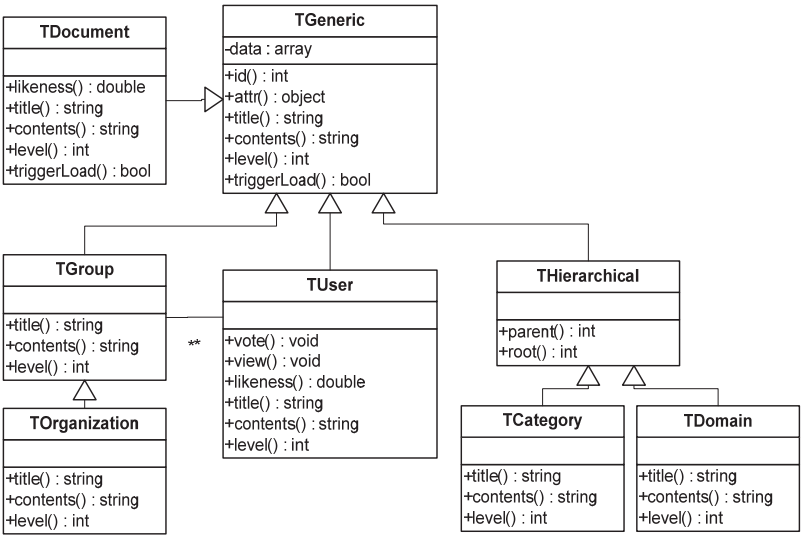


Рис. 2. Фрагмент иерархии классов

Все классы прямо или опосредованно наследуют базовому типу TGeneric. Благодаря этому к основным, не зависящим от спыецифики типа свойствам можно обращаться через унифицированный интерфейс.

Иерархия включает следующие типы, но не ограничивается ими:

– TGeneric — базовый абстрактный класс;

– TUser — пользователь;

– TGroup — группа пользователей;

– TOrganization — организация;

– TDocument — документ;

– THierarchical — абстрактный класс для создания объектов, упорядоченных иерархически;

– TCategory — тип документа;

– TDomain — предметная область документа.

К основным операциям с объектами относятся:

– id — получение идентификатора объекта (числа, уникального в пределах типа);

– attr — получение и установка атрибутов;

– title — получение названия объекта;

– contents – получение HTML-представления объекта;

– level — уровень привилегий, необходимый для доступа к объекту.

Материалы организованы в динамической иерархической структуре (рисунок 3). Они включают:

– публикации пользователей;
– сведения об общественной деятельности;
– служебные и справочные материалы.

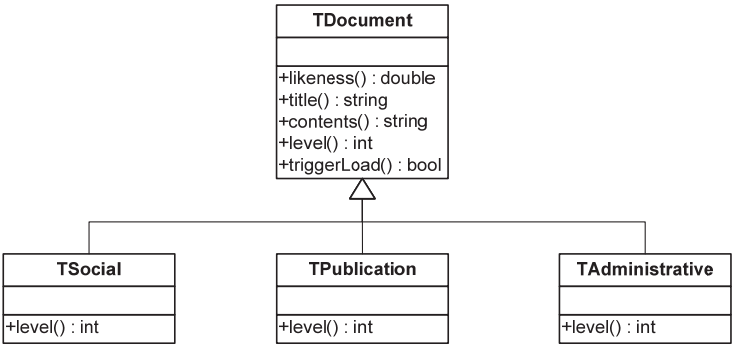


Рис. 3. Организация материалов

Зарегистрированный пользователь системы имеет логин и пароль, которые он сообщает системе в процессе регистрации. Эти данные используются в дальнейшем при входе в систему и удостоверяют его права на доступ к информации и публикацию материалов. Неавторизованные пользователи называются гостями и имеют ограниченный доступ. Пользователям присваивается уровень доступа, который может определять их полномочия в широких пределах.

10. Заключение. Выработка рекомендаций к применению того или иного криптографического стандарта или ресурса информационной системы с учетом индивидуальных особенностей каждого пользователя требует использования статистических методов оценки деятельности пользователя в этой системе, методов обработки неструктурированных данных и контекстного анализа. На этих методах основывается предложенный подход к построению групповой контекстно-зависимой рекомендующей системы. Подход позволяет учитывать функциональные и правовые ограничения субъектов, использующих нормативные документы в области информационной безопасности.

В качестве основного направления будущих исследований предлагается разработка Web-ресурса для гармонизации стандартов и регламентирующих документов на основе их онтологического описания, которое включает построение таксономий терминов предметной области, предикативных отношения между терминами, логический вывод на основе дескриптивной логики, а также средства интеграции онтологий и рекомендующих систем для учета требований пользовfte-

ля. Процессом достижения цели будет построение терминологических таксономий, предикативных отношений, дескриптивных ограничений (ontological restrictions) для вывода новых типов данных и расширение множества правил вывода. Уточнение терминологии и отношений может происходить непосредственно в процессе разработки онтологий (серии онтологий). Все методики предполагается применять для проверки корректности использования криптостандартов в области облачных вычислений.

Литература

1. *Atiskov A.Yu., Vorobev V.I., Fedorchenko L.N. et al.* Theory and Practice of Cryptography Solutions for Secure Information Systems // IGI Global. 2012. pp.101–130.
2. *Sennewald C., Baillie C.* International Security Standards // Effective Security Management (Sixth Edition). 2016. pp. 205–212.
3. *Воробьев В.И., Фаткиева Р.Р.* Природа уязвимостей программного кода // Программируемые инфокоммуникационные технологии. Сборник статей. М.: Радиотехника. 2009. С. 53–55.
4. *Баранов С.Н., Шишкин В.М.* Современные тенденции индустрии разработки программных продуктов // Информационно-измерительные и управляющие системы. 2012. Т. 10. № 5. С. 24–33.
5. ISO/IEC 15408-1:2009: Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. 2009.
6. Официальный сайт компании «Аудит информационной безопасности». URL: http://www.audit-ib.ru/ (дата обращения: 10.04.2016).
7. IT Governance Green Paper INFORMATION SECURITY & ISO 27001. URL: http://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf (дата обращения: 13.05.2016).
8. Перспективные направления развития науки в Петербурге / Отв. ред. Ж.И. Алферов, О.В. Белый, Г.В. Двас, Е.А. Иванова // СПб.: Из-во ИП Пермяков С.А. 2015. 543 с.
9. *Городецкий В.И., Тушканова О.Н.* Онтологии и персонификация профиля пользователя в рекомендующих системах третьего поколения // Онтологии проектирования. 2014. № 3 (13). С. 7–31.
10. *Wang J., Pouwelse J.* Distributed Collaborative Filtering for Peer-to-Peer File Sharing Systems // Proceedings of the 2006 ACM symposium on Applied computing. pp. 1026–1030.
11. *Melville P., Mooney R.J., Nagarajan R.* Content-Boosted Collaborative Filtering for Improved Recommendations // Proceedings of 18th National ACM Conference of Artificial Intelligence. 2002. pp. 187–192.
12. *Королёва Д.Е., Филиппов М.В.* Анализ алгоритмов обучения коллаборативных рекомендательных систем // Инженерный журнал: наука и инновации. 2013. Вып. 6. URL: http://engjournal.ru/catalog/it/hidden/816.html (дата обращения: 29.02.2016).
13. *Adomavicius G., Mobasher B., Ricci F., Tuzhilin A.* Context-Aware Recommender Systems // AI Magazine. 2011. pp. 67–80.
14. *Wang J., de Vries A. P., Reinders M.J.T.* Unifying user-based and item-based collaborative filtering approaches by similarity fusion // Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval. ACM New York. NY. USA. 2006. pp. 501–508.
15. *Cios K.J. et al.* Data Mining: A Knowledge Discovery Approach // Springer. 2007. 606 p.
16. *Gonzalez-Perez C. et al.* An Ontology for ISO software engineering standards: 2) Proof of concept and application // Computer Standards & Interfaces. 2016. vol. 48. pp. 112–123.
17. *Van Ruijven L.C.* Ontology for Systems Engineering // Procedia Computer Science. 2013. vol. 16. pp. 383–392.

18. *Raissi J.* Dynamic Selection of Optimal Cryptographic Algorithms in a Runtime Environment // Proceedings of IEEE International Conference on Evolutionary Computation. 2006. pp. 184–191.
19. *Хованов Н.В.* Оценка сложных объектов в условиях дефицита информации. К столетию метода сводных показателей А.Н. Крылова // Моделирование и анализ безопасности и риска в сложных системах: Сб. научн. трудов 8-й международной научной школы. СПб.: ИПМАШ РАН. 2008. С. 18–28.
20. *Yudaeva M., Hovanov N., Kolesov D.* Double randomized estimation of Russian "Blue Chips" based on imprecise information // Advances in Intelligent Systems and Computing. Springer International Publishing Switzerland. 2014. vol. 299. pp. 155–164.
21. *Fedorchenko L., Baranov S.* Equivalent Transformations and Regularization in Context–Free Grammars / Bulgarian Academy of Sciences // Cybernetics and Information Technologies (CIT). Sofia. 2014. vol. 14. no 4. pp. 29–44.

Воробьев Владимир Иванович — д-р техн. наук, профессор, главный научный сотрудник лаборатории информационно-вычислительных систем и технологий программирования, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: информационная безопасность, облачные и параллельные вычисления. Число научных публикаций — 110. vvi@iias.spb.su; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7(812)3284369, Факс: +7(812)3284450.

Евневич Елена Людвиговна — к-т физ.-мат. наук, старший научный сотрудник лаборатории информационно-вычислительных систем и технологий программирования, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: распределенные и облачные вычисления, когнитивные технологии, информационная безопасность. Число научных публикаций — 50. eva@iias.spb.su; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: 8(812)3284369, Факс: 8(812)3284450.

Левоневский Дмитрий Константинович — научный сотрудник лаборатории информационно-вычислительных систем и технологии программирования, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: информационная безопасность, защита информации, компьютерные сети, моделирование компьютерных процессов, технологии программирования. Число научных публикаций — 15. dl@iias.spb.su; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7-812-328-43-69, Факс: +7 (812)350-1113.

Фаткиева Роза Равильевна — к-т техн. наук, доцент, старший научный сотрудник лаборатории информационно-вычислительных систем и технологии программирования, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: моделирование информационных систем. Число научных публикаций — 35. rrf@iias.spb.su; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7-812-328-43-69, Факс: +7 (812)350-1113.

Федорченко Людмила Николаевна — к-т техн. наук, старший научный сотрудник лаборатории прикладной информатики и проблем информатизации общества, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: теория формальных языков и трансляций, регуляризация грамматик, технология разработки трансляторов. Число научных публикаций — 70. lnf@iias.spb.su; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7(812)3281919, Факс: +7(812)3284450.

V.I. VOROBIEV, E.L. EVNEVICH, D.K. LEVONEVSKIY, R.R. FATKIEVA, L.N. FEDORCHENKO

A STUDY AND SELECTION OF CRYPTOGRAPHIC STANDARDS ON THE BASIS OF TEXT MINING

Vorobiev V.I., Evnevich E.L., Levonevskiy D.K., Fatkieva R.R., Fedorchenko L.N. **A Study and Selection of Cryptographic Standards on the basis of Text Mining.**

Abstract. This paper discusses the problems of application and choice of cryptographic standards taking into account user requirements and preferences. User profiles are created by means of the ontology apparatus. On the basis of user profiles and document features an appropriate set of documents is formed, the elements of which are then arranged according to the degree of compliance to user requirements. Various filtration methods, such as collaborative filtering, content analysis and filtering, as well as hybrid methods combining both approaches, are used. Thus, a recommender system for choosing cryptographic standards and algorithms is built. If there are several user selection criteria, it is reasonable to apply an integral index of object's relevance to user preferences. This index is defined as the weighed sum of the particular indices.

Keywords: cryptography, standards, recommender system, collaborative filtration algorithms, hybrid methods, ontologies

Vorobiev Vladimir Ivanovich — Ph.D., Dr. Sci., professor, chief researcher of computing & information systems and programming technologies laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: information security, distributed and cloud computations. The number of publications — 110. vvi@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)3284369, Fax: +7(812)3284450.

Evnevich Elena Lyudvigovna — Ph.D., senior researcher of computing & information systems and programming technologies laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: distributed and cloud computations, network security, cognitive technologies. The number of publications — 50. eva@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: 8(812)3284369, Fax: 8(812)3284450.

Levonevskiy Dmitriy Konstantinovich — researcher of computing & information systems and programming technologies laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: information security, computer security, computer networks, modeling of information processes, programming technology. The number of publications — 15. dl@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-812-328-43-69, Fax: +7 (812)350-1113.

Fatkieva Roza Ravilievna — Ph.D., associate professor, senior researcher of computing & information systems and programming technologies laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: modeling of information systems. The number of publications — 35. rrf@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-812-328-43-69, Fax: +7(812)3501113.

Fedorchenko Ludmila Nickolayevna — Ph.D., senior researcher of applied informatics and society informatization problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: theory of formal lan-

guages and translations, regularization of grammars, development of compilers. The number of publications — 70. lnf@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)3281919, Fax: +7(812)3284450.

References

1. Atiskov A.Yu., Vorobev V.I., Fedorchenko L.N. et al. Theory and Practice of Cryptography Solutions for Secure Information Systems. IGI Global. 2012. pp.101–130.
2. Sennewald C., Baillie C. International Security Standards. Effective Security Management (Sixth Edition). 2016. pp. 205–212.
3. Vorobiev V.I., Fatkieva R.R. [Nature of program code vulnerabilities]. *Programmiruemye infokommunikacionnye tehnologii. Sbornik statej* [Programmed information and communication technologies. Collected papers]. M.: Radiotehnika, 2009. pp. 53–55. (In Russ.).
4. Baranov S.N., Shishkin V.M. [The Actual Trends of the Software Industry]. *Informatsionno-izmeritelnye i upravlyayushchie sistemy – Measurement and control systems*. 2012. vol. 10. no. 5. pp. 24–33. (In Russ.).
5. ISO/IEC 15408-1:2009: Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model. 2009.
6. Oficial'nyj sajt kompanii Audit informatsionnoy bezopasnosti [Official web site of the Information security audit company]. Available at: http://www.audit-ib.ru/ (accessed 10.04.2016). (In Russ.).
7. IT Governance Green Paper INFORMATION SECURITY & ISO 27001. Available at: http://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf (accessed 13.05.2016).
8. *Perspektivnyie napravleniya razvitiya nauki v Peterburge. Otv. red. Zh.I. Alferov, O.V. Belyj, G.V. Dvas, E.A. Ivanova* [Actual trends of science development in St. Petersburg. Edited by Zh.I. Alferov, O.V. Belyiy, G.V. Dvas, E.A. Ivanova]. SPb.: Iz-vo IP Permyakov S.A. 2015. 543 p. (In Russ.).
9. Gorodetsky V.I., Tushkanova O.N. [Ontology-based user profile personification in 3g recommender systems]. *Ontologiya proektirovaniya – Ontology of design*. 2014. vol. 3(13). pp. 7–31. (In Russ.).
10. Wang J., Pouwelse J. Distributed Collaborative Filtering for Peer-to-Peer File Sharing Systems. Proceedings of the 2006 ACM symposium on Applied computing. pp. 1026–1030.
11. Melville P., Mooney R.J., Nagarajan R. Content-Boosted Collaborative Filtering for Improved Recommendations. Proceedings of 18th National ACM Conference of Artificial Intelligence. 2002. pp. 187–192.
12. Korolyova D.E., Filippov M.V. [Analysis of collaborative recommender system learning algorithms] *Inzhenerny zhurnal: nauka i innovatsii – Engineering journal: science and innovation*. 2013. vol. 6. Available at: http://engjournal.ru/catalog/it/hidden/816.html (дата обращения: 29.02.2016). (In Russ.).
13. Adomavicius G., Mobasher B., Ricci F., Tuzhilin A. Context-Aware Recommender Systems. *AI Magazine*. 2011. pp. 67–80.
14. Wang J., de Vries A. P., Reinders M.J.T. Unifying user-based and item-based collaborative filtering approaches by similarity fusion. Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval. ACM New York. NY. USA. 2006. pp. 501–508.
15. Cios K.J. et al. Data Mining: A Knowledge Discovery Approach. Springer. 2007. 606 p.
16. Gonzalez-Perez C. et al. An Ontology for ISO software engineering standards: 2) Proof of concept and application. *Computer Standards & Interfaces*. 2016. vol. 48. pp. 112–123.

17. Van Ruijven L.C. Ontology for Systems Engineering. Procedia Computer Science. 2013. vol. 16. pp. 383–392.
18. Raissi J. Dynamic Selection of Optimal Cryptographic Algorithms in a Runtime Environment. Proceedings of IEEE International Conference on Evolutionary Computation. 2006. pp. 184–191.
19. Hovanov N.V. [Complex objects estimation in conditions of lack of information] *Trudyi 8-y mezhdunarodnoy nauchnoy shkolyi «Modelirovanie i analiz bezopasnosti i riska v slozhnyih sistemah»* [Proceedings of the 8th international scientific school "Modeling and analysis of security and risks in complex systems"]. SPb.: IPMASh-HRAN, 2008. pp. 18–28. (In Russ.).
20. Yudaeva M., Hovanov N., Kolesov D. Double randomized estimation of Russian "Blue Chips" based on imprecise information. Advances in Intelligent Systems and Computing. Springer International Publishing Switzerland. 2014. vol. 299. pp. 155–164.
21. Fedorchenko L., Baranov S. Equivalent Transformations and Regularization in Context–Free Grammars. Bulgarian Academy of Sciences. Cybernetics and Information Technologies (CIT). Sofia. 2014. vol. 14. no 4. pp. 29–44.

УДК 004.056 **DOI** 10.15622/sp.48.5

И.В. Гаврилов

АЛГОРИТМ ОЦЕНИВАНИЯ СЛОВЕСНОЙ РАЗБОРЧИВОСТИ РЕЧИ НА ОСНОВЕ ФУНКЦИИ КОГЕРЕНТНОСТИ

Гаврилов И.В. **Алгоритм оценивания словесной разборчивости речи на основе функции когерентности.**

Аннотация. Задача оценивания защищенности речевой информации конфиденциального характера в настоящее время крайне актуальна. Но в условиях применения средств акустической защиты, то есть в условиях сильных шумов, существующие инструментально-расчетные методы дают большую погрешность при сравнении с крайне трудозатратными артикуляционными методами.

В работе исследован метод оценки показателя защищенности речевой информации на основе корреляционного коэффициента Пирсона, но данный коэффициент обладает плохой чувствительностью к спектральным свойствам акустических сигналов. Поэтому автором предложен подход к определению показателя защищенности речевой информации на основе математического аппарата функции когерентности исходного и зашумленного сигнала.

В статье предлагается весь речевой частотный диапазон функции когерентности разбить на отдельные октавы. Посчитать математическое ожидание составляющих функции когерентности в октавах и на основе функции свертки получить выражение для расчета показателя защищенности речи.

Предложенный алгоритм к определению показателя защищенности речевой информации позволяет повысить точность проводимой оценки.

Ключевые слова: маскирующий шум, словесная разборчивость речи, коэффициент корреляции, частотный спектр сигнала, средства активной защиты, функция когерентности

1. Введение. Основным способом коммуникации между людьми является речь. Этот факт подтверждают исследовательские работы в области изучения специфики речевого воздействия и взаимодействия [1].

Во многих случаях при организации речевых коммуникаций необходимо уделять особое внимание их защите от перехвата. Поэтому часто возникает необходимость в построении систем защиты [2, 3] и в последующей оценке защищенности речевой информации [4, 5].

Актуальность оценки защищенности различных помещений от утечки речевой информации подтверждается большим количеством публикуемых материалов на данную тему [3, 4, 5, 6].

Например, совершенствованию способов определения показателя защищенности речевой информации посвящена статья [4], в которой предлагается использовать в качестве измерителя линейный частотно-модулированный сигнал. Структурно-пространственная модель канала утечки речевой информации легла в основу методики оценки технической защищенности речевой информации в помещениях, представленной в [5]. Эффективность защиты речевой информации на основе

ставшего уже классическим расчета интегрального индекса артикуляции по «октавным» индексам артикуляции предложено оценивать в работе [6]. В работе [7] представлен подход к определению защищенности речи в случае перехвата лазерными микрофонами, а также показана взаимосвязь подходов к определению параметров каналов утечки информации (показателей защищенности) и каналов передачи.

Однако описанные к настоящему времени в литературе объективные способы оценки защищенности речевой информации не позволяют достоверно оценивать речевую разборчивость в условиях использования средств активной защиты (условия сильных шумов). Поэтому задачей настоящего исследования является разработка алгоритма оценивания словесной разборчивости речи, который позволит повысить достоверность определения показателя защищенности при использовании средств защиты.

2. Способы определения показателей защищенности речевой информации. В качестве показателей защищенности речевой информации при использовании средств защиты применяются оценочные характеристики маскирующих шумов и характеристики «искаженной» маскирующими шумами речи. Оценке маскирующего шума путем уточнения энтропийного коэффициента была посвящена следующая работа [8]. Данный способ оценки целесообразно проводить на этапе проектирования систем защиты. При оценке готовых решений по защите речевой информации в качестве показателя защищенности принято использовать разборчивость речи (словесную, слоговую, формантную), которая определяет степень понятности смысла и содержания передаваемой информации [9, 10].

Разборчивость может быть рассчитана объективными и субъективными методами [11]. Для объективных методов оценочный показатель является зависимым от измерительного тракта. В случае субъективных методов показатель разборчивости речи не зависит от измерительного тракта.

В настоящей работе в условиях действия маскирующих шумов разного уровня в диапазоне от минус 20 дБ до минус 5 дБ для проведения моделирования и оценки эффективности предлагаемого решения используется метод артикуляции, описанный в [12], где за счет известного аудиторам словаря достигается снижение дисперсии оценки рассчитываемого показателя разборчивости. В соответствии с артикуляционным методом формируется артикуляционная группа из трех человек с нормальным слухом. Двумя дикторами (мужчина и женщина) начитываются и записываются в виде аудиофайлов артикуляционные таблицы слов, на которые накладывается шум в пакете

прикладных программ Matlab. Группа аудиторов проходит тренировочные испытания до тех пор, пока в одинаковых условиях испытаний не дает устойчивые повторимые результаты по оценке словесной разборчивости речи (рисунок 1).

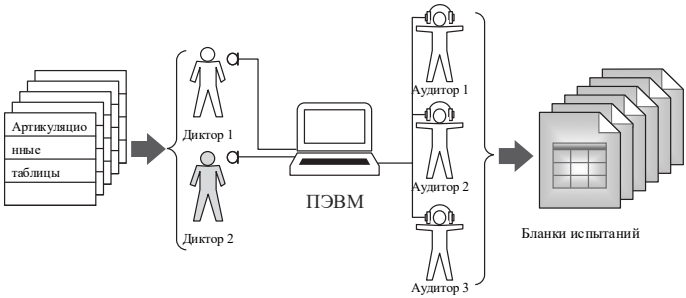


Рис. 1. Схема проведения артикуляционных испытаний

Далее приводится подробное описание исходных данных для проведения артикуляционных испытаний, результаты которых представлены на рисунке 16.

3. Описание исходных данных для моделирования. Для моделирования процессов зашумления используется тестовая запись речи диктора длительностью 5 с, оцифрованная с частотой дискретизации 22 050 Гц.

При моделировании процессов зашумления в системе Matlab используется аддитивная модель канала:

$$s'(t) = \gamma \cdot s(t - \tau) + n(t), \qquad (1)$$

где *s(t)* — исходный речевой сигнал;

s'(t) — зашумленный речевой сигнал;

γ — постоянный коэффициент передачи канала;

τ — задержка в канале;

n(t) — шум.

В настоящей работе для моделирования приняты следующие условия: отсутствие задержки в канале и стремление постоянного коэффициента к единице.

В качестве шумовой составляющей взяты реализации шумов, описание которых приведено в таблице 1, и далее по тексту на рисунках 2-9 темным цветом.

Таблица 1. Характеристики шумов, использованных в работе

Название шума	Краткое описание вида шума
«Белый» шум	Спектральные составляющие шума равномерно распределены по всему задействованному диапазону частот
«Розовый» шум	Спектральная плотность шума затухает на 3 дБ на каждую октаву
«Красный» шум	Спектральная плотность шума затухает на 6 дБ на каждую октаву
«Серый» шум	Субъективно воспринимаемый на слух как равномерный, но имеющий провал на средних частотах

Отношение минус 20 дБ рассматривается как примерная критическая точка, ниже которой словесная разборчивость речи в случае зашумления «белым шумом» стремится к нулю [6, 9, 10].

Для «белого» шума временная реализация и спектр тестового речевого сигнала на фоне шума представлены на рисунках 2 и 3.

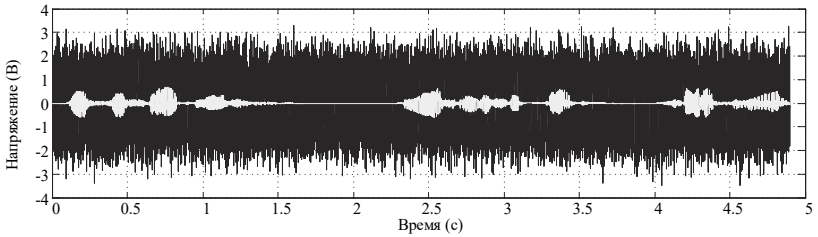


Рис. 2. Временная реализация тестового сигнала на фоне реализации «белого» шума (С/Ш — минус 20дБ)

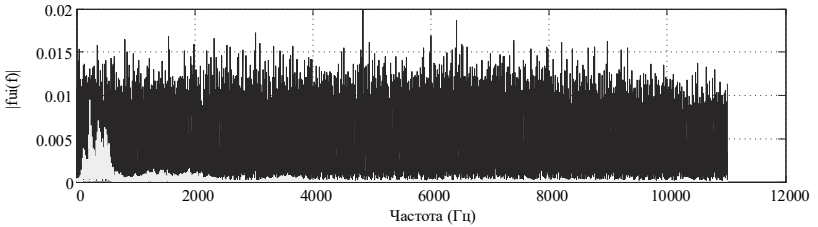


Рис. 3. Амплитудный спектр тестового сигнала на фоне амплитудного спектра «белого» шума (С/Ш — минус 20дБ)

Для подкрашенных шумов представлены следующие пары рисунков. Временная и частотная реализации тестового фрагмента речи на фоне «розового» шума отображены на рисунках 4 и 5.

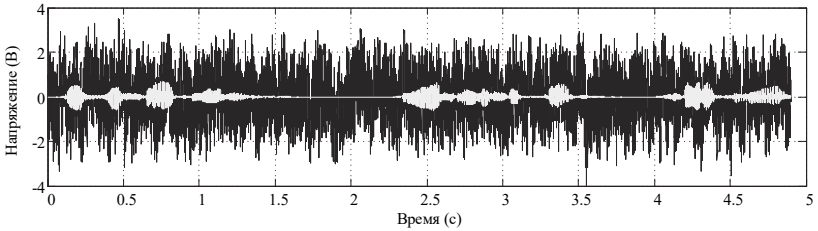


Рис. 4. Временная реализация тестового сигнала на фоне реализации «розового» шума (С/Ш — минус 20дБ)

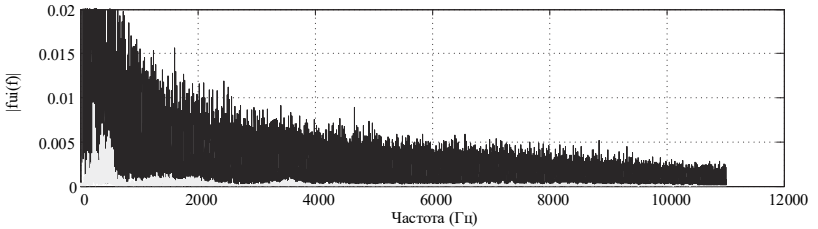


Рис. 5. Амплитудный спектр тестового сигнала на фоне амплитудного спектра «розового» шума (С/Ш — минус 20дБ)

Тестовый речевой сигнал с «красным» шумом в виде временных отсчетов и спектральных составляющих показан на рисунках 6 и 7.

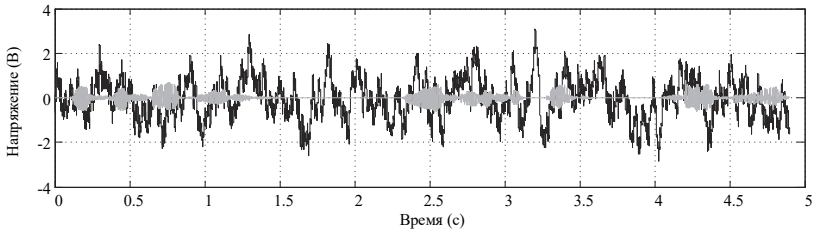


Рис. 6. Временная реализация тестового сигнала на фоне реализации «красного» шума (С/Ш — минус 20дБ)

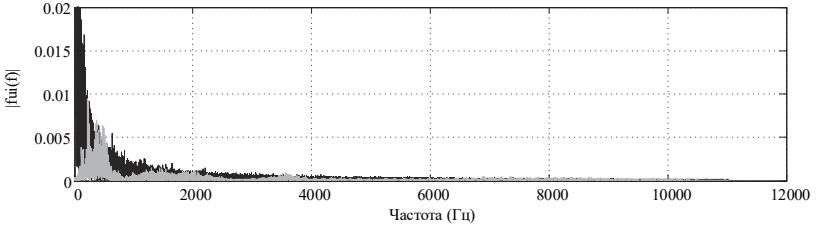


Рис. 7. Амплитудный спектр тестового сигнала на фоне амплитудного спектра «красного» шума (С/Ш — минус 20дБ)

На рисунках 8 и 9 содержатся временная реализация и амплитудный спектр тестового сигнала и «серого» шума при указанном ранее соотношении «сигнал-шум» минус 20 дБ.

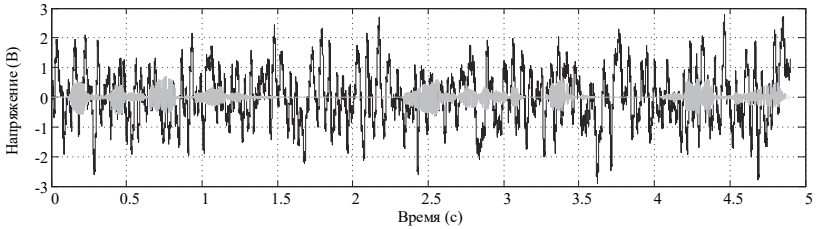


Рис. 8. Временная реализация тестового сигнала на фоне реализации «серого» шума (С/Ш — минус 20дБ)

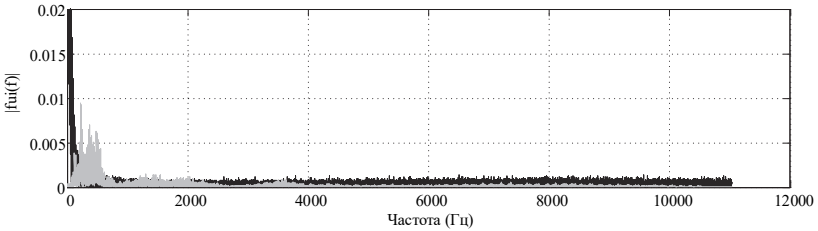


Рис. 9. Амплитудный спектр тестового сигнала на фоне амплитудного спектра «серого» шума (С/Ш — минус 20дБ)

По частотному спектру представленных сигналов прослеживаются маскирующие свойства рассматриваемых шумов. Так «белый» и «розовый» шумы наиболее полно перекрывают спектр речевого сигнала, более того, «розовый» шум должен давать лучший маскирующий эффект при снижении соотношения «сигнал-шум».

В следующих пунктах статьи описываются подходы к определению показателей защищенности речевой информации в условиях действия на речевой сигнал рассмотренных шумов: подход на основе коэффициента корреляции и подход на основе математического аппарата функции когерентности.

4. Применение коэффициента корреляции Пирсона в задачах определения показателя защищенности речевой информации. В ряде работ, посвященных оценке эффективности маскировки речи [7, 13, 14] исследуется возможность применения корреляционных методов для оценки показателя защищенности.

Для расчета коэффициента корреляции между дискретизированными исходным речевым сигналом *s(t)* и сигналом *s'(t)*, зашумлен-

ным акустическим шумом, необходимо пользоваться следующим выражением [15]:

$$r_{ss'} = \frac{M\{[s - M(s)]\cdot[s' - M(s')]\}}{\sqrt{D(s)}\cdot\sqrt{D(s')}}, \qquad (2)$$

где *M(...)* — математическое ожидание; *D(...)* — дисперсия.

При смешивании речевого тестового сигнала с «белым» и «подкрашенными» шумами в области низкого отношения «сигнал-шум» (от минус 20 дБ до минус 5 дБ) установлено, что коэффициент корреляции между исходным речевым сигналом и зашумлённой последовательностью зависит от типа подкрашенного шума (рисунок 10).

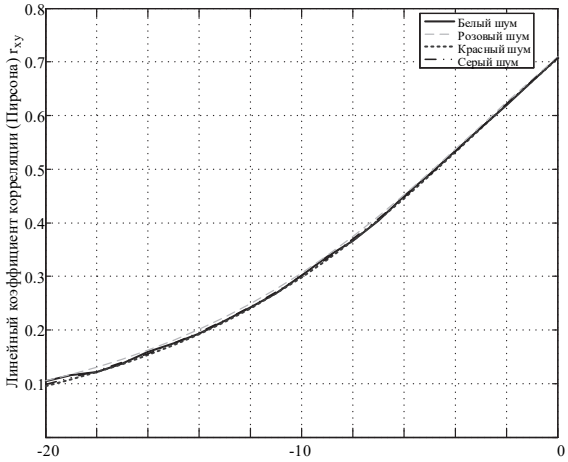


Рис. 10. Зависимость коэффициента корреляции от отношения «сигнал-шум» (для разных типов шумов)

Среднее расхождение полученных значений коэффициента корреляции для четырех указанных типов шумов, исходя из полученных зависимостей, в диапазоне от минус 20 дБ до минус 5 дБ составляет 4,85 %, а для серого и белого шумов — 0,12 %, что подтверждает недостаточную чувствительность данного коэффициента. Поэтому необходимо использовать другой математический аппарат, в качестве которого в настоящем исследовании предлагается применять функцию когерентности [16, 17], которая также, как и коэффициент корреляции показывает степень взаимосвязи сигналов только для области частот, то есть более чувствительна к изменению частотного спектра.

5. Использование функции когерентности сигналов в задаче оценки словесной разборчивости. Для оценки защищенности речевой информации в случае использования средств защиты путем оценки соответствия перехваченной смеси зашумленных сигналов с разных каналов исходному речевому сигналу возможно использование функции когерентности. Данный подход применялся в различных задачах по анализу сигналов, примером чему стали следующие работы [16, 17, 18].

Функция когерентности определяется на основе вычисления квадрата модуля $\Gamma^2_{ss_m}(f)$ по формуле 3 [16-23].

$$\Gamma^2_{ss_m}(f) = \frac{\left|S_{ss_m}(f)\right|^2}{S_{ss}(f) \cdot S_{s_m s_m}(f)}, \quad (3)$$

где $\left|S_{ss_m}(f)\right|$ — взаимная спектральная плотность мощности сигналов s и s_m;

$S_{ss}(f)$ — автоспектральная плотность мощности сигнала s;

$S_{s_m s_m}(f)$ — автоспектральная плотность мощности сигнала s_m.

Функция когерентности показывает постепенное развитие связанности двух процессов на некоторой частоте f_k при дискретном времени, которое изменяется с шагом T, являющимся более длительным временным отрезком, чем интервал дискретизации, характерный для корреляционной функции, которая описывает связи на протяжении лишь одной реализации [16, 21, 23].

Общий вид функции когерентности исходного речевого сигнала и зашумленного речевого сигнала представлен на рисунке 11.

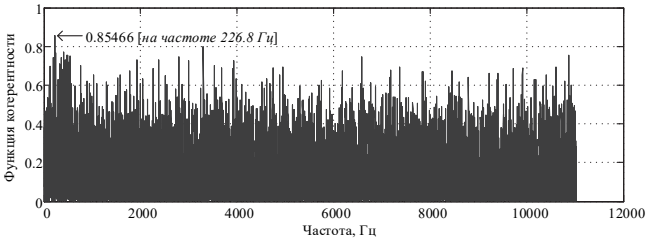


Рис. 11. Функция когерентности сигнала и смеси «сигнал-белый шум» (-20 дБ)

В соответствии с рисунком 11 можно отметить, что наибольшие значения функция когерентности при использовании в процессе моделирования «белого» шума принимает на частотах примерно до 500 Гц с пиком на частоте 226,8 Гц, что, возможно, говорит о

наибольшей информативности речевого сигнала на низких частотах и будет проверено далее.

Так как речевой сигнал является частотозависимым, то для использования функции когерентности в качестве показателя защищенности речевой информации в условиях сильных шумов возникает необходимость применения усредненных значений функции когерентности в отдельных частотных областях. Принимая во внимание особенности речевых сигналов, весь частотный диапазон был разделен на семь октавных полос в соответствии с таблицей 2.

Таблица 2. Значения октавных полос для речевых сигналов

Частотные границы полосы, $f_н$ … $f_в$, Гц	Среднегеометрическая частота полосы, f_i, Гц
88 ... 177	125
177 ... 355	250
355 ... 710	500
710 ... 1 420	1 000
1 420 ... 2 840	2 000
2 840 … 5 680	4 000
5 680 … 11 360	8 000

При исследовании влияния шумов различного уровня на функцию когерентности были получены следующие зависимости математического ожидания функции когерентности в октавных полосах для белого шума (рисунок 12).

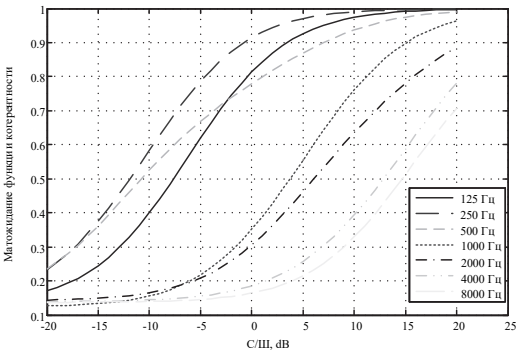


Рис. 12. Зависимость математического ожидания функции когерентности в октавных полосах от отношения «сигнал-шум» (белый шум)

Стоит отметить, что октавные полосы со среднегеометрическими значениями частот 125 Гц, 250 Гц и 500 Гц имеют большие значения при соответствующих значениях отношения «сигнал-шум», нежели остальные октавы, что в случае использования «белого» шума

при маскировании (то есть равномерной в спектре помехи) может говорить о большей информативности речи в области низких частот. В случае использования в качестве маскирующего сигнала других подкрашенных шумов зависимости математического ожидания функции когерентности в октавных полосах приняли несколько другую форму (рисунки 13-15).

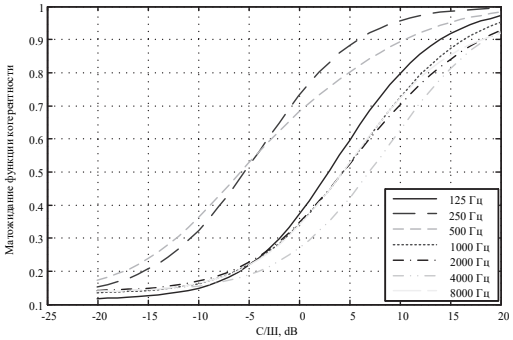


Рис. 13. Зависимость математического ожидания функции когерентности в октавных полосах от отношения «сигнал-шум» (розовый шум)

Общая картина зависимостей рисунка 13, а именно меньшие значения функции когерентности при соответствующих отношениях «сигнал-шум», показывают лучшие «защитные» свойства «розового» шума по сравнению с «белым». В случае использования «розового» маскирующего шума наибольшей информативностью о спектре речевого сигнала обладают октавы со среднегеометрическими частотами 250 и 500 Гц.

Для «красного» шума из-за спектрального состава взаимное расположение графиков претерпело значительные изменения (рисунок 14).

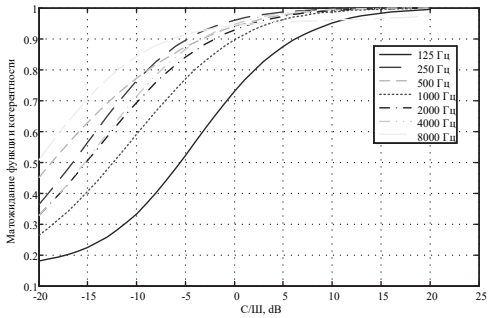


Рис. 14. Зависимость математического ожидания функции когерентности в октавных полосах от отношения «сигнал-шум» (красный шум)

На рисунке 15 представлен вариант с использованием для маскирования «серого» шума.

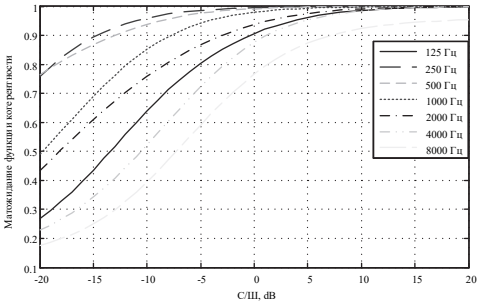


Рис. 15. Зависимость математического ожидания функции когерентности в октавных полосах от отношения «сигнал-шум» (серый шум)

С точки зрения сокрытия информации о речевом сигнале путем его маскировки различными видами шумов, исходя из рисунков 14 и 15, применение «красного» и «серого» шумов представляется нецелесообразным при их сравнении с «белым» и «розовым» шумами.

Для использования значений функции когерентности в качестве показателя защищенности речевой информации необходимо получить определенную функцию на основе преобразований значений математического ожидания функции когерентности в семи октавных полосах. В качестве таковой предлагается функция аддитивной свертки следующего вида:

$$\widehat{\Gamma}^2_{ss_m}(f) = \sum_{i=1}^{7} \left(k_i \cdot \Gamma^2_{ss_m i}(f) \right), \qquad (4)$$

где k_i — коэффициент значимости i-ой октавной полосы со значениями от минус 1 до 1.

Для определения коэффициентов значимости октавных полос были проведены артикуляционные испытания с использованием ПЭВМ в условиях сильных шумов на основе аддитивной модели наложения указанных ранее шумов на исходный тестовый речевой сигнал для различных соотношений «сигнал-шум» от минус 20 дБ до минус 5 дБ.

В результате проведения артикуляционных испытаний получены представленные на рисунке 16 зависимости разборчивости речи в условиях использования аддитивных шумов различных типов («белого», «розового», «красного» и «серого»).

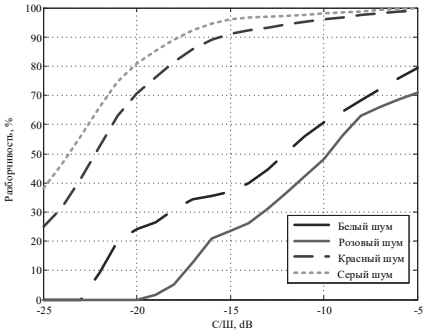


Рис. 16. Зависимость словесной разборчивости от отношения «сигнал-шум» для разных видов шумов по артикуляционным испытаниям

На основе артикуляционных испытаний получено подтверждение лучших маскирующих свойств у «белого» и «розового» шума для защиты речевого сигнала по сравнению с «красным» и «серым» шумами.

При расчете коэффициентов значимости формулы (4) необходимо опираться на значения разборчивости, полученной при проведении артикуляционных испытаний (рисунок 16). Так, для расчета коэффициентов разборчивости необходимо решить недоопределенную систему линейных неравенств (5):

$$\begin{cases} \sum_{i=1}^{7}\left(k_i \cdot \Gamma^2_{ss_{mP}i}(f, SNR)\right) \le W_P(SNR) + \delta \\ \sum_{i=1}^{7}\left(k_i \cdot \Gamma^2_{ss_{mБ}i}(f, SNR)\right) \le W_Б(SNR) + \delta \\ \sum_{i=1}^{7}\left(k_i \cdot \Gamma^2_{ss_{mK}i}(f, SNR)\right) \le W_K(SNR) + \delta \\ \sum_{i=1}^{7}\left(k_i \cdot \Gamma^2_{ss_{mC}i}(f, SNR)\right) \le W_C(SNR) + \delta \end{cases}, \quad (5)$$

где $W_{P,Б,K,C}(SNR)$ — значения словесной разборчивости для соотношения «сигнал-шум» SNR с погрешностью δ.

В результате проведенного моделирования получены зависимости, позволяющие оценивать защищенность речевой информации с учетом спектральных характеристик речи и различных видов шума в условиях применения средств защиты. Результаты построения зависимостей рассчитанной словесной разборчивости от соотношения «сигнал-шум» для различных видов шума представлены на рисунке 17.

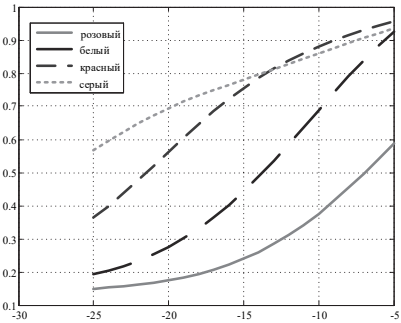


Рис. 17. Зависимости словесной разборчивости от отношения «сигнал-шум»

Графики рисунка 17 демонстрируют результат возможного моделирования относительного показателя защищенности речевой информации через функцию когерентности исходного и зашумленного сигналов для шумов различной спектральной окраски. Для реализации предлагаемого подхода разработан алгоритм оценивания словесной разборчивости речи на основе функции когерентности.

6. Алгоритм оценивания словесной разборчивости речи на основе функции когерентности. В качестве общего алгоритма оценивания показателей защищенности предложен следующий порядок действий, представленный в виде блок-схемы (рисунки 18 и 19).

В данном алгоритме приняты следующие обозначения:

dataS, *dataSN* — временные отсчеты тестового речевого сигнала и зашумленного тестового речевого сигнала;

Cxy — массив-строка спектральных отсчетов функции когерентности;

F — массив-строка частот спектральных отсчетов функции когерентности;

F_Coh — массив-строка математических ожиданий функции когерентности в октавах;

Coh — значение функции свертки математических ожиданий функции когерентности в октавных полосах;

K — массив-строка коэффициентов значимости октав для расчета свертки функции когерентности;

W — рассчитанное относительное значение словесной разборчивости речи.

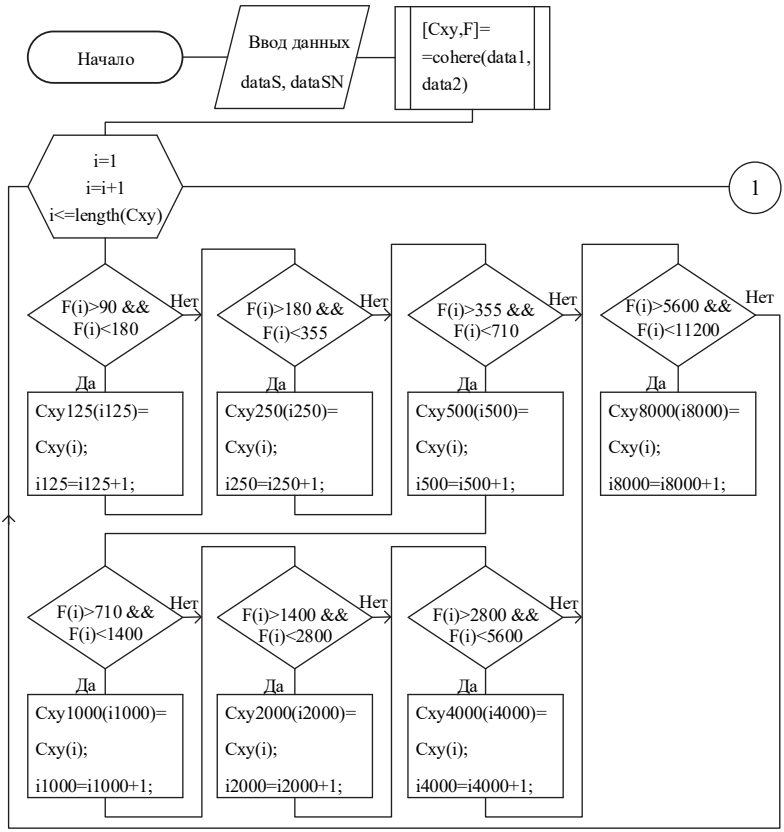


Рис. 18. Блок-схема алгоритма оценивания словесной разборчивости речи на основе функции когерентности (начало)

Входными данными алгоритма являются временные отсчеты тестового речевого сигнала и зашумленного тестового речевого сигнала. На их основе в подпрограмме рассчитывается функция когерентности на основании выражения (3). После этого в цикле дискретные значения частотных составляющих группируются по отдельным октавным полосам в соответствии с таблицей 2. По значениям частотных составляющих для каждой октавы рассчитывается их математическое ожидание, после чего вычисляется значение функции аддитивной свертки, исходя из выражения (7), на основе которой получается оценочное значение словесной разборчивости речи.

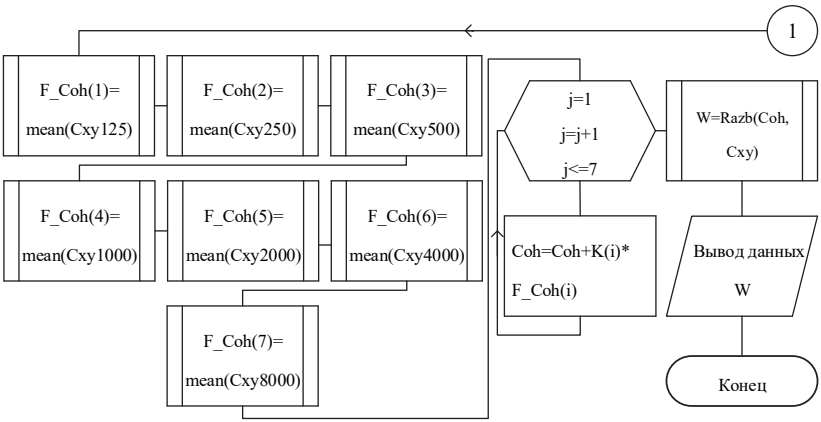


Рис. 19. Блок-схема алгоритма оценивания словесной разборчивости речи на основе функции когерентности (окончание)

При использовании в качестве маскирующего «белого» шума в диапазоне отношения «сигнал-шум» от минус 20 дБ до минус 5 дБ рассмотренными в работе методами были получены следующие данные (рисунок 20). Наиболее точные результаты показывает метод артикуляционных испытаний. Существующий подход, описанный в [6, 10], занижает значение разборчивости на 12%. Предлагаемый алгоритм оценивания словесной разборчивости на основе функции когерентности завышает значение разборчивости на 5%.

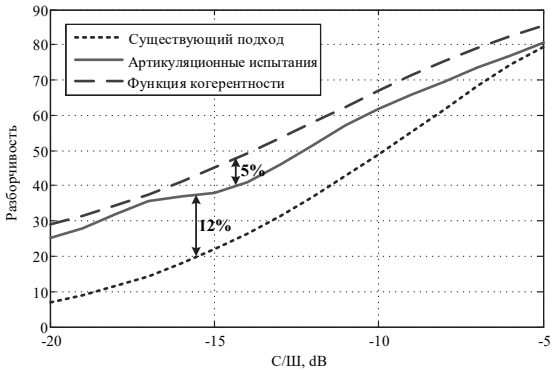


Рис. 20. Эффективность применения функции когерентности для расчета словесной разборчивости речи

В результате применения предложенного подхода было достигнуто повышение точности оценивания разборчивости на 7% по сравнению с используемой в настоящее время методикой.

7. Заключение. В исследовании показана несостоятельность применения коэффициента корреляции Пирсона для определения показателя защищенности, так как данный коэффициент обладает низкой чувствительностью к спектральному составу сигналов, что приводит к мизерной разнице между усреднёнными коэффициентами для белого и серого шума в 0,12%.

Представленные в статье результаты исследований позволяют уточнить расчет показателей защищенности речевой информации в условиях действия сильных шумов, то есть при использовании средств акустической защиты при соотношении «сигнал-шум» от минус 20 дБ до минус 5 дБ.

В работе приводится блок-схема алгоритма оценивания словесной разборчивости речи на основе функции когерентности, на основе которого представляется возможным рассчитывать значение словесной разборчивости как показателя защищенности речевой информации.

Проведенные исследования позволили повысить точность оценивания разборчивости инструментальными методами на 7% по сравнению с существующим подходом.

В дальнейшем исследования позволят с большей точностью оценивать защищенность речевой информации в условиях вынужденного использования средств акустической защиты, а на основе полученных оценок делать вывод об использовании дополнительной защиты.

Литература

1. *Гаврилова Е.С.* Структура речевого воздействия // Вестник Новгородского государственного университета имени Ярослава Мудрого. 2015. № 87. Ч. 1. С. 145–148.
2. *Гаврилов И.В.* Построение вероятностной модели комплексной системы защиты речевой информации для контроля ее защищенности // Вопросы защиты информации. 2015. № 3. С. 79–84.
3. *Аншакова Е.П., Чернышов А.К.* Методика защиты помещений от утечки речевой информации по техническим каналам // Прикаспийский журнал: управление и высокие технологии. 2010. № 1(9). С. 13–18.
4. *Железняк В.К., Раханов К.Я., Бураченок И.Б.* Оценка разборчивости речи взаимной корреляцией сигнала линейной частотной модуляции в каналах утечки инфомации // Вестн. Полоц. гос. ун-та. Сер. С. Фундаментальные науки. 2015. № 12. С. 22–27.
5. *Сагдеев К.М., Петренко В.И.* Методика оценки технической защищённости речевой информации в выделенных помещениях // Известия ЮФУ. Технические науки. 2012. № 12(137). С. 121–129.
6. *Железняк В.К., Макаров Ю.К., Хорев А.А.* Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. 2000. № 4. С. 39–45.
7. *Глущенко Л.А., Ныркова А.П., Швед Д.В.* Применение корреляционного подхода к определению качества речевой информации, зарегистрированной лазерным микрофоном // Вестник государственного университета морского и речного флота имени адмирала С.О. Макарова. 2015. Вып. 6 (34). С. 187–195.

8. *Гаврилов И. В.* Методика оценивания качества маскирующего шума // Труды СПИИРАН. 2015. Вып. 6(43). С. 179–190.
9. *Дворянкин С.В., Макаров Ю.К., Хорев А.А.* Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам // Защита информации. Инсайд. 2007. № 2(14). С. 18–25.
10. *Хорев А.А.* Контроль эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам // Защита информации. Инсайд. 2010. № 1(31). С. 34–45.
11. *Покровский Н.Б.* Расчёт и измерение разборчивости речи // М.: Связьиздат. 1962. 392 с.
12. *Быков Ю.С.* Теория разборчивости речи в линиях связи // Оборонгиз. 1954.
13. *Дворянкин С.В., Козлачков С.Б., Бонч-Бруевич А.М.* Анализ возможностей корреляционного метода оценки эффективности маскирования речи белым шумом // URL: http://runc.bmstu.ru/articles/kor_filters.pdf (дата обращения: 18.06.2016).
14. *Журавлёв В.М., Архипова Е.А.* Метод экспериментального анализа функции эффективности маскирования речи // Вестник Винницкого политехнического института. 2009. № 1.
15. *Тактаров Н. Г.* Справочник по высшей математике для студентов вузов // М.: Книжный дом «ЛИБРОКОМ». 2009. 880 с.
16. *Бендат Дж.* Прикладной анализ случайных данных // М.: Мир. 1989. 540 с.
17. *Ханян Г. С.* Некоторые аспекты конструирования и вычисления дискретной функции когерентности двух сигналов // Вестник научно-технического развития. 2010. № 7(35). С. 31–35.
18. *Бороноев В. В.* Оценка функции когерентности пульсовых сигналов при многоканальной пульсометрии // Вестник бурятского государственного университета. 2012. № 3. С. 219–221.
19. *Stoica P.* Introduction to Spectral Analysis // Upper Saddle River. NJ: Prentice-Hall. 1997. 345 p.
20. *Kay S.M.* Modern Spectral Estimation // Englewood Cliffs. NJ: Prentice-Hall. 1988. 576 p.
21. *Отнес Р.* Прикладной анализ временных рядов // М.: Мир. 1982. 432 с.
22. *Rabiner L. R.* Theory and Application of Digital Signal Processing // EnglewoodCliffs. NJ: Prentice-Hall. 1975. 762 p.
23. *Марпл. С.Л.* Цифровой спектральный анализ и его приложения // М.: Мир. 1990. 584 с.

Гаврилов Илья Вячеславович — сотрудник, Академия Федеральной службы охраны Российской Федерации. Область научных интересов: системы активной защиты информации. Число научных публикаций — 7. ilya_vch@pisem.net; Приборостроительная, 35, Орел, 302034; р.т.: +7(4862)549533.

I.V. GAVRILOV

AN ALGORITHM FOR ASSESSING VERBAL SPEECH RECOGNITION BASED ON THE COHERENCE FUNCTION

Gavrilov I.V. **An Algorithm for Assessing Verbal Speech Recognition based on the Coherence Function.**

Abstract. The problem of estimating the vulnerability of the speech information of a confidential nature is currently topical. However, in the use of means of acoustic protection, i.e. in conditions of strong noise, the existing instrumental and computational methods give greater accuracy when compared with the extremely labor intensive methods of articulation.

In the paper we study the method of estimating the security of voice data based on the Pearson correlation coefficient. This ratio has poor sensitivity to the spectral properties of the acoustic signals. Therefore, the author suggests an approach to the definition of the security indicator of voice data based on the mathematical apparatus of the coherence function of source and noisy signals.

We propose to split the entire speech frequency range of the coherence function into separate octaves. We also offer to calculate the expectation of the coherence function components in octaves and on the basis of convolution function obtain an expression for calculating the index of the vulnerability of speech.

The proposed algorithm for determining the vulnerability index of voice data allows improving the assessment accuracy.

Keywords: masking noise, correlation coefficient, frequency spectrum of the signal, active security facilities, coherence function signal spectrum, active security facilities.

Gavrilov Ilya Vyacheslavovich — researcher, The Academy of Federal Security Guard Service of the Russian Federation. Research interests: system of active information security. The number of publications — 7. ilya_vch@pisem.net; 35, Priborostroitelnaya Street, Orel, 302034, Russia; office phone: +7(4862)549533.

References

1. Gavrilova E.S. [The structure of the speech influence]. *Vestneyk Novgorodskogo gosudarstvennogo universiteta imeni Iaroslava Mudrogo – Vestnik Yaroslav Mudry Novgorod State University*. 2015. vol. 87. Part 1. pp.145–148. (In Russ.).
2. Gavrilov I.V. [Construction of a probabilistic model of the complex system of protection of the speech information to control its security]. *Voprosy zashchity informatcii – The protection of information*. 2015. vol. 3. pp. 79–84. (In Russ.).
3. Anshakova E. ., Chernyshov A.K. [Methods of protection of the premises against leakage of voice information through technical channels]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii – Caspian journal: Management and high technologies*. 2010. vol. 1(9). pp. 13–18. (In Russ.).
4. Zhelezniak V.K., Rahanov K.Ya., Burachenok I.B. [Evaluation intelligibility mutual correlation chirp signal leakage in channels Infomatsiya]. *Vestn. Polotc. gos. un-ta. Ser. S. Fundamentalnye nauki – Bulletin Polotsk State University. Series C: Basic Sciences.* 2015. vol. 12. pp. 22–27. (In Russ.).
5. Sagdeev K.M., Petrenko V.I. [Methods of evaluation of technical security of voice data in selected areas]. *Izvestiia IUFU. Tekhnicheskie nauki – Proceedings of SFU. Technical science*. 2012. vol. 12(137). pp. 121–129. (In Russ.).
6. Zhelezniak V.K., Makarov Iu.K., Horev A.A. [Some methodological approaches to evaluating the effectiveness of information security speech]. *Spetcialnaia tekhnika – Special equipment*. 2000. vol.4. pp. 39–45. (In Russ.).

7. Glushchenko L. A., Nyrkov A. P., Shved D. V. [The use of correlation approach to defining the quality of the voice information recorded by laser microphone]. *Vestnik gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S.O. Makarova – Bulletin of the State University of Maritime and River Fleet of the Admiral Makarov*. 2015. vol. 6(34). pp. 187–195. (In Russ.).
8. Gavrilov I.V. [Method of estimation of the masking sound quality]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2015. vol. 6(43). pp. 179–190. (In Russ.).
9. Dvoriankin S.V., Makarov Iu.K., Horev A.A. [Justification of criteria of efficiency of speech information protection against leakage via technical channels]. *Zashchita informatcii. Insaid – Data protection. Inside*. 2007. vol. 2(14). pp. 18–25. (In Russ.).
10. Horev A.A. [Monitoring the effectiveness of the protection of the premises allocated by the leakage of voice information through technical channels]. *Zashchita informatcii. Insayd – Data protection. Inside*. 2010. vol. 1(31). pp. 34–45. (In Russ.).
11. Pokrovskiy N.B. *Raschjot i izmerenie razborchivosti rechi* [Calculation and measurement of speech intelligibility]. M.: "Sviaz izdat". 1962. 392 p. (In Russ.).
12. Bykov Yu.S. *Teorija razborchivosti rechi v linijah svjazi* [Theory of speech intelligibility in communication lines]. Oborongiz. 1954. (In Russ.).
13. Dvoriankin S.V., Kozlachkov S.B., Bonch-Bruevich A.M. *Analiz vozmozhnostej korreljacionnogo metoda ocenki jeffektivnosti maskirovanija rechi belym shumom* [Capacity analysis of the correlation method of evaluating the effectiveness of speech masking white noise]. RUNTC «Bezopasnost» MGTU im. N.E`. Baumana. Available at: http://runc.bmstu.ru/articles/kor_filters.pdf (accessed: 18.06.2016) (In Russ.).
14. Zhuravlyov V.M., Arhipova E.A. [The method of experimental analysis of speech masking efficiency function]. *Vestneyk Vinnitckogo politekhnicheskogo instituta – Herald of Vinnitsa Polytechnic Institute*. 2009. vol. 1. (In Russ.).
15. Taktarov N. G. *Spravochnik po vysshej matematike dlja studentov vuzov* [Handbook of higher mathematics for students] M.: Knizhny`i` dom «LIBROKOM». 2009. 880 p. (In Russ.).
16. Bendat J. *Prikladnoj analiz sluchajnyh dannyh* [Applied analysis of random data]. M.: Mir. 1989. 540 p. (In Russ.).
17. Hanian G.S. [Some aspects of the design and calculation of the discrete coherence function of the two signals]. *Vestneyk nauchno-tekhnicheskogo razvitiia – Journal of Scientific and Technological Development*. 2010. vol. 7(35). pp. 31–35. (In Russ.).
18. Boronoev V.V. [Assessment of the coherence function of the pulse signals in multi-channel pulsometry]. *Vestneyk buriatskogo gosudarstvennogo universiteta – Bulletin of the Buryat State University.* 2012. vol. 3. pp. 219–221. (In Russ.).
19. Stoica P. Introductionton to Spectral Analysis. Upper Saddle River. NJ: Prentice-Hall. 1997. 345 p.
20. Kay S.M. Modern Spectral Estimation. Englewood Cliffs. NJ: Prentice-Hall. 1988. 576 p.
21. Otnes R. *Prikladnoj analiz vremennyh rjadov* [Applied time series analysis]. M.: Mir. 1982. 432 p. (In Russ.).
22. Rabiner L. R. Theory and Application of Digital Signal Processing. EnglewoodCliffs. NJ: Prentice-Hall. 1975. 762 p.
23. Marpl-ml. S.L. *Cifrovoj spektral'nyj analiz i ego prilozhenija* [Digital Spectral Analysis and Its Applications]. M.: Mir. 1990. 584 p. (In Russ.).

УДК 004.82 **DOI** 10.15622/sp.48.6

Г.В. Каныгин, М.С. Полтинникова

КОНТЕКСТНО-ОРИЕНТИРОВАННЫЕ ОНТОЛОГИЧЕСКИЕ МЕТОДЫ В СОЦИОЛОГИИ

Каныгин Г.В., Полтинникова М.С. **Контекстно-ориентированные онтологические методы в социологии.**

Аннотация. В статье предложены контекстно-ориентированные онтологические методы описания социальных объектов. В основе методов лежит графовая модель онтологии. Модель основывается на множестве двухуровневых деревьев, называемых ветвлениями, вершины которых состоят из пар понятий. Первое понятие пары — термин, второе — контекст, относительно которого рассматривается термин. Предложено правило контекстного обобщения понятий, стоящих в позициях контекста. Разработаны алгоритмы построения графа иерархии контекстов и терминологического графа. Получен критерий логической связности онтологии, основанный на структуре терминологического графа. Особенности описываемой модели и работа пользователя при ее применении продемонстрированы на примере.

Ключевые слова: онтологические методы, контекстно-ориентированная онтология, ветвление, контекстное обобщение понятий, графовая модель, терминологический граф, граф иерархии контекстов.

1. Введение. Функциональность языков объектно-ориентированного программирования (ООП) (например, C#, Java, Python, Free Pascal), представляющая собой основу компьютерных технологий двух последних десятилетий [1], построена на средствах типизации программных единиц и их связывании в виде отношений наследования, инкапсуляции и полиморфизма. С одной стороны, функциональность ООП совершенствует структурное программирование с его принципами «разработки сверху» и модульной организации кода, с другой — получает развитие в виде идей и методов концептуального моделирования, разновидностью которого служат онтологические методы управления знанием [2-4].

Основным средством конструктивного определения функциональности как в случае программирования, так и концептуального моделирования, является язык спецификации [3]. Язык спецификации имеет, как правило, текстовую форму [5, С.14]. Вместе с тем развиваются графические языки [6, 7].

Разработчики языков спецификаций готовы применять их для концептуализации как естественно-научных (physical world), так и гуманитарных предметных областей (social world) [8]. Однако при концептуализации социологических предметных областей важно учитывать, что социальная реальность конструируется самими участниками социальных процессов [9], и социологические

определения создаются с точностью до индивида [10].

Тем самым оказывается, что в случае социологической концептуализации важно не только воспроизведение «объекта», но и кто этот «объект» воспроизводит. Поэтому вызывают сомнение, во-первых, взгляд на понятия социологической предметной области (social world) как на предметно обусловленные (верования, желания, намерения и др.), организованные в специализированные онтологии UFO-C [11]; во- вторых, сама идея моделировать подобные понятия на основе предварительно разработанных онтологических спецификаций общего назначения UFO-A, UFO-B [6, 11].

Онтологический язык для социологических приложений должен быть рассчитан на описание с его помощью тех лиц и их сообществ, называемых далее *социальными акторами* или просто *акторами*, которые проводят концептуализацию в процессе своей социальной коммуникации. Многоплановость и сложность социальной коммуникации не вызывает сомнения. Поэтому первым требованием к языку спецификации в области социологии является реализуемость с его помощью современной компьютерной функциональности и приводящих к созданию сложно взаимосвязанных систем современного информационного общества [12].

Согласно современным тенденциям в области социологии [13], описание социальной коммуникации следует осуществлять с помощью акторов, являющихся участниками этой коммуникации. Поэтому онтологические средства, рассчитанные на применение в области социологии, должны удовлетворять еще одному требованию: они должны быть доступны в прикладном применении для пользователя компьютера, не обладающего специальными знаниями в области языков создания онтологий.

В настоящей статье описаны базовые модели инструментальных средств концептуализации, удовлетворяющие выдвинутым требованиям. Синтаксис этих средств задается в виде графов. Семантика рассчитана на коллективное построение онтологий сообществом пользователей, не являющихся профессионалами в компьютерной области.

В составе предлагаемых средств рассмотрены: модели аналитических единиц концептуализации (понятий); структурный механизм их типизации (термин, контекст, пояснение, контекст пояснений); графовый синтаксис локальных отношений между понятиями и алгоритмы компиляции единой концептуальной модели на основе локальных отношений.

2. Графовая модель онтологии. *Понятие* — это элементарная аналитическая единица (дескриптор), с помощью которой автор может

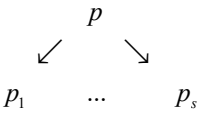
назвать (поименовать, описать) любой интересный для него объект (сюжет, тему, случай). Понятие может быть словом или словосочетанием.

Словарь — это неупорядоченное множество $T = \{t_1, t_2, ..., t_q\}$, где t_1 — понятия, а q — их количество.

Потребуем, чтобы для обозначения описываемого объекта автор онтологии (далее автор) использовал пару понятий множества T: одно понятие для обозначения объекта, второе понятие для обозначения условий или контекста, при которых этот объект рассматривается. Описание объектов парами понятий реализуется через задание отношений на множестве $T \times T$.

Пусть $P = \{p_1, ..., p_s\} = \{(x_1, y_1), ..., (x_s, y_s)\} \subset T \times T$ — множество (упорядоченных) пар, введенных автором (авторами) к некоторому моменту времени.

2.1. Определение ветвления. Назовем *ветвлением* или *контекстно-фиксированным разъяснением* двухуровневое ориентированное дерево E с вершинами из множества $P \times P$:



Здесь s — количество пар, заданных пользователем на нижнем уровне дерева, $s < q$. Далее будем обозначать ветвление E так:

$$E: p \to \{p_1, ..., p_1\} \text{ или } E: (x, y) \to \{(x_1, y_1), ..., (x_s, y_s)\}.$$

Будем называть x *термином*, y — *контекстом*, x_k — *пояснением*, y_k — *контекстом пояснения*, $k = 1, ..., s$. Пару (x, y) назовем *головной*, а пару (x_k, y_k) — *разъяснением*. Множество пар $\{p_k\} = \{(x_k, y_k)\}$, где $k = 1, ..., s$ будем называть *множеством разъяснений*. Заметим, что одно и то же понятие словаря в различных ветвлениях может выступать в качестве термина, контекста, пояснения или контекста пояснения.

Множество разъяснений $\{p_1, \ldots, p_s\}$ получается из ответа на вопрос о том, какие понятия участвуют в определении термина x при условиях, обозначенных понятием y . Множество разъяснений может быть пустым.

Рассмотрим пример, в котором в качестве понятий будем

использовать слова и словосочетания естественного языка:

$T =$ {семья, определения семьи, семья в социологии, семья в юриспруденции, семья в педагогике}.

Зададим ветвление E_0: (семья, определения семьи) → {(семья в социологии,...),(семья в юриспруденции,...), (семья в педагогике,...)}.

Здесь семья — термин, определения семьи — контекст, семья в социологии, семья в юриспруденции и семья в педагогике — пояснения, . . . — неуказанные контексты пояснений. Головная пара — (семья, определения семьи), три разъяснения (семья в социологии, ...); (семья в юриспруденции, ...); (семья в педагогике, ...) образуют множество разъяснений.

Пусть $E = \{E_1, E_2, ..., E_k\}$ — множество всех ветвлений, введенных автором для некоторого словаря Т . Понятие называется однозначным, если задающий его термин х разъясняется ровно в одном ветвлении множества E . Понятие называется многозначным, если задающий его термин x разъясняется более, чем в одном ветвлении множества E .

В нашем примере пополним множество T элементами социология, юриспруденция, педагогика, а множество E ветвлениями (определения семьи, социология) → ∅ ; (определения семьи, юриспруденция) → ∅ ; (определения семьи, педагогика) → ∅ . Тогда семья — однозначное понятие, а определения семьи — многозначное.

2.2. Определение КО тезауруса. Предположим, что для T и E выполнено следующее условие: для любого $t \in T$ найдется $E \in E$, в котором участвует термин t . Пусть P — множество всех пар понятий, участвующих в ветвлениях множества E . Тогда множество P со структурой, порождаемой ветвлениями множества E , назовем контекстно-ориентированным тезаурусом сокращенно КО тезаурусом: $G := \{P, E\}$.

КО тезаурус представляет собой ориентированный граф (орграф), у которого элементы множества P — это вершины, а ребра — это ребра деревьев (ветвлений) из E . Такая структура соответствует классическому определению онтологии [14].

Заметим, что в определении ветвления запрещено определять головную пару понятий через множество разъяснений, содержащее ее же. Тем не менее в графе КО тезауруса могут появиться циклы, что свидетельствует об ошибках структуры. Наша пробная программа показывает авторам эти циклы, чтобы они могли тем или иным способом изменить структуру КО тезауруса. Алгоритм поиска циклов выходит за рамки данной статьи.

Продолжим пример концептуализации понятия семьи. Существует ряд «академических» определений этого понятия [15, 16]. Авторы конкретных исследований предлагают свои формулировки. Приведем одну из таких наработок: «С точки зрения социологии, семья — это группа людей, связанная кровным родством и брачными узами. Юридическая наука дополняет данное определение и говорит, что семья является объединением нескольких совместно проживающих лиц, которые связаны между собой правовыми отношениями, определенным кругом обязанностей, возникающих после заключения брака и вступления в родство. В педагогике и в психологии делается упор на личные взаимоотношения членов семьи и разных поколений, на воспитательную и социальную роль представителей старшего поколения в развитии младших участников общественной группы.

Данное понятие многогранно. Но каждое определение подтверждает, что это малая группа, ячейка общества, в которой люди связаны между собой определенными отношениями» [17].

Мы уже начали строить словарь T и множество ветвлений E в соответствии с сюжетом [17]. Продолжим это построение, поясняя предлагаемые структурные модели и алгоритмы.

2.3. Фиксация контекста термина. Пусть имеются два понятия x и y. Фиксация контекста термина — это операция связывания x и y в головную пару. Для этого достаточно, чтобы автор создал ветвление вида: $(x, y) \to \varnothing$.

В нашем примере, чтобы зафиксировать контекст социология для понятия определения семьи, мы создали ветвление вида: (определения семьи, социология) $\to \varnothing$. Далее можно разъяснить термин социология так:

$$(\text{социология, старая школа социологии}) \to \varnothing;$$
$$(\text{социология, новая школа социологии}) \to \varnothing.$$

В словарь при этом добавляются понятия старая школа социологии и новая школа социологии, а понятие социология становится многозначным.

В процессе введения понятий у автора в какой-то момент наступает необходимость указать последний контекст, не подлежащий дальнейшему разъяснению. В качестве соглашения мы считаем, что в любом тезаурусе имеется понятие общее знание, которое выступает контекстом для понятий, рассматриваемых автором в качестве самых общих.

Подчеркнем, что для фиксации контекста термина пользователь может не указывать пояснения и их контексты. В нашем примере может быть построен следующий набор ветвлений:

(новая школа социологии, гуманитарные науки) $\rightarrow \varnothing$;
(старая школа социологии, гуманитарные науки) $\rightarrow \varnothing$;
(гуманитарные науки, наука) $\rightarrow \varnothing$;
(наука, общее знание) $\rightarrow \varnothing$.

2.4. Контекстное дополнение пояснений. Работа с КО тезаурусом всегда происходит на основе пар понятий, то есть для каждого понятия из T необходимо зафиксировать контекст, в котором понятие рассматривается как термин. Такая фиксация контекста осуществляется пользователем путем заполнения головной пары некоторого ветвления E. Установление связей понятий головной пары E с другими понятиями словаря осуществляется пользователем путем указания множества разъяснений ветвления E.

Для заполнения новых разъяснений автор может использовать контексты, имеющиеся к данному моменту в КО тезаурусе. В парах разъяснений можно указывать только пояснения, а контекст оставлять пустым. В этом случае любая пустая позиция контекста пояснения может быть заполнена одним из имеющихся контекстов КО тезауруса.

Представим себе ветвление с незаполненной позицией контекста: $E:(x,y)\rightarrow\{(x_i,...)\}, i=1,...,k.$ Для того чтобы иметь возможность заполнить эту позицию на основе просмотра тезауруса автоматически, без участия пользователя, введем следующее правило. Если x_i является однозначным и служит термином в головной паре ветвления $(x_i, y_i) \rightarrow$ {множество разъяснений}, то контекст y_i будет автоматически подставлен на место контекста пояснения для пояснения x_i.

В случае многозначности понятия, задаваемого x_i, выбор контекста пояснения должен сделать пользователь. Программа-онторедактор при этом только предлагает контексты из найденных головных пар.

Операцию автоматизированного дополнения контекста для пояснения x_i ветвления E по имеющимся головным парам с x_i, находящимся в положении термина, назовем *контекстным дополнением пояснения.*

Покажем, как это происходит на примере. Ранее было задано

ветвление E_0: (семья, определения семьи) → {(семья в социологии,...), (семья в юриспруденции,...), (семья в педагогике,...)}., которое не содержало контекстов пояснений.

Дополним словарь T понятиями малая группа, круг обязанностей, отношения поколений семьи, личные взаимоотношения, а множество E ветвлениями вида:

(семья в социологии, социология) → {(малая группа,...)};
(семья в юриспруденции, юриспруденция) → {(малая группа,...); (круг обязанностей,...)};
(семья в педагогике, педагогика) → {(малая группа,...); (отношения поколений семьи,...); (личные взаимоотношения,...)};

По правилу контекстного дополнения программа автоматически дополнит контексты пояснений для E_0 следующим образом:

(семья, определения семьи) → {(семья в социологии, социология), (семья в юриспруденции, юриспруденция), (семья в педагогике, педагогика)}.

2.5. Контекстное обобщение понятий. Пусть термин t_0 пояснен в некотором контексте t_1, а термин t_1 пояснен в контексте t_2:

$$(t_0, t_1) \to \{\cdots\}, \quad (t_1, t_2) \to \{\cdots\}.$$

Тогда t_2 называется *контекстным обобщением* t_1, что записывается так: $t_1 \hookrightarrow t_2$.

Другими словами, если t_1 — контекст и имеется ветвление $(t_1, t_2) \to \{\cdots\}$, то $t_1 \hookrightarrow t_2$.

Рассмотрим $\{y_1, y_2, ..., y_n\}$ — все контексты тезауруса G. Граф иерархии контекстов — это граф с вершинами y_k и ребрами, заданными с помощью контекстного обобщения.

Обозначим через $G_1, ..., G_r$ компоненты связности графа иерархии контекстов. Далее мы будем рассматривать одну из компонент связности, полагая, что именно ее контексты отвечают за связные части онтологии.

В нашем примере (см. Приложение) имеется следующее

множество контекстов: C ={определения семьи, социология, юриспруденция, педагогика, старая школа в социологии, новая школа в социологии, социальные науки, наука, гуманитарные науки, естественные науки}.

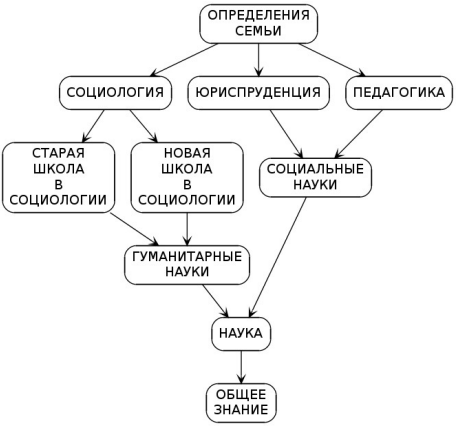


Рис. 1. Граф иерархии контекстов «Определения семьи»

Покажем, каким образом контекстное обобщение работает при построении иерархии контекстов для понятия определения семьи. Найдем ветвления, в которых оно стоит на позиции термина:

(определения семьи, социология) $\rightarrow \varnothing$;
(определения семьи, юриспруденция) $\rightarrow \varnothing$;
(определения семьи, педагогика) $\rightarrow \varnothing$.

В силу определения контекстного обобщения получим три связи:

определения семьи ↪ социология; определения семьи ↪ юриспруденция; определения семьи ↪педагогика.

На рисунке 1 эти связи выражены в виде перехода от корня к первому уровню. Каждое из понятий, получаемых в результате контекстного обобщения (социология, юриспруденция, педагогика), также контекстно обобщается. Этот процесс продолжается, пока не исчерпаются ветвления тезауруса для множества C . В результате получаем граф иерархии контекстов, представленный на рисунке 1.

На рисунке 2 показана иерархия контекстов как результат «компиляции» КО тезауруса, выполненной нашей пробной программой. Эта иерархия контекстов состоит из набора отдельных ветвей и имеет повторяющиеся вершины.

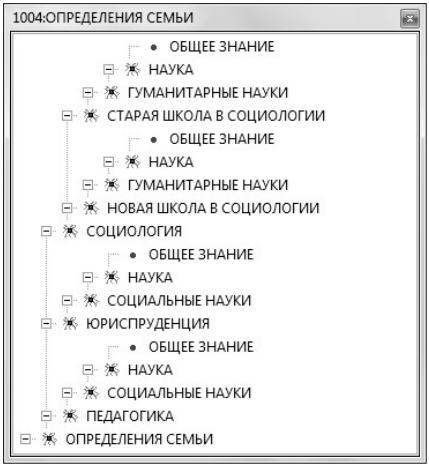


Рис. 2. Иерархия контекстов «Определения семьи»

2.6. Терминологический граф. Для построения терминологического графа мы выбираем корневую вершину $(x, y) \in P$, ветвление $E_0 : (x, y) \to \{(x_1, y_1), (x_2, y_2), ..., (x_s, y_s)\}$ и правило связи контекстов $f(y)$, которое представляет собой некоторый граф иерархии кон- текстов с началом в y.

Если в ветвлении E_0 не заполнены контексты пояснений $(x, y) \to \{(x_1, ...); (x_2, ...); ...(x_s, ...)\}$, то, применив к каждому пояснению операцию контекстного дополнения, получим ветвление $(x, y) \to \{(x_1, y_1); (x_2, y_2); ...(x_s, y_s)\}$.

Затем из множества пояснений ветвления E_0 мы выбираем только те пары, контексты которых связаны правилом $f(y)$. Пусть первый уровень графа $f(y)$ содержит $k \le s$ контекстов ветвления E_0 : $f1(y) = \{y_{r1}, \ldots y_{rk}\}$. Получим двухуровневый терминологический граф вида:

$$(x, y)$$
$$\swarrow \quad \searrow$$
$$(xr1, yr1) \quad ... \quad (xrk, yrk).$$

Затем операция повторяется: для каждой из вершин первого

уровня находим ветвление (если оно существует). Из этих ветвлений во второй уровень терминологического графа попадают только те вершины, контексты которых совпадают с контекстами второго уровня графа $f(y)$. Получим двухуровневый терминологический граф, и т.д.

Этот процесс наращивания вершин конечен (с точностью до циклов) в силу конечности КО тезауруса. Алгоритм построения терминологического графа в качестве выхода предъявляет все получившиеся циклы. Вопрос о том, как изменить КО тезаурус, чтобы убрать циклы, решает автор этого тезауруса.

Правила связи контекстов $f(y)$ могут быть различными. Мы рассмотрим правило, по которому в $f(y)$ входят все контекстные обобщения y. Покажем на примере (см. Приложение), как работает такое правило. Введем правило f (определения семьи) на основе построенной иерархии контекстов, представленной на рисунке 3.

Далее рассмотрим, каким образом функционирует это правило на примере формирования узлов терминологического графа при построении ветвления пары (семья в социологии, социология). В качестве возможных преемников указаны пары, которые образует термин *малая группа*. Тезаурус содержит 4 такие пары: (малая группа, старая школа в социологии), (малая группа, новая школа в социологии), (малая группа, социальные науки), (малая группа, педагогика).

Чтобы решить, какие из этих пар будут использованы, рассмотрим иерархию контекстов, задающую правило $f(y)$ (рисунок 3). Получим, что в качестве преемников пары (семья в социологии, социология) могут быть приняты пары (малая группа, старая школа в социологии) и (малая группа, новая школа в социологии). По тем же основаниям пары (малая группа, социальные науки) и (малая группа, педагогика) должны быть отсеяны при построении терминологического графа. Аналогичным образом строятся и все остальные ветви терминологического графа.

Рис. 3. Правило связи контекстов f (определения семьи)

Результат построения терминологического графа для корневой вершины (семья, определения семьи) и правила связи контекстов из рисунка 2 (это правило включает все возможные связи контекстов) представлен на рисунке 4.

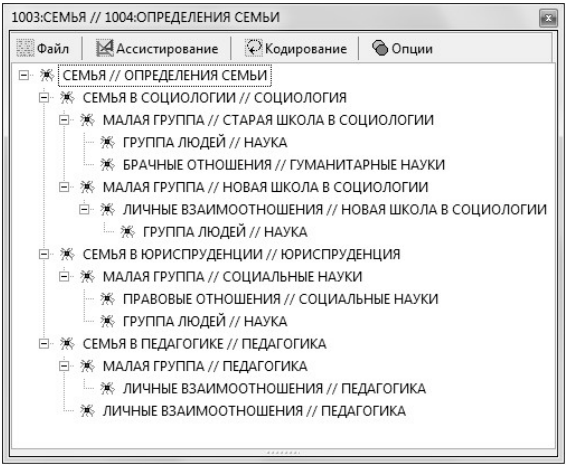


Рис. 4. Терминологический граф «Семья» для полного графа Контекстов

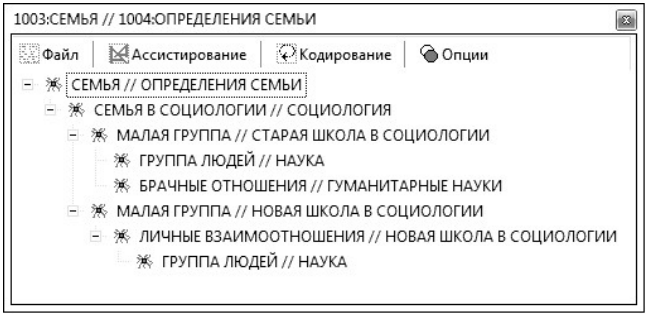


Рис. 5. Терминологический граф «Семья» для ветви «СОЦИОЛОГИЯ» графа Контекстов

Результат построения терминологического графа для корневой вершины (семья, определения семьи) и правила связи контекстов из рисунка 3 представлен на рисунке 5.

3. Заключение. В статье описаны и продемонстрированы контекстно-ориентированные онтологические методы. Они удовлетворяют требованиям, позволяющим использовать их при решении задач коллективного сбора и анализа социальной информации. Предложенные методы, основываясь на описании социальных объектов в естественно-языковом виде, дают в распоряжение пользователя средства структурирования, характерные для современных информационных технологий. Методы контролируют связность естественно-языковых описаний, предложенных коллективом пользователей для описания социальных объектов. Компьютерная реализация описанных методов позволяет строить систему знаний, отдельные части которой коллективно доступны и коллективно наращиваемы. Развитие и совершенствование контекстно-ориентированных онтологических методов в виде визуальной компьютерной среды позволяет предложить новые средства алгоритмизации и контроля деятельности социальных акторов для информационно-аналитических систем социального управления.

Приложение. Рассмотрим КО тезаурус, построенный пробной программой-онторедактором. В нем проведена концептуализация понятия семьи из [17].

Множество понятий T :

{семья, определения семьи, семья в социологии, семья в юриспруденции, семья в педагогике, социология, юриспруденция, педагогика, старая школа в социологии, новая школа в социологии,

социальные науки, малая группа, группа людей, кровное родство, брачные от- ношения, личные взаимоотношения, наука, гуманитарные науки, круг обязанностей, отношения поколений семьи, естественные науки}.

Множество контекстно-фиксированных разъяснений *E*:

(семья, определения семьи) → {(семья в социологии,...), (семья в юриспруденции,...), (семья в педагогике,...)}; (определения семьи, социология) → ∅;
(определения семьи, юриспруденция) → ∅;
(определения семьи, педагогика) → ∅;
(социология, старая школа в социологии) → ∅;
(социология, новая школа в социологии) → ∅;
(юриспруденция, социальные науки) → ∅;
(педагогика, социальные науки) → ∅;
(малая группа, старая школа в социологии) → {(группа людей,...), (кровное родство,...), (брачные отношения,...)};
(малая группа, новая школа в социологии) → {(личные взаимоотношения,...)};
(малая группа, юриспруденция) → {(правовые отношения,...), (группа людей,...)};
(малая группа, педагогика) → {(личные взаимоотношения,...)}; (группа людей, наука) → ∅;
(правовые отношения, социальные науки) → ∅;
(брачные отношения, гуманитарные науки) → ∅;
личные взаимоотношения, педагогика) → ∅;
(личные взаимоотношения, новая школа в социологии) → {(группа людей,...)};
(семья в социологии, социология) → {(малая группа,...)};
(семья в юриспруденции, юриспруденция) → {(малая группа,...), (круг обязанностей,...)};
(семья в педагогике, педагогика) → {(малая группа,...), (отношения поколений семьи,...), (личные взаимоотношения,...)};
(наука, общее знание) → ∅;
(социальные науки, наука) → ∅; (естественные науки, наука) → ∅;
(новая школа в социологии, гуманитарные науки) → ∅;
(старая школа в социологии, гуманитарные науки) → ∅;
(гуманитарные науки, наука) → ∅ .

Литераура

1. PC Week/RE 2003. № 28. С. 10 и № 29. С. 20.
2. *Бениаминов Е.М., Лапшин В.А.* Уровни представлений онтологий, языки, математические модели и проект Веб-сервера онтологий в стиле Веб 2.0 // НТИ. Серия 2. Информационные процессы и системы. 2012. № 3. С. 1–10.
3. *Рубашкин В.Ш.* Онтологическая семантика. Знания. Онтологии. Онтологически ориентированные методы информационного анализа текстов // М.: Физматлит, 2013. 348 с.
4. *Кашевник А.М.* Онтологический подход к контекстно-ориентированному управлению знаниями в интеллектуальной среде // Труды СПИИРАН. 2013. Вып. 1(24). С. 291–302.
5. *Иванов Д.Ю., Новиков Ф.А.* Основы моделирования на UML: Учеб. пособие // СПб.: Изд-во Политехн. ун-та, 2010. 249 с.
6. UML2.5: OMG Unified Modeling Language TM (OMG UML) Version 2.5. URL: http://www.omg.org/spec/UML/2.5/PDF (дата обращения: 10.11.2015).
7. *Горячкин А.А., Зюбин В.Е., Лубков А.А.* Разработка графического формализма для описания алгоритмов в процесс-ориентированном стиле // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2013. Т. 11. № 2. С. 44–54.
8. *Mylopoulos J.* Conceptual modeling and Telos // Conceptual Modeling, Databases, and CASE. Wiley. 1992. pp. 49–68.
9. *Бергер П., Лукман Т.* Социальное конструирование реальности. Трактат по социологии знания // М.: Медиум, 1995. 323 с.
10. *Weber M.* Über einige Kategorien der verstehenden Soziologie // Logos. 1913. vol. 4(3). pp. 253–294.
11. *Guizzardi G., Wagner G., Almeida J.P.A., Guizzardi R.S.S.* Towards Ontologica Foundations for Conceptual Modeling: The Unified Foundational Ontology (UFO) Story // Applied ontology. 2015. vol. 10. no. 3–4. pp. 259–271.
12. *Castells M.* The Rise of the Network Society (The Information Age: Economy, Society and Culture. vol. 1): 2nd ed //. Wiley–Blackwell. 2009. 656 pp.
13. *Doan A., Ramakrishnan R., Halevy A.* Crowdsourcing systems on the World-Wide Web // Communications of the ACM. 2011. vol. 54. no. 4. pp. 86–96.
14. *Gruber T.R.* A Translation Approach to Portable Ontology Specifications // Knowledge Acquisition. 1993. vol. 5(2). pp. 199–220.
15. Энциклопедический социологический словарь. Ред. Осипов Г.В. // М.: ИСПИ РАН, 1995. 665 с.
16. *Харчев А.Г.* Брак и семья в СССР // М.: Мысль, 1979. 214 с.
17. Психология: Онлайн-gopsy // URL:http://gopsy.ru/semja/chto-takoe-semja-opredelenie.html#a_menu (дата обращения: 10.11.2015).
18. Hozo-ontology // URL: http://www.hozo.jp/ (дата обращения: 10.11.2015).
19. Intez //URL: http://www.inttez.ru/ (дата обращения: 10.11.2015).
20. Proteger-2000 // URL: http://protege.stanford.edu/ (дата обращения:10.11.2015).

Каныгин Геннадий Викторович — д-р соц. наук., зав. сектором теории и методологии СИ РАН. Область научных интересов: компьютерные методы в социологических исследованиях, анализ качественных данных, компьютерное ассистирование интервьюированию, онтологические методы управления знаниями. Число научных публикаций — 47. g.kanygin@gmail.com; СИ РАН, ул. 7-ая Красноармейская 25/14, СПб, 190005, РФ; р.т. +7(921)352-1441.

Полтинникова Мария Сергеевна — канд. физ.-мат. наук, старший научный сотрудник сектора теории и методологии СИ РАН. Область научных интересов: динамические системы, размерностные характеристики динамических систем, математическое моделирование, компьютерные методы в социологических исследованиях, онтологические методы управления знаниями. Число научных публикаций — 17; maria.poltinnikova@gmail.com; СИ РАН, ул. 7-ая Красноармейская 25/14, СПб, 190005, РФ; р.т. +7(921)352-1441.

G.V. KANYGIN, M.S. POLTINNIKOVA

CONTEXT-ORIENTED ONTOLOGICAL METHODS IN SOCIOLOGY

Kanygin G.V., Poltinnikova M.S. **Context-Oriented Ontological Methods in Sociology.**

Abstract. The article suggests the context-oriented ontological methods for describing social objects. The methods are based on the graph model of ontology. The model is based on the set of two-level trees, called branches, the vertices of which are pairs of concepts. The first concept of any pair is called term, the second is a context to this term. The rule of linking concepts that serve as contexts is proposed. Algorithms for constructing a graph of the contexts hierarchy as well as a terminological graph are developed. A criterion of logic verification based on the structure of the terminological graph for ontology is obtained. Features of the described model and its usability are exemplified.

Keywords: ontological methods, the context-oriented ontology, branching, context generalization of a concept, graph model, terminological graph, graph of contexts hierarchy.

Kanygin Gennady Victorovich — Dr. Sc. in Sociology, head of Department of Theory and Methodology. Research interests: computer methods for social research, qualitative data analysis, computer assisting interviewing, ontological methods for knowledge management. The number of publications — 47. g.kanygin@gmail.com; SI RAS, 25/14 7-ya Krasnoarmeyskaya str., St. Petersburg, 190005, Russia; office phone +7(921)352-1441.

Poltinnikova Maria Sergeevna Research interests: dynamical systems, dimentional caracteristics of dynamical systems, math. modelling, computer methods for social research, ontological methods for knowledge management. The number of publications — 17; maria.poltinnikova@gmail.com; SI RAS, 25/14 7-ya Krasnoarmeyskaya str., St. Petersburg, 190005, Russia; office phone +7(921)352-1441.

References

1. PC Week/RE 2003. no. 28. p. 10, and no. 29. p. 20.
2. Beniaminov E.M. Lapshin V.A. [Levels of Presenting Ontologies, Languages, Mathematical Models, and Ontology Web-Server Project in Web 2.0]. *NTI. Seriya 2. Informacionnye processy i sistemy – STI. Series 2. Information processes and systems.* 2012. no. 3. pp. 1–10 (In Russ).
3. Rubashkin V.Sh. Ontologicheskaja semantika. Znanija. *Ontologii. Ontologicheski orientirovannye metody informacionnogo analiza tekstov* [Ontological semantics. Knowledge. Ontologies. Ontology-oriented methods of information analysis of texts]. Moscow: Fizmatlit, 2013. 348 p. (In Russ.).
4. Kashevnik A.M. [Ontological approach for context-oriented knowledge management in smart environment]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2013. vol. 1(24). pp. 291–302. (In Russ.).
5. Ivanov D.Ju., Novikov F.A. *Osnovy modelirovanija na UML: Ucheb. posobie* [Fundamentals of modeling UML: Textbook]. St. Petersburg: Izd-

vo Politehn. un-ta, 2010. 249 p. (In Russ.).
6. UML2.5: OMG Unified Modeling Language TM (OMG UML) Version 2.5. Available at: http://www.omg.org/spec/UML/2.5/PDF (accessed 10.11.2015).
7. Gorjachkin A.A., Zjubin V.E., Lubkov A.A. [Development of graphical formalism to describe algorithms in process-oriented style]. *Vestnik Novosibirskogo gosudarstvennogo universiteta. Serija: Informacionnye tehnologii – Bulletin of the Novosibirsk State University. Series: Information Technology*. 2013. vol. 11. no. 2. pp. 44–54. (In Russ.).
8. Mylopoulos J. Conceptual modeling and Telos. *Conceptual Modeling, Databases, and CASE.* Wiley. 1992. pp. 49–68.
9. Berger P., Lukman T. *Social'noe konstruirovanie real'nosti. Traktat po sociologii znanija* [Social Construction of Reality. A treatise on the sociology of knowledge]. Moscow: Medium, 1995. 323 p. (In Russ.).
10. Weber M. U¨ber einige Kategorien der verstehenden Soziologie. *Logos*. 1913. vol. 4(3). pp. 253–294.
11. Guizzardi G., Wagner G., Almeida J.P.A., Guizzardi R.S.S. Towards Ontological Foundations for Conceptual Modeling: The Unified Foundational Ontology (UFO) Story. *Applied ontology*. 2015. vol. 10. no. 3–4. pp. 259–271.
12. Castells M. The Rise of the Network Society (The Information Age: Economy, Society and Culture. vol. 1): 2nd ed. Wiley–Blackwell. 2009. 656 pp.
13. Doan A., Ramakrishnan R., Halevy A. Crowdsourcing systems on the World- Wide Web. *Communications of the ACM*. 2011. vol. 54. no. 4. pp. 86–96.
14. Gruber T.R. A Translation Approach to Portable Ontology Specifications. *Knowledge Acquisition*. 1993. vol. 5(2). pp. 199–220.
15. *Jenciklopedicheskij sociologicheskij slovar'* [Sociological Encyclopedic Dictionary]. Osipov G.V. (ed.). Moscow: ISPI RAN, 1995. 665 p. (In Russ.).
16. Harchev A.G. *Brak i sem'ja v SSSR* [Marriage and family in the Soviet Union]. Moscow: Mysl', 1979. 214 p. (In Russ.).
17. *Psihologija Onlajn-gopsy* [Psychology Online-gopsy]. Available at: http://gopsy.ru/semja/chto-takoe-semja-opredelenie.html#a_menu (accessed 10.11.2015). (In Russ.).
18. Hozo-ontology. Available at: http://www.hozo.jp/ (accessed 10.11.2015).
19. Intez. Available at: http://www.inttez.ru/ (accessed 10.11.2015).
20. Proteger-2000. Available at: http://protege.stanford.edu/ (accessed 10.11.2015).

УДК 338.24; 330.4 **DOI** 10.15622/sp.48.7

В.В. Карасев, Е.Д. Соложенцев

ГИБРИДНЫЕ ЛОГИКО-ВЕРОЯТНОСТНЫЕ МОДЕЛИ ДЛЯ УПРАВЛЕНИЯ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ

Карасев В.В., Соложенцев Е.Д. **Гибридные логико-вероятностные модели для управления социально-экономической безопасностью.**

Аннотация. В развитие работ лауреатов Нобелевской премии Дж. Бьюкенена и Дж. Хекмана предлагается новый подход к анализу и управлению экономической безопасностью социально-экономических систем (СЭС) на основе новой научной дисциплины «топ-экономика». Вводится понятие «невалидность» в экономике по аналогии с «риск» в надежности в технике. Введены новые булевы события-высказывания и новые ЛВ-модели риска для управления экономической безопасностью.
В логико-вероятностных (ЛВ) моделях риска СЭС учитываются: инициирующие события (ИС), зависящие от государства, бизнеса, науки и общества, а также сигнальные события об изменениях в экономике, политике, праве и законах, инновациях, о стихийных бедствиях и войнах, об изменении ситуации на мировом рынке для коррекции вероятностей ИС.

Выполнены обобщения по разработке гибридных ЛВ-моделей для оценки и анализа риска неуспеха СЭС. Определены свойства, достоинства и особенности невалидности и «топ-экономики»; разработаны примеры гибридных ЛВ-модели риска неуспеха следующих СЭС: противодействие коррупции, противодействие наркотизации населения, управление системой инноваций страны.
Приведены примеры сценариев неуспеха субъектов (правительства, бизнеса, ученых и общества), решающих проблему, и объектов (задач), составляющих суть проблемы. Изложены структурные, логические и вероятностные модели риска неуспеха СЭС. Описаны программные комплексы Expa (для синтеза вероятностей событий в гибридных ЛВ-моделях по экспертной информации) и Арбитр (для структурно-логического моделирования гибридных ЛВ-моделей риска).

Ключевые слова: гибридные ЛВ-модели риска, социально-экономические проблемы, коррупция, наркотизация, система инноваций, топ-экономика, невалидность.

1. Введение. В работах лауреатов Нобелевской премии Джеймса Бьюкенена [1] и Джеймса Хекмана [2] рассматриваются связи экономики и политики в развитии государства на основе теории игр и анализа статистических данных.

В развитие этих работ предлагается новый подход к анализу и управлению экономической безопасностью социально-экономических систем (СЭС) на основе топ-экономики [3, 4]. Рассматриваются связи экономики, государства, политики, бизнеса, науки и общества. В ЛВ-модели риска учитываются: инициирующие события, зависящие от государства, бизнеса, науки и общества, а также сигнальные события об изменениях в экономике, политике, праве, инновациях, о стихийных бедствиях и войнах, об изменении ситуации на мировом

рынке для коррекции вероятностей инициирующих событий (ИС) в ЛВ-модели риска СЭС.

Топ-экономика имеет унифицированную систему моделей, методов, технологий и специальные *Software* для управления социально-экономической безопасностью СЭС. Для обозначения этой унифицированной системы знаний и методов, базой которых служат ЛВ-модели риска и ЛВ-исчисление, предлагается название «топ-экономика». Научная и практическая значимость «Топ-экономики» определяется ее достоинствами и особенностями по сравнению с макроэкономикой и микроэкономикой.

Существует следующая иерархия социально-экономических систем и проблем: большие СЭС (страны), социально-экономические проблемы стран, СЭС государства. В настоящей работе подробно рассматриваются апробированные ЛВ-модели риска для управления экономической безопасностью СЭС государства на примере России. Эти системы существуют в реальности, понятны населению страны. С помощью ЛВ-моделей оценивают и анализируют риск невалидности СЭС и ежегодно выделяют ресурсы для управления невалидностью.

В СЭС ведущей является гибридная ЛВ-модель риска неуспеха, но для всестороннего анализа безопасности систем используются также ЛВ-модели риска невалидности, концептуальные ЛВ-модели для прогнозирования и индикативные ЛВ-модели опасности системы.

Описания СЭС приведены в работе [3]. Группа СЭС-1, первостепенной важности для государства, направлена на уменьшение потерь средств и увеличение их поступления. Группа СЭС-2 содержит комплексные СЭС государства и регионов, зависящие от нескольких министерств и законодательных органов. Группа СЭС-3 содержит локальные СЭС для компаний, успех которых зависит в основном от их желаний и возможностей.

Цель работы — обобщить технологии разработки гибридных ЛВ-моделей для оценки и анализа риска неуспеха СЭС.

Задачи работы:

– описать свойства, достоинства и особенности невалидности и «топ-экономики»;

– разработать гибридные ЛВ-модели риска неуспеха следующих СЭС: противодействие коррупции; противодействие наркотизации населения; управление системой инноваций страны;

– привести сценарии неуспеха субъектов (правительства, бизнеса, ученых и общества), решающих проблему, и объектов (задач), составляющих суть проблемы;

– привести структурные, логические и вероятностные модели риска неуспеха гибридных ЛВ-моделей риска неуспеха СЭС;

– описать программный комплекс *Expa* для синтеза вероятностей событий в гибридных ЛВ-моделях по экспертной информации;

– описать программный комплекс *Арбитр* для структурно-логического моделирования гибридных ЛВ-моделей риска;

– сделать обобщения по разработке и использованию гибридных ЛВ-моделей риска.

2. Основные положения «Топ-экономики». Научная дисциплина «Топ-экономика» (Top-economics), или «Управление экономической безопасностью» включает в себя следующие компоненты [3, 4]:

1. *Методы:* понятие невалидности в экономике, ЛВ-исчисление с булевыми событиями-высказываниями;

2. *Модели:* Гибридные ЛВ-модели риска неуспеха решения проблем, ЛВ-модели невалидности, концептуальные ЛВ-модели прогнозирования, индикативные модели опасности состояния СЭС.

3. *Технологии Управления Риском* в СЭС [5];

4. *Задачи*: оценка, анализ, прогнозирование и управление риском в СЭС;

5. *Объекты управления*: группы СЭС-1, СЭС-2, СЭС-3;

6. *Специальные программные средства* [6, 7].

7. *Примеры приложений.*

Определение невалидности. Необходимость разработки специальной науки о невалидности систем возникла из-за появления задач оценки качества систем и изделий по требованиям ВТО и управлению состоянием и развитием СЭС.

Наряду с бытовым пониманием слова «невалидность» как отклонение параметров системы от заданных, для количественной ее оценки требуется научное определение термина невалидность. Невалидность (invalidity) — это событие, после возникновения которого система может выполнять заданное назначение, но с потерей качества.

Невалидность в экономике рассматривается как событие по аналогии с отказом в надежности и как состояние системы с пониженным качеством [2, 3]. Невалидность имеет много состояний-значений в интервале (0, 1). Значение невалидности рассматривается как вероятность события невалидности. Для невалидности сформулированы следующие определения:

1. В отличие от отказа в технике, невалидность имеет не два значения (отказ и не отказ, 0 и 1), а множество значений (multi-state) на интервале (0, 1).

2. Международный стандарт и ГОСТ Р ИСО 9000—2001 использует по существу термины «валидность» и «невалидность» для оценки качества выполняемых работ, оказываемых услуг, производства продукции, систем управления.

3. Невалидность системы — это отклонение ее состояния от значения, заданного техническим заданием и техническими условиями. Невалидность показателя системы — это отклонение его значения от заданного или нормативного.

4. Невалидность состояния рассматривается как событие-высказывание, которому сопоставлена логическая переменная. Степень или характеристика невалидности имеет значения в интервале (0, 1) и рассматривается как риск или вероятность состояния системы.

5. Невалидность системы как события вычисляется по невалидности ее показателей.

6. Если параметр const, то он не рассматривается как событие в состоянии системы. Например, «число женщин» есть параметр const в текущем состоянии СЭС «Рождаемость в стране».

7. ЛВ-модели невалидности разных СЭС можно объединять в одну модель логическими операциями *AND, OR, NOT*.

Субъективное и объективное в невалидности. В практической деятельности возникают затруднения в оценке невалидности и безопасности [8]. По одному и тому же факту могут быть разные суждения относительно невалидности системы. Что здесь объективно, а что субъективно? Всякую систему можно описать конечной совокупностью требований, которым она должна удовлетворять. Составление совокупности требований связано с деятельностью некоторых лиц и, следовательно, является субъективным актом, зависящим от полноты знаний о системе, опыта и других фактов.

Несмотря на субъективный характер установления требований к системе, в любой момент времени должна быть зафиксирована совокупность этих требований, по отношению к которой можно объективно судить о невалидности системы. В этом и состоит диалектика субъективного и объективного в оценке невалидности.

Достоинства и особенности топ-экономики. Научная и практическая значимость топ-экономики для управления социально экономической безопасностью определяется ее достоинствами и особенностями по сравнению с микро- и макроэкономикой:

1. Целевое управление экономической безопасностью осуществляют по критерию риска с оценкой возможных потерь.

2. Возможность построения ЛВ-модели невалидности системы по параметрам одного состояния системы.

3. Новые типы ЛВ-моделей невалидности могут быть использованы для одной СЭС для всестороннего анализа и управления ее экономической безопасностью.

4. Топ-экономика имеет междисциплинарный характер, ибо рассматривает экономические, социальные и информационные аспекты управления безопасностью.

5. Управление экономической безопасностью СЭС имеет комплексный характер, так как зависит от нескольких министерств, ведомств и органов.

6. Связь ЛВ-моделей риска состояния разных СЭС осуществляется через повторные ИС, которые входят в ЛВ-модели риска разных СЭС.

7. Динамичность ЛВ-моделей риска СЭС обеспечивается коррекцией вероятностей ИС при появлении новых статистических данных о состояниях системы и сигнальных событий.

Объекты топ-экономики. Объектами топ-экономики являются социально-экономические системы (СЭС) следующих групп:

Группа СЭС-1 содержит СЭС наивысшей важности для государства, направленные на уменьшение потерь средств и увеличение их поступления [3, 4]:

1) Управление состоянием системы инноваций страны.

2) Противодействие взяткам и коррупции.

3) Противодействие наркотизации страны.

4) Управление резервированием капитала банков по *Базель III.*

5) Управление качеством систем и продукции по *ВТО.*

6) Мониторинг и управление процессом кредитования банков.

Группа СЭС-2 включает в себя комплексные СЭС для государства и регионов, зависящие от нескольких министерств, ведомств и законодательных органов, например, следующие: ЛВ-модель риска состояния рождаемости в стране, ЛВ-модель риска неуспеха решения проблемы образования, ЛВ-модель риска неуспеха решения проблемы информатизации и др.

Группа СЭС-3 включает в себя локальные СЭС для компаний и фирм, успех которых зависит в основном от их желаний и возможностей, например, следующие: ЛВ-управление риском и эффективностью ресторана «Престиж»; ЛВ-модели риска неуспеха

менеджмента компании ЗАО «Транзас», ЛВ-модели риска компании «Логвин Роуд+Рэйл Рус».

Заметим, что в микро- и макроэкономике не решаются задачи управления экономической безопасностью социально-экономических систем групп СЭС-1, СЭС-2, СЭС-3.

Новые типы событий-высказываний в экономике. Введены новые типы булевых событий, являющиеся высказываниями и имеющими вероятности истинности. Совокупность предложений (высказываний) образует сложное производное событие. Фактически, положения стандартов, инструкций, требований и прогнозов сформулированы как предложения, имеющие вероятность истинности, успеха или опасности. В управлении экономической безопасностью СЭС по критерию риска для событий используют вероятности успеха/неуспеха, опасности/неопасности, валидности/невалидности.

Вклад выдающихся ученых Дж. Буля, П. Порецкого, С. Бернштейна, А. Колмогорова и В. Гливенко в ЛВ-исчисление для оценки надежности технических систем оценил И. Рябинин [8]. В развитие ЛВ-метода мы вводим новые виды событий-высказываний: неуспех субъектов, сигнальные события, события невалидности, концептуальные события, индикативные события [3, 4]:

1) События-высказывания о неуспехе решения трудной проблемы субъектом: государством, бизнесом, банками, учеными, общественным мнением.

2) Сигнальные события-высказывания в экономике, политике, праве и законах, инновациях, изменениях на мировом рынке используют для коррекции вероятностей ИС.

3) События-высказывания о невалидности — это высказывания об отклонении показателей от заданных значений. Показатели нормированы и принимают значения в интервале (0, 1). Событие-высказывание о невалидности имеет риск, равный самому показателю.

4) Концептуальные события-высказывания прогнозируют развитие системы. Вероятности истинности событий-высказываний оценивают по экспертной информации.

5) Индикативные события-высказывания рассматриваются как невалидные события. Их мерой опасности является отклонение значений параметра от заданных.

6) События-высказывания о латентности. Вероятности событий-высказываний оценивают по результатам общественных опросов и информации социальных сетей.

Новые типы ЛВ-моделей риска. На основе событий-высказываний введены новые типы ЛВ-моделей риска СЭС [3, 4]:

1. Гибридные ЛВ-модели риска неуспеха решения социально-экономических проблем. Их строят на основе сценария риска для субъектов, участвующих в решении проблемы, и сценария риска для объектов-задач, составляющих суть проблемы.

2. ЛВ-модели невалидности строят по невалидным событиям.

3. Концептуальные ЛВ-модели прогнозирования риска состояния или развития системы. Они строятся на основе описаний специалистов, понимающих суть проблемы.

4. Индикативные ЛВ-модели опасности системы строят по невалидным индикативным показателям.

Эти новые типы ЛВ-моделей риска могут быть использованы для всестороннего анализа и управления экономической безопасностью СЭС-1, СЭС-2 и СЭС-3.

Концептуальная ЛВ-модель рассмотрена на примере ЛВ-модели прогнозирования развития наркотизации [3]. Общая концептуальная ЛВ-модель прогнозирования развития объединяет шесть процессов (ЛВ-моделей). Концептуальная ЛВ-модель прогнозирования каждого процесса развития является Л-объединением ИС-высказываний. Их риски оценивают по экспертной информации.

Индикативная ЛВ-модель опасности состояния СЭС. Состояния СЭС описывают набором показателей. Например, состояние системы инноваций описывают 84 показателя, состояние наркотизации страны — 40 показателей [3]. Наборы показателей позволяют сравнивать разные страны и устанавливать их рейтинги. Не все показатели могут быть индикаторами опасности системы, но по ним строят идикативные показатели опасности.

Невалидная ЛВ-модель состояния системы. Рассмотрим построение ЛВ-моделей риска невалидности СЭС на примере системы Y, которая может иметь опасные состояния $Y_1,\ldots,Y_6$. Обозначим опасные состояния событиями и логическими переменными с теми же идентификаторами. Состояния вызывают невалидные параметры $Z_1,\ldots,Z_{11}$, которые могут быть неприемлемыми или опасными и рассматриваются как инициирующие для появления невалидных состояний $Y_1,\ldots,Y_6$. Невалидные состояния $Y_1, Y_2,\ldots,Y_6$ вызываются ($\leftarrow$) невалидными параметрами: $Y_1 \leftarrow Z_3,Z_8,Z_9,Z_{10}$; $Y_2 \leftarrow Z_1,Z_5,Z_6,Z_{11}$; $Y_3 \leftarrow Z_1,Z_4,Z_5,Z_{10}$; $Y_4 \leftarrow Z_2,Z_3,Z_8,Z_5,Z_{11}$; $Y_5 \leftarrow Z_4,Z_7,Z_9,Z_{10}$; $Y_6 \leftarrow Z_2,Z_6,Z_8,Z_{11}$. Сценарий, например невалидного состояния Y_1 зависит от $Z_3 \wedge Z_8 \wedge Z_9 \wedge Z_{10}$. Связь невалидных состояний системы с невалидными параметрами записывается таблицей связей, и строятся логическая и вероятностная модели риска невалидного состояния СЭС.

В гибридной ЛВ-модели риска неуспеха СЭС участвуют субъекты: правительство, бизнес, ученые, общественное мнение.

Гибридные ЛВ-модели риска неуспеха СЭС включают в себя также объекты (задачи), составляющие суть проблемы. Ниже гибридные ЛВ-модели рассматриваются для СЭС-1.

Событие-высказывание о неуспехе субъекта представляется в виде логического сложения событий «Отсутствие желания» и «Отсутствие возможностей». Некоторые субъекты не желают решения проблемы. Лауреат Нобелевской премии Дж. Бьюкенен показал, что государство склонно сотрудничать с коррупцией и преступностью. Необходимы желания и возможности общественного мнения (в лице оппозиции, демократии, газет и телевидения), чтобы заставить правительство работать в интересах людей. Общественное мнение выражается также депутатскими запросами и демонстрациями.

Важная роль при построении гибридных ЛВ-моделей риска отводится сценариям, которые используются также для оценки вероятностей событий-субъектов и событий-объектов методом рандомизированных сводных показателей [9].

3. Гибридные ЛВ-модели риска СЭС. *Гибридная ЛВ-модель риска противодействия коррупции.* Сценарий неуспеха решения этой социально-экономической проблемы (difficulty problem) формулируется так (рисунок 1) [3]: неуспех решения трудной проблемы *DP* происходит из-за неуспеха субъектов (subjects) *S* и неуспеха объектов (objects) *T*.

Неуспех события-высказывания *S* зависит от субъектов S_1, $S_2,\ldots,S_5$ (правительства, бизнеса, служб противодействия экономическим преступлениям, ученых, общественного мнения). Неуспех события *T* зависит от объектов — решения задач T_1, T_2, T_3. Здесь *DP*, *S*, *T*, S_1, $S_2,\ldots$, S_5, T_1, T_2, T_3 — события неуспеха и соответствующие Л-переменные.

Логические функции неуспеха событий:

$$DP = S \wedge T; \quad S = S_1 \vee S_2 \vee \ldots \vee S_5; \quad T = T_1 \vee T_2 \vee T_3. \tag{1}$$

В-функции неуспеха событий:

$$P\{DP = 0\} = P\{S = 0\} \bullet P\{T = 0\}; \tag{2}$$

$$P\{S = 0\} = P\{S_1 = 0\} + P\{S_2 = 0\}(1 - P\{S_1 = 0\}) + P\{S_3 = 0\}(1 - P\{S_1 = 0\})(1 - P\{S_2 = 0\}) + \ldots;$$

$$P\{T = 0\} = P\{T_1 = 0\} + P\{T_2 = 0\}(1 - P\{T_1 = 0\}) + P\{T_3 = 0\}(1 - P\{T_1 = 0\})(1 - P\{T_2 = 0\}).$$

ЛВ-модель риска неуспеха субъектов. Риск неуспеха события S зависит от риска неуспеха субъектов (рисунок 1): Государства S_1, Бизнеса S_2, Служб экономических преступлений S_3, Ученых S_4, Общественного мнения S_5. События-субъекты связаны логической операцией *ИЛИ* и обозначаются логическими переменными S_1, S_2, S_3, S_4, S_5. Событие неуспеха субъектов S_j будем представлять как сложное событие в виде логического сложения событий «отсутствие желаний» W_j и «отсутствие возможностей» O_j, имеющих вероятности.

Если принять риски неуспеха субъектов S_1, S_2, S_3, S_4, S_5 равными $P_1=P_2=\ldots=P_5=0.5$, то риск неуспеха события S велик, $P\{S=0\} = 0,97$.

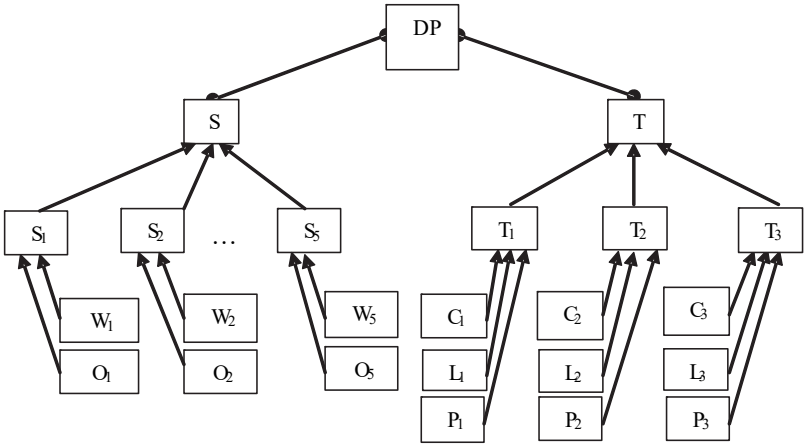


Рис. 1. Структурная модель риска неуспеха решения проблемы коррупции

Объекты гибридной ЛВ-модели риска следующие: T_1 — ЛВ-модель коррупции учреждения, выдающего разрешения или ресурсы; T_2 — ЛВ-модель мошенничества и воровства сотрудников, T_3 — ЛВ-модель взяток при обслуживании [3, 5]. Последовательно для каждого i-объекта строят сценарий риска неуспеха C_i, Л-модель риска неуспеха L_i и В-модель риска P_i, что оказывается часто трудоемким процессом.

Приведем сценарии риска неуспеха решения проблемы, необходимые для экспертной оценки вероятностей неуспеха P_1, P_2, P_3, P_4, P_5 субъектов S_1, S_2, S_3, S_4, S_5.

Государство. Это аппарат президента, правительство, Государственная Дума (ГД) и Совет Федераций (СФ). Желание W_1 решить проблему проявляется в многочисленных заявлениях своих руководителей, обещаниях и создании разных комиссий. Возможности O_1 решить проблему ограничены, ибо государственные органы не

имеют знаний о моделировании риска. Кроме того, существует проблема коррупции.

Бизнес. Взятка касается взяткодателя и взяткополучателя, каждый имеет свою выгоду. Взяткодатель решает свою проблему быстрее, получает привилегии, обходит закон. Взяткополучатель имеет денежную или материальную выгоду. Желания бизнеса W_2 — делать деньги как можно больше, быстрее, любыми способами и выжить в конкурентной борьбе. Однако бизнес заинтересован в стабильных правилах игры для снижения риска разорения. Государство удерживает бизнес в цивилизованных границах.

Службы экономических преступлений устраивает существующая система с оперативно-розыскными мероприятиями, дающая немалый доход.

Ученые создали ЛВ-модели риска мошенничеств чиновников и менеджеров, афер с инвестициями, построили модель риска взяток в учреждении, выдающем ресурсы и разрешения, и модель выявления взяток чиновников по анализу параметров обслуживания.

Общественное мнение имеет желание W_5 решить проблему взяток и коррупции. Свои возможности оно осуществляет через средства массовой информации (телевидение, газеты) через проведение митингов, демонстраций и т.д. Без изменения политики государства и поведения бизнеса, привлечения ученых и общественного мнения актуальную для страны проблему не решить.

Гибридная ЛВ-модель риска неуспеха противодействию наркотизации рассмотрена без учета и с учетом коррупции [3].

ЛВ-модель риска без учета коррупции. Гибридная ЛВ-модель риска неуспеха решения проблемы наркотизации объединяет сценарии риска для субъектов и объектов. Неуспех решения проблемы DP_{nar} зависит от субъектов $S_{nar}(S_1,S_2\ldots,S_{11})$, принимающих участие в решении проблемы, и объектов — задач $T_{nar}(TN_{1,},\ldots,TN_6)$, составляющих суть проблемы (рисунок 2, правая часть).

Проблему решают субъекты: S_1 — Президент; S_2 — Правительство; S_3 — ГД; S_4 — СФ; S_5 — Прокуратура; S_6 — Федеральная служба по контролю за оборотом наркотиков; S_7 — Федеральная таможенная служба; S_8 — Федеральная служба безопасности; S_9 — Органы здравоохранения и социального развития; S_{10} — Ученые; S_{11} — Общественное мнение.

Объектами являются: TN_1 — система мониторинга наркоситуации; TN_2 — гибридные ЛВ-модели риска неуспеха решения проблемы наркотизации; TN_4 — концептуальная ЛВ-модель риска прогнозирования

наркотизации; TN_5 — индикативная ЛВ-модель опасности наркотизации; TN_6 — методики ЛВ-анализа и управления риском.

Обозначим DP_{nar}, S_{nar} , T_{nar}, S_1, $S_2,\ldots,S_{11}$, TN_1, $TN_2,\ldots,TN_6$ как события и соответствующие Л-переменные. Сценарий неуспеха решения этой трудной проблемы DP_{nar} формулируется так: неуспех события DP_{nar} происходит из-за неуспеха событий S_{nar} и событий T_{nar} .

Логические функции неуспеха событий:

$$DP_{nar} = S_{nar} \wedge T_{nar};\ \ S_{nar} = S_1 \vee S_2 \vee \ldots \vee S_{11};$$
$$T_{nar} = TN_1 \vee TN_2 \vee \ldots \vee TN_6. \tag{3}$$

Вероятностные функции неуспеха событий:

$$P\{DP_{nar} = 0\} = P\{S_{nar} = 0\} \bullet P\{T_{nar} = 0\}; \tag{4}$$

$$P\{S_{nar} = 0\} = P\{S_1 = 0\} + P\{S_2 = 0\}(1 - P\{S_1 = 0\}) +$$
$$+P\{S_3 = 0\}(1 - P\{S_1 = 0\})(1 - P\{S_2 = 0\}) + \ldots;$$

$$P\{T_{nar} = 0\} = P\{TN_1 = 0\} + P\{TN_2 = 0\}(1 - P\{TN_1 = 0\}) +$$
$$+P\{TN_3 = 0\}(1 - P\{TN_1 = 0\})(1 - P\{TN_2 = 0\}) + \ldots$$

Составляются сценарии для субъектов ЛВ-модели риска, в которых учитываются их желания и возможности. Для моделей риска объектов разрабатываются сценарии, логические и вероятностные модели риска.

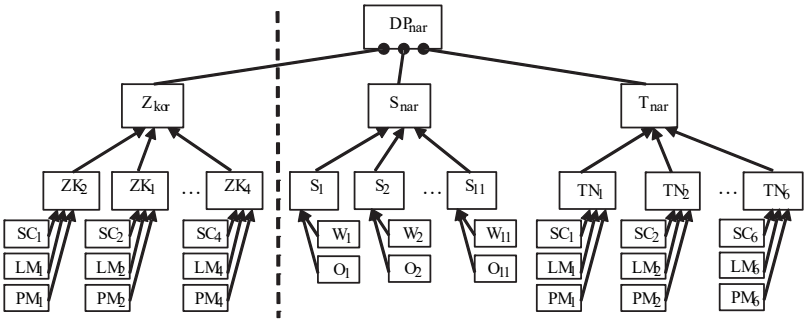


Рис. 2. Структурная модель риска неуспеха решения проблемы наркотизации

Государство $S_1 – S_4$. Это президент, правительство, ГД, СФ.

Блок $S_5 — S_9$. Это Прокуратура, ФС по контролю за оборотом наркотиков и др.

Ученые S_{10} создали ЛВ-модели для противодействия наркотизации регионов и противодействию коррупции.

Общественное мнение S_{11} имеет желание W_{11} решить проблему наркотизации страны. Свои возможности O_{11} оно осуществляет через оппозицию, средства массовой информации (телевидение, газеты), проведение митингов, демонстраций и т. д.

Объекты гибридной ЛВ-модели риска. Задачам TN_1, $TN_2,\ldots,TN_6$ соответствуют ЛВ-модели риска. Последовательно для каждой i-задачи строят сценарий SC_i, Л-модель LM_i и В-модель риска PM_i. В задачах используются статистические данные.

ЛВ-модель риска неуспеха с учетом коррупции. Структурная модель риска неуспеха противодействию наркомании с учетом противодействия коррупции приведена на рисунке 2 (левая и правая часть рисунка). Она логически объединяет ЛВ-модель противодействия наркомании и задачи противодействия коррупции субъектов S, принимающих участие в решении проблемы. Левая часть схемы заимствована из ЛВ-модели риска неуспеха противодействия коррупции Z_{kor}. ЛВ-модель содержит следующие задачи-события: ZK_1 — создание системы мониторинга коррупции в субъектах; ZK_2 —противодействие коррупции в учреждении и ZK_3 — мошенничеству чиновников; ZK_4 — противодействие взяткам при обслуживании.

Далее нужно записать Л-модели риска, выполнить их ортогонализацию, получить соответствующие В-модели риска неуспеха противодействию наркотизации.

Гибридная ЛВ-модель риска неуспеха системы инноваций объединяет сценарии риска для субъектов и объектов [3]. Неуспех решения этой проблемы DP_{inn} зависит от субъектов $S_1,S_2,\ldots,S_5$, *участвующих* в решении проблемы, и задач $T_{inn}(T_1,T_2,T_3)$ составляющих проблемы (рисунок 3).

Субъекты, принимающие участие в решении проблемы инноваций: S_1 — Государство (президент, правительство, ГД, СФ); S_2 — Бизнес, S_3 — Банки, S_4 — Ученые, S_5 — Общество.

Задачами, составляющими суть проблемы, являются: T_1 — выделение характеристик системы поддержки инноваций в стране; T_2 — создание концептуальной ЛВ-модели риска развития системы поддержки инноваций; T_3 — создание индикативной ЛВ-модель риска разработки и внедрения конкретной инновации; создание ЛВ-модели невалидности системы наркотизации.

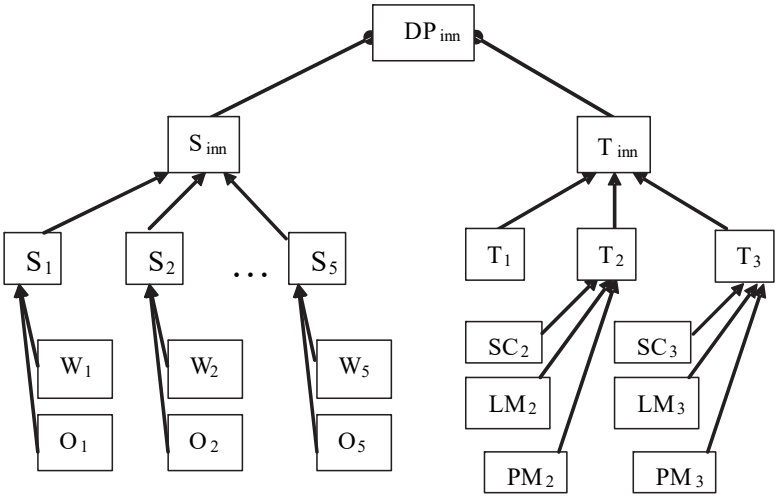


Рис. 3. Гибридная ЛВ-модель риска проблемы инноваций

Вероятности инициирующих событий $S_1, S_2, ..., S_5, T_1, T_2, T_3$ оцениваются методом рандомизированных сводных показателей по нечисловой, неточной и неполной экспертной информации (ННН-информации) [6, 9]. Составляются сценарии для субъектов ЛВ-модели риска, в которых учитываются их желания и возможности. Для моделей риска объектов-задач разрабатываются структурные, логические и вероятностные модели риска.

Приведем сценарии для субъектов, принимающих участие в решении проблемы инноваций, которые будем использовать для построения ЛВ-моделей риска и оценки вероятностей событий по ННН-экспертной информации.

Государство S_1. Это Президент, Правительство, ГД, СФ. Желание W_1 решить проблему государство проявляет в многочисленных декларативных заявлениях своих руководителей, обещаниях и создании постановлений и законов. Возможности O_1 решить проблему ограничены из-за отсутствия знаний и ресурсов.

Бизнес S_2. Желание W_2 бизнеса — зарабатывать как можно больше, быстрее, любыми способами и выжить в конкурентной борьбе. Бизнес поддержит те инновации, которые в краткосрочной перспективе принесут ему прибыль. Государство как регулятор может обязывать бизнес отчислять часть прибыли в фонд инноваций.

Банки S_3. Желание W_3 банков — зарабатывать как можно больше и выжить в конкурентной борьбе. Банки заинтересованы дать

кредит под инновации, которые без риска принесут ему прибыль. Государство как регулятор может обязывать банки отчислять часть прибыли в фонд инноваций.

Ученые S_4 создали для анализа и управления системой инноваций гибридную и индикативную ЛВ-модели, а также соответствующие программные комплексы.

Общественное мнение S_5. Риски неуспеха событий, зависящих от «отсутствие желаний» и «отсутствие возможностей» у субъектов разные. Некоторые субъекты могут не желать решения проблемы. Необходимы желания и возможности ученых и общественного мнения бороться с непрофессиональным правительством.

4. Специальное математическое обеспечение безопасности. *Концепции и принципы* управления социально-экономической безопасностью СЭС:

1) Принцип управления по критерию риска с оценкой потерь;

2) Концепция социальной справедливости в обществе Нобелей: значительную часть прибыли они тратили на рабочих: платили достойную зарплату, строили дома, детские сады и школы, обеспечивали бесплатные медицинские услуги, повышали квалификацию рабочих, вкладывали средства в науку и инновации;

3) Концепция китайского руководства (Ли Кэцян), заключающаяся в том, что ставится знак равенства между инновациями технологическими и инновациями в управлении, в том числе государственном;

4) Принцип управления развитием системы как сложным объектом с движением по заданной программной траектории и коррекцией в случае отклонения от нее;

5) Принцип управления по сигнальным событиям с коррекцией вероятностей инициирующих событий ЛВ-моделей риска СЭС.

Новая математика в ЛВ-моделях риска. В топ-экономике используются следующие новые математические методы и алгоритмы:

1. Понятие «невалидность» в экономике по аналогии с отказом в надежности в технике, но имеющая много значений (multi-state).

2. Новые булевы события-высказывания в экономике: события неуспеха субъектов (государства, бизнеса, ученых, общественного мнения); сигнальные события (в экономике, политике, праве, инновациях, стихийных бедствиях и изменениях на мировом рынке); события невалидности систем; концептуальные события-высказывания прогнозирования риска; индикативные события-высказывания опасности системы; события-высказывания о латентности опросов и информации социальных сетей; несовместные события.

3. Логико-вероятностное исчисление.

4. Новые ЛВ-модели риска с событиями-высказываниями: гибридные ЛВ-модели риска неуспеха в управлении СЭС; ЛВ-модели невалидности систем, концептуальные ЛВ-модели прогнозирования состояния систем; индикативные ЛВ-модели опасности систем.

5. Метод сводных рандомизированных показателей для синтеза вероятностей событий.

6. Методы построения, анализа и управления риском СЭС.

7. Метод нелинейной идентификации для задач с большим числом вещественных оцениваемых переменных (около ста) и целочисленным критерием оптимизации.

8. Доказательство невозможности сформировать тестирующие выборки в задачах классификации объектов, заданных показателями с градациями.

9. Алгоритм исключения некорректных и устаревших данных в задачах классификации объектов.

10. Алгоритм управления предприятиями по вкладам случайных событий в «хвосты» распределения параметра эффективности.

11. Алгоритм замены ЛВ-модели риска в задаче классификации после формирования и анализа сигнальных партий объектов.

12. Алгоритм перехода от ЛВ-модели эффективности к ЛВ-модели прогнозирования риска в пространстве состояний.

13. Формула Байеса при ограниченном количестве информации.

14. Специальные software Expa и Arbiter для вычислений и лабораторных работ по учебному курсу «Топ-экономика».

15. Преобразование любой базы данных (БД) в базу знаний (БЗ) — систему логических уравнений для задач риска.

16. Связь ЛВ-моделей риска СЭС с внешней средой через сигнальные события-высказывания.

17. Связь ЛВ-моделей риска разных СЭС через повторные инициирующие события.

Специальное математическое обеспечение технологии управления социально-экономической безопасностью и основы ЛВ-исчисления должны изучаться студентами и специалистами.

Синтез вероятностей событий в экспертной системе. В технологии ЛВ-управления риском состояния и развития СЭС, когда нет других данных, оценивают вероятности событий по ННН-экспертной информации [6, 9]. Динамичность ЛВ-моделей риска СЭС обеспечивается коррекцией вероятностей ИС в следующих случаях:

- – появление новых данных о состояниях системы;
- появление сигнальных событий в экономике, политике, праве;

– повышение квалификации персонала;
– изменение ситуации на мировом рынке;
– проведение реформ в образовании, науке и экономике.

Метод рандомизированных сводных показателей используют для синтеза вероятностей ИС по ННН-информации. Эксперт не может дать точную оценку вероятности события. Он сделает это точнее и объективнее, если будет оценивать 2-4 альтернативные гипотезы и учитывать их весомости (эксперта «раскачивают»).

Формулируют гипотезы $A_1, A_2, ..., A_n$. Весовые коэффициенты гипотез $w_1, w_2, ..., w_n$ отсчитывают дискретно с шагом $h = 1/n$, , где n — число градаций весомости гипотез (например, n = 50). То есть весомости принимают значения из множества

$$\{0,\ 1/n,\ 2/n, ...,\ (n-1)/n,\ 1\}. \tag{7}$$

Множество $W(m,n)$ всех возможных векторов весовых коэффициентов равно:

$$W(m,n) = N_1 N_2 ... N_m, \tag{8}$$

где $N_1, N_2, ..., N_m$ — число градаций в весовых коэффициентах.

Экспертную информацию по весомостям задают в виде ординальной порядковой информации и интервальной информации.

Ординальная порядковая экспертная информация:

$$OI = \{w_i > w_j, w_r = w_s; i, j, r, s \in \{1, ..., m\}\}. \tag{9}$$

Интервальная экспертная информация:

$$II = \{a_i \le w_i \le b_i;\ i \in \{1, ..., m\}\}. \tag{10}$$

Объединенную экспертную информацию называют нечисловой, неточной и неполной (ННН). Выполняется также условие:

$$w_1 + w_2 + ... + w_m = 1. \tag{11}$$

Условия (9–11) выделяют область допустимых значений весовых коэффициентов $w_1, w_2, ..., w_n$. В качестве числовых оценок весовых коэффициентов используют математические ожидания рандомизированных весовых коэффициентов, а точность этих оценок измеряют при помощи стандартных отклонений.

Вычисления повторяют для двух и более экспертов. Составляют таблицу оценок весовых коэффициентов гипотез от всех экспертов. Вычисляют весовые коэффициенты $w_1^*, w_2^*, ..., w_n^*$ гипотез $A_1, A_2, ..., A_m$ по данным таблицы и весомостям самих экспертов.

Динамичность гибридных ЛВ-моделей риска неуспеха. Динамичность гибридных ЛВ-моделей риска неуспеха СЭС обеспечивается коррекцией вероятностей ИС при появлении новых статистических данных о состояниях системы, сигнальных событий об изменениях в экономике, политике, в законах, в инновациях; изменении ситуации на мировом рынке; проведении реформ в образовании, науке и экономике [3, 4, 10–12]. Эти данные получают от системы мониторинга. Коррекцию вероятностей выполняют один или несколько экспертов с использованием системы *Expa.*

5. Специальные Software для гибридных ЛВ-моделей риска *Expa* для синтеза вероятностей событий. Применение метода рандомизированных сводных показателей из-за перебора большого числа вариантов сопряжено с вычислительными сложностями. Для преодоления этого создано Software *Expa* [6].

Внешний вид программного комплекса в режиме определения переменных представлен на рисунке 4.

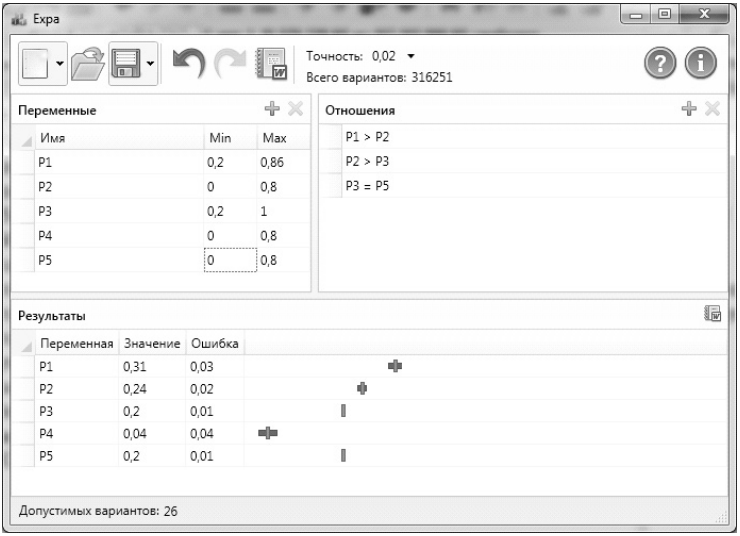


Рис. 4. Программа *Expa.* Синтез вероятностей альтернатив:1 – раздел переменных; 2 – раздел отношений; 3 – раздел результатов расчетов

Термин «переменная» используется для общности. Алгоритм работы следующий:

– В разделе 1 (окне) вводится перечень переменных.

– В том же разделе назначаются допустимые интервалы (интервальная информация).

– В разделе 2 вводятся отношения (ординальная информация).

– В строке управления назначается точность моделирования (0,01; 0,02; 0,04; 0,05) и автоматически вычисляется число возможных вариантов решения (316251).

Производится запуск вычислений, результаты выводятся в разделе 1. Возможно также построение отчёта в формате *Word*.

Сводные оценки от множества экспертов выполняются в последовательности (рисунок 5):

– В разделе 4 вводится перечень экспертов;

– Назначаются допустимые интервалы для весов каждого эксперта (колонки);

– В разделе 5 вводятся значения оценок от каждого эксперта.

– В разделе 6 задаются отношения предпочтения для экспертов.

– Назначается точность моделирования (0,01; 0,02; 0,04; 0,05).

– Запуск вычислений, результаты выводятся на экран (рисунок 6).

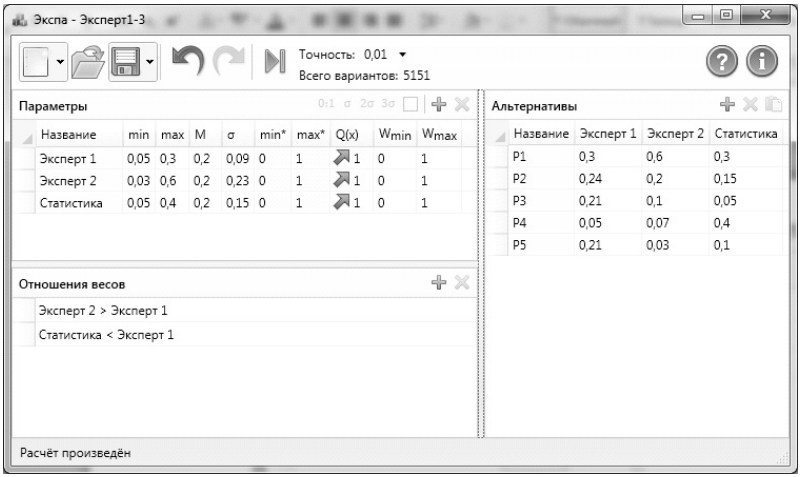


Рис. 5. Программа *Expa*. Получение сводных оценок от нескольких экспертов: 4 — перечень экспертов; 5 — таблица со значениями оценок от каждого эксперта; 6 — таблица отношений для весов экспертов

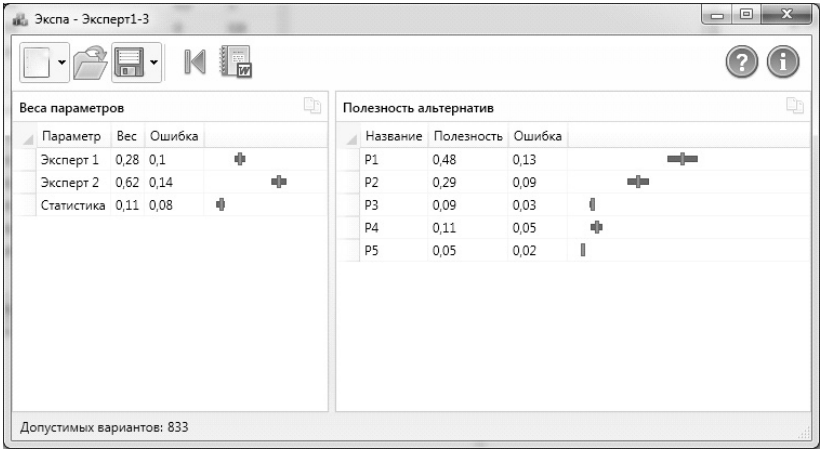


Рис. 6. Программа *Expa* (результаты вычислений для нескольких экспертов): 7 — вычисленные веса экспертов; 8 — сводные оценки вероятностей

Арбитр для структурно-логического моделирования основан на общем ЛВ-методе системного анализа (ОЛВМ) [7] и реализует технологию автоматизированного структурно-логического моделирования сложных систем (рисунок 7).

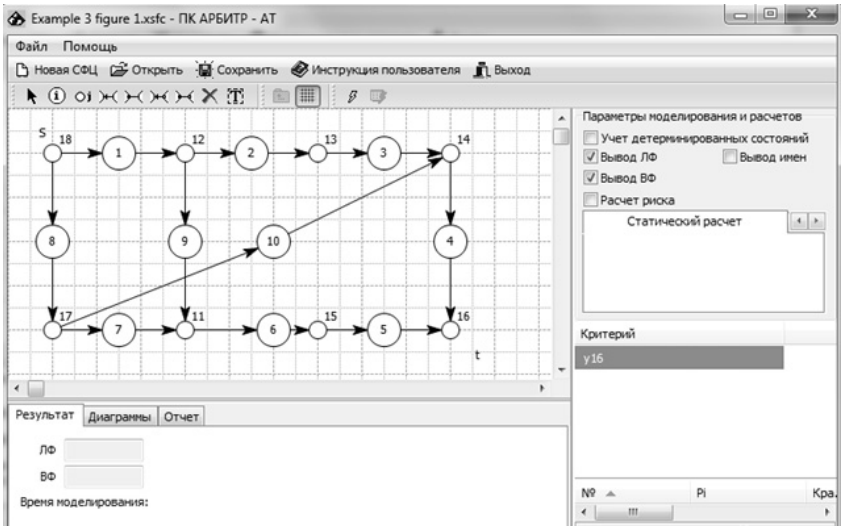


Рис. 7. Основное окно ПК *Арбитр*

Software *Арбитр* аттестован Ростехнадзором РФ в 2007 г. и является первым отечественным программным средством, основанным на ОЛВМ и реализующим новую технологию монотонного и немонотонного ЛВ-анализа (моделирования и расчета показателей) различных свойств надежности и безопасности структурно-сложных системных объектов различного назначения.

Арбитр применяют более 30 организаций России, в том числе 12 высших учебных заведений. Для вузов *Арбитр* поставляется в сетевой версии на 15 рабочих мест на льготных условиях.

6. Пример исследований на ЛВ-модели риска. Выполним количественную оценку и анализ риска неуспеха противодействию коррупции на гибридной ЛВ-модели (рисунок 1). На экспертной системе *Expa* группа из четырех экспертов синтезировала вероятности инициирующих событий (ИС), приведенных в таблицах 1 и 2. Логические переменные для производных событий приведены в таблице 3.

Таблица 1. Риски инициирующих событий W_i, O_i, i = 1, …, 10

Инициирующие события субъектов и объектов, их логические переменные и вероятности									
W_1	O_1	W_2	O_2	W_3	O_3	W_4	O_4	W_5	O_5
Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}
0.4	0.2	0.2	0.3	0.2	0.3	0.4	0.3	0.4	0.3

Таблица 2. Риски инициирующих событий W_i, O_i, i = 11, …, 19

Инициирующие события субъектов и объектов, их логические переменные и вероятности								
C_1	L_1	P_1	C_2	L_2	P_2	C_3	L_3	P_3
Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}	Y_{17}	Y_{18}	Y_{19}
0.05	0.02	0.03	0.05	0.02	0.03	0.05	0.02	0.03

Таблица 3. Обозначение производных событий и логических переменных

События-субъекты и события-объекты	DP	S	T	S_1	S_2	S_3	S_4	S_5	T_1	T_2	T_3
Логические переменные	Y_{30}	Y_{29}	Y_{28}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}	Y_{17}	Y_{18}	Y_{19}

Логическая модель риска неуспеха противодействия коррупции (машинный документ программного комплекса *Арбитр*):

$$Y_{30} = 10.19 + 9.19 + 8.19 + 7.19 + 6.19 + 5.19 + 4.19 + 3.19 + 2.19 + 1.19 + 10.18 + 9.18 + 8.18 + 7.18 + 6.18 + 5.18 + 4.18 + 3.18 + 2.18 + 1.18 + 10.17 + 9.17 + 8.17 + 7.17 + 6.17 + 5.17 + 4.17 + 3.17 + 2.17 + 1.17 + 10.16 + 9.16 + 8.16 + 7.16 + 6.16 + 5.16 + 4.16 + 3.16 + 2.16 + 1.16 + 10.15 + 9.15 + 8.15 + 7.15 + 6.15 + 5.15 + 4.15 + 3.15 + 2.15 + 1.15 + 10.14 + 9.14 + 8.14 + 7.14 + 6.14 + 5.14 + 4.14 + 3.14 + 2.14 + 1.14 + 10.13 + 9.13 + 8.13 + 7.13 + 6.13 + 5.13 + 4.13 + 3.13 + 2.13 + 1.13 + 10.12 + 9.12 + 8.12 + 7.12 + 6.12 + 5.12 + 4.12 + 3.12 + 2.12 + 1.12 + 10.11 + 9.11 + 8.11 + 7.11 + 6.11 + 5.11 + 4.11 + 3.11 + 2.11 + 1.11, \quad (12)$$

где в машинном документе инициирующие логические переменные Y_1 — Y_{19} заданы своими номерами, знак «+» — операция Л-сложения; знак «·» — операция Л-умножения.

Вероятностная модель неуспеха противодействию коррупции, построенная после ортогонализации Л-модели риска (13), следующая:

$$P\{Y30=0\} = P19 + P18.Q19 + P17.Q18.Q19 + P16.Q17.Q18.Q19 + P15.Q16.Q17.Q18.Q19 + P14.Q15.Q16.Q17.Q18.Q19 + P13.Q14.Q15.Q16.Q17.Q18.Q19 + 12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P8.Q9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P7.Q8.Q9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P6.Q7.Q8.Q9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P5.Q6.Q7.Q8.Q9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P4.Q5.Q6.Q7.Q8.Q9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P3.Q4.Q5.Q6.Q7.Q8.Q9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P2.Q3.Q4.Q5.Q6.Q7.Q8.Q9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19 + P1.Q2.Q3.Q4.Q5.Q6.Q7.Q8.Q9.Q10.Q11.Q12.Q13.Q14.Q15.Q16.Q17.Q18.Q19, \quad (13)$$

где P_i — риск i-инициирующего события; $Q_i=1–P_i$; «точка» — знак арифметического умножения и «плюс» знак арифметического сложения (в машинном документе *Арбитр*).

Анализ гибридной ЛВ-модели риска. Значимости и вклады ИС в риск неуспеха системы $P\{Y_{DP}\}$ приведены в таблице 4 для случая конъюнктивной логической связи событий Y_S и Y_T .

Результаты расчетных исследований показали, что основной вклад в риск неуспеха противодействию коррупции и взяткам вносят субъекты $P\{Y_T\}=0.97344$. События-объекты вносят меньший вклад $P\{Y_S\}=0.26351$, так как ученые уже разработали основные методики,

алгоритмы и программное обеспечение. Общий риск неуспеха противодействию коррупции и взяткам равен $P\{Y_{DP}\}=0.256517$. Вклады и значимости инициирующих событий в риск неуспеха (таблица 1, столбцы 3–5), из-за простой структуры модели риска, примерно пропорциональны значениям риска этих событий.

При дизъюнктивной логической связи событий Y_S и Y_T, получены следующие результаты: $P\{Y_T\}=0.97344$; $P\{Y_S\}=0.26351$; $P\{Y_{DP}\}= 0,98044$. Результаты исследований по противодействию коррупции свидетельствуют о необходимости реформ в стране.

Таблица 4. Значимости и вклады инициирующих событий

НомерИС	Риск, P_i	Значимость ИС	Вклад на «-»	Вклад на «+»
1	0.400000	+1.16619E-02	-4.66476E-03	+6.99713E-03
2	0.200000	+8.74642E-03	-1.74928E-03	+6.99713E-03
3	0.200000	+8.74642E-03	-1.74928E-03	+6.99713E-03
4	0.300000	+9.99591E-03	-2.99877E-03	+6.99713E-03
5	0.200000	+8.74642E-03	-1.74928E-03	+6.99713E-03
6	0.300000	+9.99591E-03	-2.99877E-03	+6.99713E-03
7	0.400000	+1.16619E-02	-4.66476E-03	+6.99713E-03
8	0.300000	+9.99591E-03	-2.99877E-03	+6.99713E-03
9	0.400000	+1.16619E-02	-4.66476E-03	+6.99713E-03
10	0.300000	+9.99591E-03	-2.99877E-03	+6.99713E-03
11	0.050000	+7.54663E-01	-3.77331E-02	+7.16930E-01
12	0.020000	+7.31561E-01	-1.46312E-02	+7.16930E-01
13	0.030000	+7.39103E-01	-2.21731E-02	+7.16930E-01
14	0.050000	+7.54663E-01	-3.77331E-02	+7.16930E-01
15	0.020000	+7.31561E-01	-1.46312E-02	+7.16930E-01
16	0.030000	+7.39103E-01	-2.21731E-02	+7.16930E-01
17	0.050000	+7.54663E-01	-3.77331E-02	+7.16930E-01
18	0.020000	+7.31561E-01	-1.46312E-02	+7.16930E-01
19	0.030000	+7.39103E-01	-2.21731E-02	+7.16930E-01

Национальная безопасность. Рассмотрим использование ЛВ-моделей риска для управления национальной безопасностью страны. Связь науки и национальной безопасности исследована в работе [13]. Ведение экономических войн с санкциями описан в работе [3] с использованием ЛВ-моделей невалидности социально-экономического систем страны. Методика основа на анализе значимостей и вкладов ИС в риск системы (таблица 4).

Суть экономической войны состоит в том, что для своих СЭС мы хотим иметь минимальный риск, а противник желает увеличить его. И наоборот, противник хочет иметь минимальный риск своих СЭС, а мы хотим увеличить его.

Для количественного прогнозирования риска экономического состояния от угроз и санкций других стран следует построить ЛВ-модели невалидности СЭС страны и вычислить на них вклады ИС, чтобы установить самые опасные ИС и способы их защиты.

Для количественного прогнозирования риска экономического состояния противодействующей страны от угроз и санкций своей страны следует построить ЛВ-модели невалидности СЭС противоборствующей страны и вычислить на них вклады ИС, чтобы установить опасные ИС, их комбинации и выбрать самые эффективные санкции.

Таким образом, топ-экономика рассматривает не только управление социально-экономической безопасностью, но и некоторые аспекты управления национальной безопасностью страны, а именно:

1. Методика экономических войн с санкциями с использованием ЛВ-моделей риска социально-экономических систем (СЭС).

2. Гибридные ЛВ-модели риска неуспеха следующих значимых СЭС в национальной безопасности страны:

– Противодействие коррупции;

– Противодействие наркотизации;

– Управление системой инноваций страны.

3. Технология построения гибридных ЛВ-моделей для оценки и анализа риска неуспеха сложных систем, процессов и проектов по национальной безопасности страны.

7. Заключение. Основные результаты работы следующие:

1. Сделаны обобщения по разработке гибридных ЛВ-моделей для оценки риска неуспеха социально-экономических систем.

2. Изложены положения невалидности для построения гибридных ЛВ-моделей риска неуспеха СЭС.

3. Описаны гибридные ЛВ-модели риска неуспеха СЭС: противодействие коррупции; противодействие наркотизации населения; управление системой инноваций страны.

4. Обобщена схема построения гибридной ЛВ-модели риска неуспеха СЭС: составляют сценарии неуспеха субъектов, решающих проблему, и неуспеха объектов, составляющих суть проблемы; оценивают вероятности событий-высказываний, строят и анализируют гибридную логико-вероятностную модель риска.

5. Описаны и апробированы программные комплексы *Арбитр* для структурно-логического моделирования и *Expa* для синтеза вероятностей событий-субъектов и событий-объектов.

6. Рассмотрено применение гибридных ЛВ-моделей риска в обеспечении национальной безопасности страны.

7. Полученные результаты позволяют улучшить *у*правление экономикой страны.

8. Гибридные ЛВ-модели риска неуспеха социально-экономических систем нашли практическое применение учебном курсе и лабораторных работах экономического факультета ГУАП.

Литература

1. *Buchanan J.* Selected Works (Death of the West, etc) // Moscow: Alfa Press. 1997.
2. *Heckman J.J., Leamer E.* Handbook of econometrics // Elsevier. 2007. vol. 6. 52 p.
3. *Соложенцев Е.Д.* Топ-экономика. Управление экономической безопасностью. 2-е изд. // СПб: Троицкий мост. 2016. 272 с.
4. *Соложенцев Е.Д.* Невалидность и события-высказывания в логико-вероятностных моделях для управления риском в социально-экономических системах // Проблемы анализа риска. 2015. № 6. С. 30–43.
5. *Соложенцев Е.Д.* Технологии управления риском в структурно-сложных системах: уч. пособие // СПб.: ГУАП. 2013. 435 с.
6. *Алексеев В.А., Карасева Е.И.* Синтез и анализ вероятностей событий по нечисловой, неточной и неполной экспертной информации // Проблемы анализа риска. 2014. № 3. С. 22–31.
7. *Можаев А.С.* Аннотация программного средства "АРБИТР" (ПК АСМ СЗМА) // Научно-технический сборник «Вопросы атомной науки и техники. Серия «Физика ядерных реакторов». М.: РНЦ «Курчатовский институт». 2008. Вып.2. С.105–116.
8. *Рябинин И.А*. Надежность и безопасность структурно-сложных систем: 2-е изд. // СПб.: Изд-во С.-Петерб. ун-та. 2007. 276 с.
9. *Hovanov N., Yadaeva M., Hovanov K.* Multicriteria Estimation of Probabilities on the Basis of Expert Non-numerical, Inexact and Incomplete Knowledge // European Journal of Operational Research. 2007. vol. 195. no. 3. pp. 857–863.
10. *Соложенцев Е.Д., Карасев В.В.* Мониторинг и управление процессом кредитования банка с использованием логико-вероятностных моделей риска // Проблемы анализа риска. 2013. Вып. 10. № 6. С.78–87.
11. *Solozhentsev E.D.* Logic and probabilistic risk models for management of innovations system of country // IJ RAM. 2015. vol. 18. no. ¾. pp. 237–255.
12. *Solozhentsev E.D.* Risk Management Technologies with Logic and Probabilistic Models // Dordrecht, Heidelberg, New York, London: Springer. 2012. 328 p.
13. *Юсупов, Р.М.* Наука и национальная безопасность: 2-е изд., переработанное и дополненное // СПб.: Наука. 2011. 360 с.

Карасев Василий Владимирович — к-т техн. наук, старший научный сотрудник лаборатории интегрированных систем автоматизированного проектирования, Институт проблем машиноведения Российской академии наук (ИПМаш РАН). Область научных интересов: математическая логика, теория вероятностей, комбинаторный анализ, методы оптимизации, теория графов, методы классификации, экспертные системы, моделирование социально-экономических систем, анализ данных. Число научных публикаций — 55. vasily.karasev@gmail.com; Большой пр. В.О., 61, Санкт-Петербург, 199178; р.т.: +7(812)321-4766.

Соложенцев Евгений Дмитриевич — д-р техн. наук, профессор, заслуженный деятель науки Российской Федарации, заведующий лабораторией интегрированных систем автоматизированного проектирования, Институт проблем машиноведения Российской академии наук (ИПМаш РАН), профессор кафедры информационных технологий в бизнесе, ФГАОУВО Санкт-Петербургский государственный университет аэрокосмического приборостроения (СПбГУАП). Область научных интересов: управление риском проектирования, испытаний и эксплуатации систем, технологии управления риском, управление социально-экономической безопасностью систем. Число научных публикаций — 300. esokar@gmail.com, http://www.ipme.ru/ipme/labs/iisad/sol1.htm; Большой пр. В.О., 61, Санкт-Петербург, 199178; р.т.: +7(812)321-4766, Факс: +7(812)321-4771.

V.V. Karasev, E.D. Solozhentsev

HYBRID LOGICAL AND PROBABILISTIC MODELS FOR RISK MANAGEMENT OF SYSTEMS.

Karasev V.V., Solozhentsev E.D. **Hybrid Logical and Probabilistic Models for Risk Management of Systems.**

Abstract. We offer a new approach to analysis and economic safety management in socio-economic systems (SES) on the basis of a new scientific discipline "top-economics" as further development of works by Nobel Prize Laureates J. Buchanan and J. Heckman. We introduce the "invalidity" concept by analogy with reliability and safety in engineering. We use new Boolean events-propositions and new LP risk models for economic safety management.

Logical and probabilistic (LP) risk models of SES take into account initiating events (IEs), which depend on the state, business, science and society, and signal events about changes in economics, politics, law, innovations, natural disasters and wars, global market fluctuations in order to correct probabilities of IEs.

We have performed generalizations in the development of hybrid LP-models for estimation and analysis of SES failure risk. Properties, advantages and features of "invalidity" and "top-economics" have been determined. Examples of the following hybrid LP risk models of SESs have been developed: counteraction to corruption, counteraction to drug addiction, country's innovation system management.

We present examples of scenarios of failure of subjects (government, business, scientists and society) that solve the problem, and objects (tasks) that are the essence of the problem. Structural, logical and probabilistic risk models of SESs failure are stated. Software "Expa" (for synthesis of probabilities of events in hybrid LP-models using expert information) and "Arbiter" (for structural and logical modeling of hybrid LP risk models) are described.

Karasev Vasily Vladimirovich — Ph.D., senior researcher of intellectual integrated systems of automated design laboratory, Institute of Problems of Mechanical Engineering of Russian Academy of Sciences (IPME RAS). Research interests: logic, probability theory, combinatorial analysis, optimization methods, graph theory, classification methods and expert systems, socio-economic system modeling, data analysis. The number of publications — 55. vasily.karasev@gmail.com; 61, Bolshoy pr. V.O., Saint-Petersburg, 199178, Russia; office phone: +7(812)321-4766.

Solozhentsev Eugene Dmitrievich — Ph.D., Dr. Sci., professor, Honoured Worker of Science of Russian Federation, head of intellectual integrated systems of automated design laboratory, Institute of Problems of Mechanical Engineering of Russian Academy of Sciences (IPME RAS), professor of information technologies in business Department, St. Petersburg State University of Aerospace Instrumentation. Research interests: modeling, analysis and management of safety and risk on stages of design, testing and operation of engineering and socioeconomic systems. The number of publications — 300. esokar@gmail.com, http://www.ipme.ru/ipme/labs/iisad/sol1.htm; 61, Bolshoy pr. V.O., Saint-Petersburg, 199178, Russia; office phone: +7(812)321-4766, Fax: +7(812)321-4771.

References

1. Buchanan J. Selected Works (Death of the West, etc). Moscow: Alfa Press. 1997.
2. Heckman J.J., Leamer E. Handbook of econometrics. Elsevier. 2007. vol. 6. 52 p.
3. Solozhentsev E.D. *Top-ekonomika. Upravlenie ekonomicheskoy bezopasnostiu* [Top-economics. Economic safety management]. SPb: GUAP. 2015. 256 p. (In Russ.).
4. Solozhentsev E.D. [Invalidity and events-propositions in logical and probabilistic models for risk management in socio-economic systems]. *Problemy analiza riska – Issues of risk analysis.* 2015. vol. 6. pp. 30–43. (In Russ.).

5. Solozhentsev E.D. *Tehnologii upravlenija riskom v strukturno-slozhnyh sistemah. Uch. Posobie* [Risk management technologies in structural mplex systems]. SPb: GUAP. 2013. 435 p. (In Russ.).
6. Alexeev V.F., Karaseva E.I. [Synthesis and analysis of probabilities of events by non-numerical, inaccurate and incomplete information]. *Problemy analiza riska – Issues of risk analysis*. 2014. vol. 3. pp. 22–31. (In Russ.).
7. Mozhaev A. S. [Software “Arbitr” (PK ASM SZMA) annotation]. *Nauchno-tehnicheskij sbornik «Voprosy atomnoj nauki i tehniki. Serija «Fizika jadernyh reaktorov» – Scientific and technical collectiont "Problems of Atomic Science and Technology. "Physics of nuclear reactors" series*. M.: RNC «Kurchatovskij institut». 2008. vol. 2. pp.105–116. (In Russ.).
8. Ryabinin I.A. *Nadezhnost' i bezopasnost' strukturno-slozhnyh system: 2-e izd.* [Reliability and safety of structural complex systems: second edition]. SPb.: Izd-vo S.-Peterb. un-ta. 2007. 276 p. (In Russ.).
9. Hovanov N., Yadaeva M., Hovanov K. Multicriteria Estimation of Probabilities on the Basi of Expert Non-numerical, Inexact and Incomplete Knowledge. *European Journal of Operational Research*. 2007. vol. 195. no 3. pp. 857–863.
10. Solozhentsev E.D., Karasev V.V. [Monitoring and management of the bank lending process with the use of logical and probabilistic risk models]. *Problemy analiza riska – Issues of risk analysis*. 2013. vol. 10. no. 6. pp. 78–87. (In Russ.).
11. Solozhentsev E.D. Logic and probabilistic risk models for management of innovations system of country. *International Journal of Risk Assessment and Management*. 2015. vol. 18. no. ¾. pp. 237–255.
12. Solozhentsev E.D. Risk Management Technologies with Logic and Probabilistic Models. Dordrecht. Heidelberg. New York. London: Springer. 2012. 328 p.
13. Yusupov R. M. *Nauka i nacional'naja bezopasnost': 2-e izd., pererabotannoe i dopolnennoe* [Science and National Security. 2nd edition, revised and enlarged]. SPb.: Science. 2011. 360 p. (In Russ.).

УДК 004.003 **DOI** 10.15622/sp.48.8

О.В. Карсаев

ОБЗОР ТРАДИЦИОННЫХ И ИННОВАЦИОННЫХ СИСТЕМ ПЛАНИРОВАНИЯ МИССИЙ КОСМИЧЕСКИХ АППАРАТОВ

Карсаев О.В. **Обзор традиционных и инновационных систем планирования миссий космических аппаратов**

Аннотация. В статье выполняется обзор традиционных и инновационных систем планирования миссий космических аппаратов, выполняющих задачи наблюдения целевых объектов на Земле и/или в космическом пространстве. В традиционных системах планирования космические аппараты выполняют планы, рассчитанные на Земле. В таком случае возникает ряд объективных недостатков, которые могут существенно ограничивать эффективность использования космических аппаратов и их ресурсов. В статье приводится описание и анализ таких недостатков. Наличие таких недостатков и новые постановки задач, возникающие в связи с тенденцией использования малых космических аппаратов, являются основными причинами развития инновационных методов и систем планирования. Инновационные методы и системы планирования главным об-разом предполагают развитие двух основных возможностей: автономное адаптивное планирование на борту космических аппаратов и информационное взаимодействие между ними. Развитие второй возможности рассматривается как основа для обеспечения адаптивного группового поведения космических аппаратов.

В обзоре рассматриваются примеры инновационных систем планирования, которые либо уже используются в экспериментальных режимах в текущих миссиях, либо находятся на стадии исследований, на уровне компьютерного моделирования. Статья также содержит обзор нескольких перспективных решений в области связи между космическими аппаратами, так как возможность использования таких решений оказывает существенное влияние на постановку задачи планирования миссий космических аппаратов.

Ключевые слова: автономное планирование, информационное взаимодействие, групповое поведение.

1. Введение. В данной статье выполняется обзор работ, позволяющий проиллюстрировать текущее состояние и актуальные направления исследований в области планирования миссий космических аппаратов (КА), выполняющих задачи наблюдения целевых объектов на Земле и/или в космическом пространстве. Под планированием миссий КА подразумевается планирование целевых задач, выполняемых с помощью специальной аппаратуры КА.

Основными источниками являются труды следующих наиболее рейтинговых международных конференций и семинаров. Конференция *International Conference on Space Operations* — очередная, 13-ая по счету, конференция состоится в 2016 году. Конференция *Conference on Small Satellites* признается международным сообществом одной из ведущих конференций по малым КА. Она проводится ежегодно, начиная с 1987 года. В 2015 году состоялась 29-ая по счету конференция. Се-

минар *International Workshop on Planning and Scheduling for Space.* 9-ый по счету семинар прошел в 2015 году. *International Symposium on Artificial Intelligence, Robotics, and Automation for Space.* 12-ый по счету симпозиум прошел в 2014 году.

В обзоре рассматриваются традиционные (существующие и используемые в реальной практике) системы планирования миссий КА и инновационные системы, различие между которыми кратко можно охарактеризовать следующими основными свойствами. В традиционных системах планирование выполняется в наземных комплексах управления (НКУ). Сформированные планы выполнения целевых задач передаются КА, а бортовые комплексы управления (БКУ) КА обеспечивают только выполнение этих планов операций. В инновационных системах планирования БКУ КА уже рассматриваются не только как системы исполнения полученных команд, а также используются для автономного планирования и обработки полученных результатов наблюдений. Это обеспечивает существенное повышение эффективности целевого функционирования КА за счет использования таких возможностей, как распределение или перераспределение целей наблюдения между КА и планирование операций с учетом текущего фактического состояния КА, оперативная коррекция планов операций при появлении новых задач в результате обработки полученных результатов наблюдений и других дополнительных возможностей.

Круг организаций (научных, коммерческих, государственных, военных и др.), заинтересованных в развитии космических исследований, крайне широк. По понятным причинам особую заинтересованность в этих исследованиях имеют различные военные организации и ведомства. В связи с этим следует отметить, что в 2007 году конгрессом США был образован офис для управления программой «*Оперативно реагирующий космос*» (*Operationally Responsive Space*), основной целью которой является обеспечение и координация космических исследований в интересах Министерства обороны США. Общую информацию об этой программе можно найти в статье [1]. В этой статье приводится общее описание организации исследований, а также ретроспективное описание выполненных миссий программы (ORS 1, 2, 3 и 4) и задачи новой миссии ORS-5. В рамках этой миссии в 2017 году планируется запуск группировки малых КА, которые будут обеспечивать решение таких задач, как: тактическая круглосуточная разведка, сбор информации и распознавание целей, радиолокационные наблюдения, обнаружение пуска ракет и обеспечение связи. Разработка решений в области планирования и управления орбитальными группи-

ровками (ОГ) малых КА также является одним из основных направлений исследований в данной программе.

Обзор имеет следующую структуру. В первой части обзора приводится краткое описание традиционных решений. Инновационные решения сгруппированы в рамках трех направлений: автономное планирование, связь и информационное взаимодействие между КА, которые описываются в последующих трех частях обзора. Обзор исследований в области развития связи между КА необходим, так как новые виды и решения организации связи оказывают критически важное влияние на постановку и содержание задач планирования.

2. Традиционное планирование. К настоящему времени существует достаточно много систем планирования, реализующих традиционный подход и используемых на практике для управления различными миссиями. Обзор таких систем (*APSI, ASPEN, EUROPA, flexplan* и других — всего 14) можно найти в работе [2]. В данной работе на примере этих систем приводится обобщенное описание задач и процессов планирования. В рамках этого обобщенного описания содержательный контекст задач представляется в виде совокупности моделей, описывающих свойства и ограничения отдельных элементов и понятий космических систем и КА. Планирование в целом сводится к моделированию процессов и сценариев поведения элементов системы, и целевое функционирование КА при этом представляется в виде множества временных графиков состояния элементов системы, взаимосвязанных между собой. На промежуточных этапах планирования эти графики используются для выявления и устранения конфликтов и нарушений ограничений, а также для оптимизации финального плана выполнения полученных заявок, и рассматриваются в виде основополагающих конструкций систем планирования. В связи с этим в работе основное внимание уделяется анализу и описанию математических моделей и методов, используемых для описания этих конструкций. Краткое описание каждой из систем планирования в работе [2] рассматривается в виде сопоставления с обобщенным описанием задач и процессов планирования.

В качестве примера для иллюстрации и пояснения такого обобщенного представления задач и процессов планирования можно использовать систему планирования *CPAW (Collection Planning & Analysis Workstation)* [3]. Эта система разработана в компании *Orbit Logic* (США). Она используется для планирования различных миссий наблюдения за целевыми объектами на Земле и в космическом пространстве и, в частности, для планирования миссий в интересах военных ведомств США. Система предназначается для планирования функционирования нескольких КА и проведения съемок целевых объ-

ектов с помощью различных средств наблюдения: оптико-электронных, радиоэлектронных, инфракрасных средств наблюдения, радаров с синтезированной апертурой и др.

Контекст задачи планирования в этой системе описывается с помощью совокупности следующих моделей и временных графиков:

– модели камер и моделирование процессов съемки;

– модели КА и моделирование вращений и нацеливания КА;

– модели солнечных батарей и моделирование процессов генерации и потребления электроэнергии;

– модели памяти и моделирование процессов использования памяти и сеансов связи передачи данных наблюдений на Землю;

– модели и моделирование условий освещенности целей в рамках возможных временных интервалов проведения съемок;

– модели и моделирование технологических ограничений и условий использования камер, определяющих необходимые интервалы времени между проведением съемок;

– модели антенн и моделирование процессов передачи данных, моделирование возможностей проведения съемок во время передачи данных на Землю;

– модели и моделирование условий облачного покрова над целевыми районами наблюдений в рамках возможных временных интервалов проведения съемок.

Системы планирования могут разрабатываться для планирования какой-то одной конкретной миссии или различных миссий с учетом различий и специфики разнообразных КА. Преимущества и недостатки таких подходов рассматриваются в работе [4]. Система CPAW разрабатывалась в рамках второго подхода, т.е. предполагается, что она может использоваться для планирования различных миссий и различных КА. В связи с этим в работе [3] кроме достаточно детального описания перечисленных выше моделей также приводится описание возможностей их настройки на специфику различных КА.

Процесс планирования в системе CPAW предполагает решение следующей совокупности задач.

Регистрация заявок. Эта задача включает описание координат целей, а также описание условий и ограничений проведения съемки: допустимые углы разворота КА/камеры, условия освещенности и облачности и др.

Планирование сеансов связи. Планирование сеансов связей выполняется при наличии большого количества КА и наземных станций, когда для наземных станций в одно и то же время существует несколько временных окон видимости разных КА.

Определение горизонта планирования. Выполняется с использованием нескольких различных подходов. В простейшем случае горизонт планирования определяется на основе рассчитанного плана сеансов связей, как интервал времени между двумя последующими сеансами связи. Для разных КА могут выбираться различные горизонты времени планирования.

Фильтрация заявок и целей. Предполагает выбор целей для планирования съемок в выбранном горизонте времени. В рамках фильтрации первоначально выполняется разбиение больших целевых областей на несколько полос. Съемки полос рассматриваются в виде отдельных целей планирования и могут планироваться в разных горизонтах времени планирования. Выбор целей для планирования в заданном горизонте времени выполняется с учетом различных факторов: приоритеты целей, условия съемки, и др.

Планирование съемок целей наблюдения и передачи данных на Землю. Исходными данными для этой задачи являются: горизонт времени планирования КА, план сеансов связей КА и множество целей, выбранных в результате фильтрации и назначенных данному КА. Планирование съемок выполняется совместно с планированием использования памяти КА для регистрации результатов съемок и передачи этих результатов на Землю. Результат решения данной задачи транслируется в план целеуказаний, и передается на борт спутника.

Контроль выполнения съемок. Используется для выявления необходимости повторного планирования съемок целей, которые могут возникать либо после обработки полученных результатов съемок, либо после неуспешных сеансов связей передачи целеуказаний КА. При контроле выполнения съемок учитывается обстоятельство того, что полосы съемки, определенные для выполнения одной заявки, могут также являться частью выполнения других заявок.

Планирование работы нескольких КА выполняется с учетом координации планов различных КА. Целью координации, в частности, является избегание дублирования съемок одних и тех же и/или пересекающихся целей, согласование съемок отдельных полос территориальных целей разными КА, а также распределение целей между КА с учетом анализа факторов, обеспечивающих получение данных с различным уровнем качества. Планирование в системе может выполняться как с участием операторов, так и в полностью автоматическом режиме.

Наряду с обзором систем планирования в данном разделе далее рассматривается ряд отдельных важных аспектов, оказывающих существенное влияние на эффективность решения и/или на постановку задач планирования целевого функционирования КА.

Инкрементальность планирования. В традиционных системах планирование может выполняться в двух режимах: в пакетном режиме и в инкрементальном режиме. В пакетном режиме планирование выполняется несколько раз, как правило, два раза в сутки. Предметом планирования являются три группы заявок: 1) новые заявки; 2) заявки, не включенные ранее в планы и переданные на борт КА; 3) заявки, включенные в эти планы, но по которым получены факты их невыполнения. В инкрементальном режиме планирование выполняется непрерывно. В ходе него выполняется либо оптимизация текущего варианта плана, либо его модификация по мере поступления новых заявок или фактов невыполнения запланированных ранее заявок, а также по мере возникновения других непредвиденных событий, требующих уточнения текущего варианта плана. В системах, используемых на практике, планирование, как правило, выполняется в пакетном режиме. Недостатки пакетного режима и преимущества инкрементального режима планирования достаточно подробно рассматриваются в работе [5]. В обобщенном виде сравнительный анализ результатов планирования, описанный в этой работе, можно сформулировать следующим образом. В случае пакетного режима имеющийся в текущий момент времени план не учитывает новую информацию, которая стала известной после окончания последней сессии планирования. При этом имеющийся план уже может быть недопустимым. Например, если появилась дополнительная информация об отмене запланированного сеанса связи для передачи целеуказаний. Базовой характеристикой этого режима также является то обстоятельство, что в каждой сессии планирование выполняется «с нуля», и не учитываются те результаты планирования, которые уже были получены в ходе предыдущей сессии планирования, в частности, варианты разрешения выявленных конфликтов. При каждой последующей сессии планирования поиск вариантов разрешения уже известных конфликтов происходит заново, но уже с учетом новой информации и разрешения новых выявленных конфликтов. В случае инкрементального режима полагается, что в каждый момент времени текущий вариант плана является допустимым и учитывает всю известную к этому времени информацию.

В этой работе [5] также приводится описание системы инкрементального планирования, которая разрабатывается в Немецком центре космических операций начиная с 2014 года.

Надежность планирования и управления. Задача обеспечения надежности планирования и управления, а также описание подхода к ее решению детально рассматривается в работе [6]. Содержание задачи состоит в следующем. Пусть *t1* и *t2* моменты времени начала двух сеансов связей, *t1* — последнего прошедшего, а *t2* — предстоящего сеан-

са. Предполагается, что планирование выполняется в инкрементальном режиме. Текущий вариант плана называется *мастер планом*. Фрагмент этого плана, переданный на борт КА в ходе последнего сеанса связи, называется *исполняемым фрагментом плана*. Фрагмент исполняемого плана, как правило, рассчитывается на период времени *t1-t2*. После передачи исполняемого фрагмента плана при продолжении планирования изменения в мастер плане возможны начиная с момента времени *t2*. Таким образом, поддерживается синхронизация планирования и управления КА во времени. При неуспешном сеансе связи синхронизация нарушается, так как мастер план содержит фрагмент исполняемого плана, не переданный на КА. В этом случае при продолжении планирования мастер план по-прежнему может корректироваться, начиная с момента времени следующего сеанса связи. Но при этом требуется повторное планирование тех операций, которые были включены во фрагмент исполняемого плана, передача которого оказалась неуспешной. В такой ситуации критически важным фактором становится период времени до следующего сеанса связи с КА. Он может оказаться относительно малым, недостаточным для перепланирования мастер плана и полного восстановления синхронизации. Последовательность сеансов связей, между которыми интервалы времени малы и могут возникать такие ситуации, в статье называется *сессией сеансов связей*. Проблема обеспечения надежности управления главным образом связывается с такими сессиями сеансов связей. При этом сложность этой проблемы существенно вырастает, если планирование выполняется для нескольких КА.

Для обеспечения надежности планирования в этой статье [6] предлагается подход, в котором, исходя из реальной ситуации, на ближайшей период времени определяются все возможные сценарии развития ситуации. Они определяются всеми возможными комбинациями неуспешных сеансов связей, и для каждого возможного сценария рассчитывается соответствующий мастер план. Такой подход требует значительных вычислительных мощностей, так как возможны ситуации, когда необходимо рассчитывать десятки вариантов мастер плана. Поэтому в статье также рассматривается обоснование возможных допущений для снижения числа рассчитываемых мастер планов.

Наземная инфраструктура. Оперативность управления и получения данных съемок определяется количеством и расположением наземных станций приема информации с КА. В связи с этим следует отметить направления исследований по разработке малых и недорогих наземных станций приема информации. В частности, в работе [7] приводится описание портативной переносной наземной станции, разра-

ботанной в интересах программы «Оперативно реагирующий космос». Эта станция может быть развернута в требуемой позиции в течение дня двумя специалистами. Такая же тенденция рассматривается в работе [8], в которой описывается разработка системы сбора метеоданных для составления более точного прогноза погоды. Одним из главных требований в этой системе является обеспечение периодичности (менее часа) сбора данных в различных точках земной поверхности. Для обеспечения этого требования на основе результатов компьютерного моделирования обоснована необходимость формирования системы, состоящей из 100+ наноспутников и 50+ наземных станций. Ввиду большого количества наземные станции проектируются по аналогии с малыми КА, т.е. как малые и недорогие.

Стандартизация информационных процессов планирования и управления. Краткое описание существующих и разрабатываемых стандартов, а также описание сервисов, реализующих эти стандарты, можно найти в работе [9]. Содержательная задача, на примере решения которой в этой работе демонстрируются целесообразность и преимущества таких стандартов и сервисов, в общем виде заключается в следующем. Имеется множество КА, на которых используются различные типы сенсоров. Для управления КА и приема информации с КА используется множество различных наземных станций. Основной целью стандартизации в этом контексте является предоставление заказчикам и потребителям информации КА единого веб-приложения, с помощью которого они могли бы взаимодействовать с различными операторами КА и выбирать наилучшие варианты выполнения своих заявок.

В силу объективных обстоятельств традиционный подход к управлению КА обладает известными объективными недостатками. Основными являются следующие три группы недостатков:

1) Наземное планирование выполняется на основе прогнозирования потребления и восстановления ресурсов КА. В частности, на основе прогнозирования потребления и восстановления энергии и памяти регистрации результатов съемки целевых объектов. Для того чтобы гарантировать выполнимость планируемых операций, необходимо использовать оценки потребления этих ресурсов с определенным запасом. Например, в работе [10] при моделировании потребления свободной памяти для записи данных съемок используются оценки с четырехкратным запасом. Очевидно, что такой подход априори не позволяет использовать возможности КА наилучшим образом, так как в результате выполнения таких планов в реальности возникают простои в использовании сенсоров КА.

2) Традиционный подход предполагает, что основой для управления является наземный план операций, фрагмент которого на ближайший горизонт времени передается на борт спутника в виде командных целеуказаний. В связи с этим в работах [5] и [6] рассматриваются соответственно проблемы инкрементальности и робастности планирования. Инкрементальность, по сути, означает постоянное изменение текущего плана в режиме реального времени в связи со всеми возникающими событиями. Однако в рамках традиционного подхода инкрементальность планирования может быть обеспечена лишь частично, так как информация о событиях, возникающих на борту КА (в частности, фактические данные о выполнении целеуказаний), становится известной с существенным запозданием. Робастность планирования, по сути, должна обеспечивать своевременный расчет и передачу на борт КА оптимального плана целеуказаний с учетом всех исходных данных, известных к текущему моменту времени. Однако при традиционном подходе робастность планирования также может быть обеспечена лишь частично, так как уровень робастности определяется уровнем инкрементальности планирования.

3) Традиционный подход предполагает, что генерация целей и задач наблюдения и формирование исходных данных для планирования выполняется на Земле. Однако потребности в проведении дополнительных съемок целей или съемок новых целей могут генерироваться на борту КА в результате обработки и анализа уже проведенных наблюдений. Очевидно, что в рамках традиционного подхода реакция на возникновение таких потребностей может оказаться слишком запоздалой и не обеспечивать получение необходимых результатов.

На основании перечисленных недостатков эксперты компании SSTL Ltd в работе [4] делают вывод о том, что решение задачи оптимизации плана при наземном планировании практически является бесполезным. К этому выводу следует добавить, что использование группировок малых КА вносит свои существенные специфические уточнения в постановку и содержание задачи планирования. В общей совокупности эти выводы являются причинами активных исследований и развития инновационных подходов к решению задач планирования, которые рассматриваются в оставшейся части обзора.

3. Автономное планирование. Основные преимущества автономного планирования на борту КА предопределяются возможностями использования текущих фактических данных о состоянии КА и его ресурсов, и возможностями реагирования на возникающие события в режиме реального времени. Таким образом, автономное планирование, по сути, также является адаптивным планированием.

Следует отметить, что автономное планирование в настоящее время уже активно применяется в реальной практике в ряде миссий в экспериментальном режиме. Однако, учитывая особенности экспериментальной стадии, в большинстве случаев, как правило, рассматривается возможность использования автономного планирования в комбинации с традиционным наземным планированием. В рамках такого подхода автономное планирование сводится к адаптивному уточнению плана, рассчитанного на Земле.

Также следует отметить, что возможности автономного планирования пока еще используются в ограниченных пределах, так как они напрямую зависят от производительности бортовых процессоров. В частности, в работе [11] отмечается, что производительность бортовых процессоров в большинстве случаев пока еще соответствует уровню, который примерно на два порядка ниже по сравнению с производительностью обычных лэптопов.

Составить представление о текущем уровне развития и использования возможностей автономного планирования позволяют работы, которые далее рассматриваются в этом разделе.

В работе [12] описывается комбинированная система планирования VAMOS (Verification of Autonomous Mission Planning Onboard a Spacecraft), которая разработана в Германском центре космических операций (GSOC — German Space Operations Center). Эта система используется для планирования запущенных в 2015 году спутников Biros (Berlin Infra-red Optical System), на которых установлены системы двуспектральных инфракрасных сенсоров и трехканальных оптических камер. На спутниках также установлены экспериментальные модемы, которые используются для обеспечения дополнительной связи с наземными пунктами управления с использованием спутниковой системы связи OrbComm. На борту спутника выполняется обработка снимков, которая позволяет определять облачность, а также выявлять некоторые типы объектов и событий, например, мосты и наводнения. В миссии предусмотрены три последовательных этапах, на которых планирование будет выполняться в различных режимах. На начальном этапе планирование будет выполняться традиционным образом — на Земле.

Второй и третий этапы по времени запланированы на 2016 год. На втором этапе предполагается проведение экспериментов по использованию автономного планирования с целью оценки возможностей и эффективности коррекции плана операций на основе текущих фактических телеметрических данных, получаемых в режиме реального времени. Коррекция плана операций в рамках этих экспериментов главным образом связывается с контролем свободной памяти.

Априори предполагается, что в процессе выполнения рассчитанного на Земле плана на борту КА могут оставаться значительные объемы свободной памяти, так как при планировании используются оценки потребления свободной памяти для регистрации результатов съемок с определенным запасом. Это позволяет гарантировать регистрацию результатов запланированных съемок, но также позволяет включать в план дополнительные съемки, если фактически объем свободной памяти остается больше запланированных значений. Дополнительные объемы свободной памяти также могут появляться за счет выявления и удаления бесполезных снимков, на которых цели наблюдения скрыты облачным покровом.

В основе автономного планирования на этом этапе используются следующие обстоятельства. Рассчитанный на Земле план представляется в виде множества отдельных фрагментов, каждый из которых описывает последовательность операций для проведения одной съемки. Для каждого фрагмента плана (и соответствующей съемки) также рассчитываются совокупность параметров, определяющих допустимые начальные условия для его (ее) выполнения. В частности, такими параметрами являются интервалы времени видимости цели, оценки минимально необходимого объема свободной памяти и минимально необходимого остатка энергии. На Земле также определяются моменты времени выполнения контроля телеметрических данных. При этом автономное планирование сводится к реализации относительно простой логики последовательного выбора фрагментов плана на определенном горизонте времени на основе проверки выполнимости начальных условий и заданных приоритетов съемок.

На третьем этапе запланированы эксперименты, целью которых является оценка возможностей оперативной коррекции плана съемок при появлении новых целей. В качестве типовых примеров рассматриваются следующие сценарии.

1) На Земле генерируется срочная потребность съемки извержения вулкана. Если первая возможность спутника сделать съемку, т.е. окно видимости цели существует до наступления ближайшего сеанса связи с наземной станцией, тогда спутнику через сеть OrbComm посылаются необходимые данные для оперативного включения в план съемки данной цели.

2) Инфракрасная камера обнаружила пожар, и автономно генерируется потребность в выполнении съемки с высоким разрешением, которая может быть проведена в рамках этого же окна видимости цели за счет отклонения камеры наблюдения под углом назад.

Генерация потребностей и планирование новых съемок в соответствии с рассмотренным подходом предполагает расчет соответствующих фрагментов плана. В рамках третьего этапа расчет таких фрагментов плана выполняется на борту спутника. Для упрощения автономных вычислений на борту спутника используется библиотека заранее заготовленных шаблонов фрагментов плана. С учетом этого формирование фрагмента плана сводится к расчету значений параметров данных фрагментов.

Оперативное добавление в план нового фрагмента выполняется при соблюдении следующих трех условий:

– новый фрагмент не конфликтует с уже активированным (выполняемым) фрагментом плана;

– выполняются начальные условия выполнимости нового фрагмента;

– добавление этого фрагмента плана не влечет удаления из плана последующих съемок с большим приоритетом.

В работе [11] приводится описание комбинирования автономного и наземного планирования передачи информации в наземные пункты. Основным фактором необходимости автономного уточнения наземного плана в данной работе является неопределенность объемов данных наблюдений.

Модель задачи планирования заключается в следующем. Имеется несколько пунктов управления для передачи наземных планов, несколько пунктов приема информации с КА и несколько центров заказчиков, куда выполняется передача полученной информации. При этом Заказчики определяют пункты, через которые может передаваться информация с КА.

Проведение съемки требует нацеливания КА на объект съемки, а передача информации требует только нацеливание антенны КА на наземную станцию. Съемка и передача информации могут производиться параллельно.

Данные съемки записываются в виде нескольких файлов в разные слоты (банки) памяти. Для передачи данных используется несколько каналов связи. Файлы данных одной съемки могут одновременно передаваться по разным каналам с учетом следующих ограничений. Прерывание передачи файла не допускается. Все файлы данных одной съемки должны быть переданы в рамках одного сеанса связи. В канале не допускается чередование файлов разных съемок. Также не допускается пересечение по времени передачи разных файлов, как в каналах связи, так и из слотов памяти.

Каждый потребитель имеет свой ключ шифрования данных. Данные шифруются до передачи их в канал связи из слота памяти. Используется таблица изменений ключей шифрования с задаваемым ограниченным числом изменений. В связи с этим периодически возникает необходимость в изменении ключей шифрования и переустановке этой таблицы. Переустановка таблицы требует определенного времени и прерывания передачи данных по всем каналам в течении этого времени.

Полученные файлы данных из пунктов приема передаются в центры потребителей. При корректной передаче данных центр посылает пункту управления подтверждение, которое далее пересылается спутнику. Пункты управления используются только для передачи планов спутникам и передачи подтверждений о получении данных.

При наземном планировании выполняются раздельно расчет плана съемок и расчет плана передачи данных. Горизонт времени планирования съемок определяется интервалами времени между сеансами связи. План выполнения съемок на борту спутника практически не изменяется. Единственным исключением являются ситуации, когда съемка влечет переполнение памяти. В этом случае съемка выполняется только тогда, когда возможно удалить из памяти данные других съемок с меньшим приоритетом. Не использование автономного уточнения плана съемок обосновывается тем, что это является весьма затратной вычислительной процедурой. На основании плана съемок выбираются окна видимости наземных пунктов для передачи информации. Горизонт планирования передачи информации определяется горизонтом плана съемок. Количественные характеристики плана: 1000+ съемок и 5000+ файлов данных.

Наземное планирование передачи данных выполняется на основе эвристического подхода итеративно в три этапа. На первом этапе определяется последовательность передачи данных съемок. При этом каждой съемке назначается окно видимости пункта приема информации. Эти решения принимаются исходя из минимизации времени старения информации, которое определяется интервалом времени между съемкой и передачей данных съемки в пункт приема.

На втором этапе каждому файлу данных съемок назначается канал связи, и для каждого канала и слота памяти определяется последовательность передачи файлов данных. Последовательность передачи файлов съемки начинается с файлов большего объема. Распределение файлов данных съемки между каналами связи выполняется исходя из минимизации времени простоя каналов связи, которые могут возникать из-за перечисленных выше ограничений.

На третьем этапе выполняется расчет сроков начала и окончания передачи файлов данных, сроков перенацеливания антенны КА на пункт приема информации, сроков переустановки таблицы изменений ключей шифрования, и проверяются все ограничения. Если какое-либо ограничение нарушается, для соответствующей съемки выбирается другое окно видимости или другая позиция в последовательности передачи съемок. Если решение не найдено, съемка удаляется из плана передачи данных.

При планировании выполняется расчет нескольких вариантов плана передачи данных, из которых выбирается наилучший. В первом варианте порядок вставки съемок в план определяется с учетом следующих эвристических правил. Предпочтение имеют съемки с большим приоритетом, а при равном приоритете предпочтение имеют более ранние съемки. Для расчета каждого последующего варианта плана порядок вставки изменяется следующим образом. Позиция съемки в последовательности передачи сдвигается вперед пропорционально разности времени старения результатов данной съемки и среднего времени старения результатов других съемок с таким же приоритетом.

План передачи данных на Земле рассчитывается исходя из оценок максимального объема данных съемок с высоким приоритетом и оценок ожидаемых объемов данных съемок с низким приоритетом. Автономное уточнение плана на борту спутника выполняется с учетом фактических объемов данных и с учетом следующих правил. Передача данных съемок с высоким приоритетом может выполняться в запланированных или в более ранних окнах видимости пунктов приема информации. Передача данных съемок с низким приоритетом может выполняться в любых окнах видимости, в частности, в более поздних.

С учетом этих правил на борт спутника посылаются план передачи данных FP и упорядоченный список съемок CL, не включенных в план передачи данных. План передачи данных посылается в виде множества $FP = \{<A, W, C, L>\}$, где A — съемка, W — окно видимости передачи данных этой съемки. C — параметризованное правило изменения окна видимости для передачи этой съемки: 0 — окно может изменяться произвольно, 1 — окно не изменяется, и 2 — передача съемки возможна в более ранних окнах видимости. L — самый поздний срок начала передачи данных съемки, если $C > 0$.

Алгоритм автономного планирования разработан с учетом того, что производительность стандартного бортового процессора примерно на два порядка ниже производительности обычного компьютера. Суть данного алгоритма в общем виде состоит в следующем. Исполняемый план передача данных съемок изначально формируется в хронологиче-

ском порядке, определенном в наземном варианте плана. Поскольку фактические объемы данных съемок априори меньше используемых оценок, которые учитывались при наземном планировании, могут возникать простои в использовании каналов связи. Алгоритм пытается заполнить этот простой вставкой передачи данных другой съемки, либо из списка *CL*, либо последующих по порядку съемок из плана *FP*. Такая вставка выполняется только в том случае, если она не влечет ситуацию, когда передача последующих по порядку данных съемок с более высоким приоритетом становится невозможной.

В рассматриваемой статье [11] приведены экспериментальные оценки моделирования работы системы на основе реалистических исходных данных за 1 день функционирования КА. Параметры эксперимента: 1 спутник, 5 слотов памяти, 3 канала связи, 2 уровня приоритетов съемок, 1364 съемки и 6820 файлов, 23 пункта приема данных и 115 окон видимости. Фактические объемы файлов генерировались случайным образом в интервале $[V^{max}/4 \ldots V^{max}]$. Полученные экспериментальные оценки показывают существенное увеличение эффективности работы системы, которое, в частности, измеряется следующим соотношением. Автономное уточнение наземного плана позволяет обеспечить увеличение количества передаваемых данных в среднем с 700 до 1100 съемок.

Описанный в статье подход к автономному планированию в настоящее время используется во Французском космическом агентстве для компьютерного моделирования и проектирования космической системы. Цель — определение сбалансированных значений параметров системы: количество линий передачи данных спутника, объем передаваемых в день данных, объем памяти на борту спутника, количество и расположение наземных пунктов приема информации.

В работе [13] описывается система автономного планирования спутника MiRaTa (Microwave Radiometer Technology Acceleration). Планирование в данном случае является полностью автономным. Содержание задачи планирования главным образом определяется моделью состояний спутника. Он может находиться в одном из пяти состояний: *сбор данных, разворот, простой, передача данных, подзарядка батарей.*

В состоянии «сбор данных» спутник производит целевые измерения, для чего выполняет типовой маневр — медленное вращение по углу тангажа от 0 до 105 градусов и обратно. В этом состоянии спутник, как правило, может находиться от 22 до 30 минут. Возможные интервалы времени, когда спутник может производить измерения, определяются условиями взаимного расположения с GPS спутниками. Измерения возможны, когда как минимум 3 спутника GPS находятся в

зоне видимости спутника MiRaTa. В состоянии «разворот» выполняются необходимые развороты спутника для установления требуемой ориентации для подзарядки батарей или для передачи данных в пункт приема информации.

Процесс планирования выполняется перманентно через каждые 20 минут. В рамках каждой сессии планирования строится план на заданный горизонт времени. Определение оптимального горизонта времени планирования рассматривается в качестве основной цели в описываемых в работе экспериментах.

Планирования начинается с того, что на основе имитационного моделирования в рамках установленного горизонта планирования определяются временные окна, когда спутник может находится в состояниях «сбор данных», «передача данных» и «подзарядка батарей». На основании этих данных определяется начальная последовательность состояний, включая расчет времени начала каждого состояния и длительности нахождения спутника в этом состоянии. Постановка данной задачи сводится к задаче смешанного целочисленного и линейного программирования. В качестве критериев планирования рассматривается максимизация суммарного времени нахождения в каждом из состояний «сбор данных» и «передача данных», и максимизация среднего запаса энергии на интервале планирования. В расчетах используются переменные, описывающие скорость потребления и восстановления ресурсов (памяти и энергии) в каждом из пяти состояний спутника.

Построенный на этом шаге план может содержать нарушения ограничений по использованию энергии и памяти. Если таковые нарушения есть, выполняется «древовидный» поиск вариантов его модификации в виде множества планов-наследников. План-наследник формируется добавлением в начальный/текущий вариант плана дополнительных состояний «передача данных» и/или «зарядка батарей», и, соответственно, необходимых в связи с этим дополнительных состояний «разворот» или «простой».

В процессе планирования выполняется поиск нескольких вариантов плана по описанному выше сценарию. Поиск нового варианта плана предполагает модификацию начальной последовательности состояний и повторение описанной процедуры поиска. Модификация начального плана выполняется в соответствии со следующими правилами. Начальный вариант плана содержит все те же состояния «сбор данных», как и в предшествующем варианте. Но если в предшествующей итерации допустимый вариант план не найден, то удаляется одно или несколько состояний «сбор данных» с наименьшими временными окнами. Поиск каждого варианта плана ограничивается временем — 25 секунд.

В работе [14] описывается концепция системы автономного планирования, которая разрабатывается в компании Orbit Logic в рамках контракта с Исследовательской лабораторией ВВС США (US AFRL). Система планирования CPAW, разработанная в этой же компании и реализующая традиционный подход [3], была рассмотрена в первой части обзора.

По аналогии с ранее рассмотренной работой [12] полагается, что планирование может выполняться в трех режимах: полностью автономном, полуавтономном и традиционном режиме, когда планирование выполняется в наземном варианте. Полуавтономный режим предполагает, что спутник функционирует в соответствии с наземным планом, но при этом система автономного планирования может отдавать приоритет операциям, решение по которым принимается автономно в качестве ответных мер на обнаруженные события. В качестве начальных примеров для разработки пилотного прототипа системы рассматриваются следующие 3 ситуации:

1) Средство обзорного наблюдения спутника обнаруживает на поверхности Земли целевой объект до момента времени, когда он попадает в зону видимости радиолокационного радара с синтезируемой апертурой. В этом случае система планирования включает в план операцию наблюдения данного объекта радиолокационным радаром, рассчитывая оптимальные параметры луча выполнения съемки с учетом координат объекта.

2) В непосредственной близости со спутником обнаружен надвигающийся объект, например, космический мусор. Во избежание столкновения с этим объектом спутнику необходимо выполнить коррекцию орбиты.

3) Средства наблюдения спутника обнаружили космический объект. Для его идентификации спутник автономно принимает решение о проведении съемки обнаруженного объекта на следующем витке орбиты. Для этого необходимо рассчитать и включить в план последовательность необходимых для этого операций: нацеливание спутника на объект, настройка и включение средства наблюдения требуемого типа, регистрация данных съемки в памяти спутника, и передача данных съемки этого объекта в пункт приема информации.

Архитектура системы разрабатывается на основе многоагентного подхода. В архитектуре рассматривается один агент, мастер автономного планирования (агент MAPA), и коллекция агентов специализированного автономного планирования (агенты SAPA), которые планирует последовательности операций для выполнения целевых задач соответствующего типа. Далее эти последовательности операций об-

рабатываются МАРА агентом с целью выявления и разрешения конфликтов и уточнения итогового плана операций спутника.

Концепция системы автономного планирования предполагает использование информационного взаимодействия между спутниками. Однако в рамках данной работы этот аспект только упоминается, но детально не рассматривается.

4. Межспутниковая связь. Ограниченные возможности связи являются критическим фактором в обеспечении эффективности управления и использования спутников. Низкоорбитальные спутники генерируют значительные объемы информации, один спутник в день может генерировать до нескольких терабайт данных. Передача такого объема данных по технологии радиолиний становится проблематичной, так как для спутника в день может существовать одно или в лучшем случае несколько довольно узких временных окон для передачи данных наземной станции, а максимальная скорость передачи данных по радиоканалу составляет всего лишь порядка 300 мегабит/сек.

Возможности разрешения этой проблемы связываются с использованием геостационарных спутников ретрансляторов и перспективных видов связи, например, связи в оптическом диапазоне. В частности, в работе [15] приводятся следующие оценки. Такой канал связи обеспечивает передачу данных между низкоорбитальным и геостационарным спутником со скоростью до 1.8 Гигабит/сек. При этом геостационарный спутник ретранслятор способен передавать наземной станции в день до 16.2 терабайт информации. Другим существенным преимуществом оптического канала связи является его высокая надежность с точки зрения защищенности от перехвата. Это преимущество достигается благодаря узкому лучу оптической связи. На расстоянии между низкоорбитальным и геостационарным спутниками диаметр пятна луча оптической связи составляет приблизительно 360 метров, а диаметр пятна луча радиосвязи приблизительно 160 км. Кроме этого бортовая аппаратура оптической связи имеет существенно меньшие требования к объему, энергии и массе.

О текущем состоянии развития и перспективах практического использования оптической связи можно судить по следующим работам. В работе [16] приводится описание успешных испытаний оптической связи между спутником, находящимся на лунной орбите, и наземной станцией. В продолжение этих экспериментов в настоящее время проводятся разработки и экспериментальные исследования группировки спутников ретрансляторов TDRS (Tracking and Data Relay Satellites), запуск которых планируется на 2018 год.

В работе [15] приводится описание текущего состояния разработки Европейской спутниковой системы ретрансляции данных EDRS (European Data Relay System). На первом этапе разработки этой системы на спутниках устанавливались лазерные терминалы, которые обеспечивали связь между низкоорбитальными спутниками и связь этих спутников с наземными станциями. Второе поколение этих терминалов обеспечивает связь между низкоорбитальными и геостационарными спутниками и между геостационарными спутниками и наземными станциями. Для экспериментальных исследований такие терминалы были установлены на геостационарный спутник Alfasat, запущенный в 2013 году, и низкоорбитальный спутник Sentinel-1A, предназначенный для наблюдения земной поверхности, запущенный в 2014 году. Первый геостационарный спутник системы EDRS был выведен на орбиту в январе 2016 [17]. Запуски еще трех спутников запланированы на период времени с 2017 до 2020 годов.

Использование оптических каналов связи влечет определенное усложнение задачи планирования. Эти усложнения связаны с физическими свойствами оптических каналов связей и технологией установления таких каналов. Физические свойства заключаются в том, что использование оптической связи между ретранслятором и наземной станцией зависит от состояния атмосферы. Например, такая связь невозможна в условиях облачности. В качестве возможных путей преодоления таких ограничений рассматривается использование нескольких наземных станций, чтобы всегда иметь гарантированный канал оптической связи хотя бы с одной станцией, или передача части данных по менее скоростному радиоканалу.

Установление оптического канала связи между спутниками требует определенного времени, поэтому начинается за несколько минут до начала передачи данных. Установление связи выполняется в соответствии с определенным технологическим сценарием, в соответствии с которым каждый из спутников производит нацеливание луча лазера на другой спутник. Эта операция в качестве необходимых исходных условий предполагает, что каждый спутник обладает данными для определения текущей позиции спутника респондента, и чем точнее эти данные, тем быстрее устанавливается связь. Связь Земли с геостационарным спутником ретранслятором существует в режиме реального времени, поэтому передача файлов целевых указаний этому спутнику может выполняться либо непосредственно перед сеансом связи, либо заранее. Передача же файла целевых указаний низкоорбитальному спутнику возможна лишь тогда, когда он находится в зоне видимости наземной станции. В связи с этим планирование сеансов связей по оп-

тическому каналу выполняется в условиях двух противоречивых критериев. С точки зрения планирования работы спутника расчет времени сеансов связи должен выполняться как можно раньше. С точки зрения обеспечения более высокой точности исходных данных для установления оптического канала связи, чем позднее выполнятся этот расчет, тем лучше, точность данных выше.

Описанный выше подход к использованию оптических каналов связей в работе [18] трактуется как «использование оптических линий по технологии радиолиний, т.е. в виде отдельных сеансов связей», и подвергается критическому анализу. Вывод этого анализа в целом состоит в том, что такой подход не даст повышения оперативности получения потребителем целевой информации за счет использования оптических линий связи.

Для обоснования этого вывода в статье приводится описание и сравнительный анализ технологических операций, последовательность которых предопределяет интервал времени выполнения заявки (время между поступлением заявки и доставкой результатов наблюдений конечному потребителю). Сравниваются ожидаемые оценки времени выполнения заявок при использовании радио и оптической связи. При этом рассматривается вариант работы оптических линий отдельными сеансами связи.

Для достижения наибольшей эффективности использования оптической связи в этой работе предлагаются иные принципы проектирования и функционирования орбитальной аппаратуры оптической связи, в соответствии с которыми аппаратура должна работать автоматически, автономно и непрерывно. В соответствии с этими принципами полагается, что все необходимые расчеты навигационного обеспечения рассчитываются на борту спутника. Связь между геостационарными и низкоорбитальными спутниками поддерживается постоянно. Низкоорбитальный спутник переключается с одного спутника-ретранслятора на другой, а геостационарный спутник-ретранслятор, оснащенный несколькими терминалами аппаратуры оптической связи, может связываться одновременно с несколькими низкоорбитальными спутниками. Прерывание связи, вызываемого затенением Земли, рассматривается только в случае использования одного геостационарного спутника-ретранслятора. Но даже в этом случае вследствие достаточно короткого интервала времени точность прогноза орбит спутников-респондентов остается достаточной для восстановления работы оптической линии связи.

4. Информационное взаимодействие. Основная цель информационного взаимодействия по аналогии с автономным планировани-

ем состоит в достижении более эффективного использования возможностей спутниковых группировок для проведения требуемых наблюдений и своевременной доставки данных на Землю. Автономное планирование обеспечивает вклад в достижение данной цели за счет адаптивного изменения (или расчета) плана съемок априори назначенных спутнику целей в зависимости от возникающих непредвиденных событий и в зависимости от его текущего фактического состояния. Информационное взаимодействие предполагает использование автономного планирования и обеспечивает вклад в достижение указанной цели за счет адаптивного распределения и/или перераспределения между спутниками задач наблюдения целевых объектов и задач передачи данных на Землю в соответствии с текущей фактической ситуацией. Более кратко это можно сформулировать следующим образом: автономное планирование обеспечивает наиболее эффективное адаптивное *индивидуальное* поведение спутников, а информационное взаимодействие обеспечивает наиболее эффективное адаптивное *групповое* поведение спутников.

Неотъемлемыми составляющими задач группового поведения являются следующие дополнительные существенные и взаимосвязанные факторы, которые рассматриваются дополнительно к индивидуальному поведению спутников.

Роли и задачи спутников. Распределение целей наблюдения между спутниками выполняется в соответствии с установленной на спутниках аппаратурой. Если группировка состоит из множества однородных спутников, то все они могут выполнять одни и те же задачи. Если группировка состоит из множества разнородных спутников, тогда спутники выполняют различные задачи в зависимости от установленных на них средств наблюдения.

Кластеры и группировки спутников. Кластер можно рассматривать как частный случай группировки спутников. Кластер характеризуется тем, что спутники находятся в относительной близости между собой. В этом случае для определения позиций спутников во времени можно использовать понятие эталонной орбиты, относительно которой орбитальные данные каждого спутника могут определяться в виде малых отклонений от данных эталонной орбиты. Важным для планирования свойством кластера является то обстоятельство, что спутники кластера имеют практически одни и те же окна видимости целей наблюдения и наземных станций.

Возможности связи и динамика сети. Дальность прямой радиосвязи между спутниками внутри группировки ограничена. В частности, в работах [10] и [19] для разных моделей малых спутников приводятся

оценки в 4 и 100 км. Поэтому возможность информационного обмена на основе прямой радиосвязи на текущем этапе рассматривается пока применительно только к кластерам спутников. При этом образуемые кластерами спутников сети являются динамическими.

Информационный обмен между спутниками на более дальних расстояниях возможен с использованием спутниковых систем связи или спутников ретрансляторов. Следует отметить, что информационное взаимодействие элементов космической системы, спутников и наземных станций в целом выполняется в рамках динамической сети. Однако информационный обмен в рамках схем «наземная станция – спутник», «спутник – спутник ретранслятор», «наземная станция – спутник ретранслятор» происходит на основе априори рассчитываемых интервалов времени радиовидимости. Подобные расчеты относительно группировок спутников также возможны, но только в наземных условиях, так как они являются весьма трудоемкими. Выполнение подобных расчетов на борту спутников для обеспечения автономного группового поведения является как минимум не рациональным подходом, если вообще возможным в силу ограниченных возможностей бортовых ресурсов.

Описанные факторы и обстоятельства позволяют сделать вывод о существенном многообразии в направлениях исследований и многообразии возможных постановках задач планирования и управления в области группового поведения спутников. Далее в этом разделе приводится обзор нескольких работ в этих направлениях.

В работе [19] описывается сценарий информационного взаимодействия внутри кластера из 8-ми спутников в рамках миссии EDSN (Edison Demonstration of Smallsat Networks). Запуск спутников был запланирован на 2015 год. (https://en.wikipedia.org/wiki/Edison_Demonstration_of_Smallsat_Networks - информация о неудачном запуске) Цель миссии — измерения скорости движения заряженных частиц на низких околоземных орбитах.

Информационное взаимодействие в данном случае используется для организации передачи данных измерений в наземные пункты в соответствии со следующим сценарием. В каждый момент времени один из спутников играет роль капитана, остальные — роль лейтенантов. Капитан является центральным звеном сети. Он запрашивает у остальных спутников, лейтенантов, данные и передает их наземной станции. Роль капитана со временем передается от одного спутника другому.

Связь капитана с лейтенантом называется сессией. В начале сессии капитан в течении 50 секунд посылает 6 пинг-запросов с указа-

нием идентификатора лейтенанта, с которым устанавливается связь. Получив пинг-сигнал, лейтенант выполняет следующие действия:

1. Проверяет корректность сигнала (идентификатор «кому» и контрольную сумму).
2. Ждет 60 секунд, пока капитан продолжает посылать пинг-сигналы.
3. Посылает пакеты данных капитану. Первым посылает пакет с телеметрической информацией, далее — пакеты с данными измерений.
4. Выключает радио и удаляет все посланные пакеты данных из памяти.

Полученные пакеты данных капитан сохраняет в памяти для дальнейшей передачи на Землю по принципу FIFO.

Сессия продолжается в течение фиксированного периода времени около четырех минут. Если лейтенант не отвечает (не услышал пинг-сигналы или у него разряжены батареи), капитан ждет этот период времени и только после этого начинает сессию со следующим спутником-лейтенантом.

Последовательность сессий со всеми лейтенантами называется минорным циклом, в течение которого капитан собирает данные со всех 7 спутников-лейтенантов. После каждого минорного цикла роль капитана переходит к следующему спутнику по кругу. До начала минорного цикла каждый спутник с помощью GPS данных уточняет свои часы, позицию и скорость движения. Далее он сравнивает текущее время с моментами времени, предварительно загруженными в память, и на основании этого сравнения определяет, какой спутник будет капитаном на следующем минорном цикле.

В течение минорного цикла может происходить рассинхронизация часов спутников, до 12 секунд. Поэтому при выполнении операций используются буферные запасы времени. Например, лейтенант включает радио за 30 секунд до начала времени связи с капитаном и выключает его через 30 секунд после окончания окна времени для связи. Критическим ресурсом является запас энергии. Его априори не хватает на то, чтобы лейтенант мог держать радио все время включенным для связи с капитаном. Поэтому лейтенант включает радио только тогда, когда он ожидает получение сообщений от капитана.

Каждый минорный цикл длиться приблизительно 25 часов. Последовательность из 8-ми минорных циклов, т.е. когда каждый спутник один раз становится капитаном, называется мажорным циклом. В рамках запланированной миссии предполагается, что после 2-3 мажорных циклов спутники могут находиться слишком далеко друг от друга (более 100 км), чтобы осуществлять межспутниковую радиосвязь. Тем не менее

они будут продолжать функционировать по описанному сценарию до окончания миссии, которая запланирована на 60 дней.

Каждый спутник на основании GPS данных до начала минорного цикла моделирует свою орбиту на два минорных цикла вперед, т.е. на горизонте времени 50 часов вперед. На основании этого моделирования рассчитываются временные окна, когда и какие операции могут быть выполнены, и с учетом приоритетности операций рассчитывается план спутника. При этом часть операций планируется только на основании времени. Например, межспутниковая связь планируется через определенное время после начала минорного цикла. Часть операций планируется на основании времени и позиции спутника. В частности, связь с наземной станцией. После того как составлено расписание, все операции выполняются строго в соответствии с запланированными временными параметрами.

Таким образом, описанный сценарий информационного взаимодействия является априори разработанным и не адаптивным. Однако это, по всей видимости, соответствует начальному этапу стадии практических разработок и экспериментов, так как в качестве дальнейшего плана в статье обозначен достаточно широкий спектр направлений исследований. В их числе обозначены такие направления, как:

– управление конкретными спутниками за счет передачи им сообщений с Земли и маршрутизации сообщений в сети спутников;

– автономное конфигурирование сети и выбор капитана (или капитанов) на основе информационного взаимодействия и сравнения состояния спутников. Например, выбор капитана с учетом сравнения объема данных для передачи на землю текущих запасов энергии и с учетом качества временного окна связи с наземной станцией;

– многоэтапная маршрутизация пакетов данных при их передаче в наземный пункт через капитана;

– анализ топологии и учет фактора динамичности сети;

– использование возможности того, что несколько капитанов могут обеспечить передачу большего объема данных на землю;

– и другие.

В работе [10] описываются результаты компьютерного моделирования информационного взаимодействия внутри кластера малых спутников в рамках динамической сети. В модели предметной области полагается, что на спутниках установлены камеры для съемки, а спутники, обеспечивающие связь с наземными станциями, имеют достаточно памяти для передачи данных в режиме «запомнил — передал». Основным ограничением является запас энергии, и потребление энергии на связь оказывает значительное влияние на производительность системы.

Задача наблюдения предполагает выполнение нескольких подзадач. Результат выполнения подзадачи (например, данные съемки) передается другому спутнику, где происходит следующий шаг выполнения задачи (например, другая съемка и/или объединение данных съемок).

Моделирование выполняется на основе многоагентного подхода. Каждому спутнику в системе соответствует свой агент. Подзадачи распределяются между спутниками на основе модифицированного CNP (Contract Net Protocol) протокола. Агент спутника, инициирующий протокол информационного взаимодействия, называется аукционером. Он анонсирует данные подзадач своим прямым соседям в сети, которые далее повторяют это сообщение своим соседям и т.д. Все агенты, получившие запросы и имеющие необходимые ресурсы, рассчитывают оценку стоимости выполнения подзадачи и посылают ее аукционеру.

Оценка стоимости выполнения рассчитывается с помощью формулы, в которой в качестве параметров используются размер подзадачи, оставшийся объем энергии спутника, максимальный объем энергии, который он может потратить, и расстояние до агента аукционера, измеряемого количеством этапов передачи сообщения по сети. Оценки передаются аукционеру по маршруту получения данных подзадачи в обратном направлении. Если через агента спутника передается несколько оценок других спутников, то этот агент передает далее агенту аукционеру только одну наилучшую оценку стоимости. На основании полученных оценок аукционер выбирает агента спутника, предложившего минимальную оценку стоимости, и передает ему все необходимые данные для выполнения подзадачи. Таким образом, в соответствии с данными оценками подзадачи распределяются наиболее близким и наименее загруженным в текущий момент времени спутникам.

Динамическая сеть моделировалась с помощью расчета динамической матрицы смежности, элементы которой описывали возможность или невозможность радиосвязи между соответствующей парой спутников в зависимости от расстояний во времени. Расстояния между спутниками во времени рассчитывались с помощью Кеплеровской модели.

В статье приведены результаты эксперимента моделирования со следующими входными параметрами. Кластер состоит из 125 спутников и описывается эталонной орбитой. Орбита каждого спутника задавалась в виде случайных незначительных отклонений от эталонной орбиты. Связь между двумя спутниками полагалась возможной, если расстояние между ними не превышало 4 км. Таким образом, в эксперименте динамическая топология сети характеризуется следующим образом. В определенные моменты времени, при прохождении перигея орбиты, сеть является наиболее связанной. В промежуточные моменты

времени между ними связность сети становится ниже. Но при этом всегда существует возможность многоэтапной передачи сообщений между любыми двумя спутниками.

Верхняя граница суммарного времени на передачу сообщения между двумя спутниками и на его обработку оценивалось в 100 миллисекунд, что, по мнению авторов, является достаточно реалистическим значением.

Через каждые 100 секунд в систему вводились 5 новых задач, каждая из которых состояла из пяти подзадач. Длительность эксперимента определялась одной орбитой. Общее количество задач и подзадач 280 и 1400 соответственно.

Модель потребления энергии описывалась в условных единицах следующими оценками:

– выполнение одной подзадачи — 1 единица;
– передача сообщения между двумя спутниками — 0.005 единицы;
– передача задачи между двумя спутниками — 0.5 единицы;
– восполнение энергии — 0.005 единицы в секунду;
– максимальной объем энергии спутника — 10 единиц.

Основные результаты эксперимента и выводы заключаются в следующем. Потребление энергии на информационное взаимодействие сопоставимо с потреблением энергии на выполнение подзадач, которое в соответствии с входными параметрами эксперимента оценивается в 1400 единиц. Аукционы (распределение задач и подзадач) в большинстве случаев по времени успевают закончиться, прежде чем происходят изменения топологии сети. Время связи между двумя спутниками существенно больше, чем длительность аукциона. То есть, с точки зрения аукционера, локальная сеть в течение аукциона является статической. Если изменение сети влечет срыв аукциона, аукционер может повторно начать аукцион с большей вероятностью его успешного выполнения. Стоимость (в единицах потребления энергии) проведения аукционов в условиях динамической сети меньше, чем стоимость отслеживания изменений сети и проведение аукционов в интервалах времени между ними, когда сеть остается неизменной.

5. Заключение. Основным трендом в развитии систем планирования космических миссий в настоящее время является переход к парадигме, в соответствии с которой спутникам передаются не целевые данные, а детальные планы, определяющие временные параметры проведения съемок и передачи данных на Землю, и которые рассчитываются на борту спутников. Переход к этой парадигме главным образом создает необходимые предпосылки для преодоления объективных недостатков

традиционных методов планирования и управления, которые были рассмотрены в первом разделе обзора. Необходимость в переходе к этой парадигме также предопределяется спецификой задач планирования, которая возникает при использовании группировок малых спутников.

Наиболее распространенной практикой является ситуация, когда каждый спутник управляется и контролируется операторами в наземных пунктах управления. При этом детальный план операций спутника может уточняться в интерактивном режиме. Обзор традиционных систем планирования показывает, что эта возможность рассматривалась в качестве одного из основных требований к их разработке [4]. Однако фактор многочисленности группировок малых спутников влечет существенное увеличение нагрузки на операторов. Кроме того, планирование миссий группировок малых спутников предполагает координацию действий спутников, и уже не сводится к расчету множества отдельных и независимых планов спутников. Очевидно, что наличие таких обстоятельств может только усилить проявление объективных недостатков традиционных методов планирования и управления.

Реализация новой парадигмы сводится к развитию и использованию методов автономного адаптивного планирования и информационного взаимодействия спутников. Реализация этих методов, в свою очередь, существенным образом зависит от реальных и перспективных технических возможностей спутников и спутниковых систем, а именно от возможностей бортовых вычислительных процессоров и возможностей связи со спутниками и между спутниками. В связи с этим можно отметить, что развитие и использование этих методов находятся на различных стадиях исследований. Различные методы автономного адаптивного планирования уже находятся на стадии экспериментальных летных испытаний. Методы информационного взаимодействия спутников пока еще находятся на стадии теоретических исследований с использованием методов компьютерного моделирования. Единственная известная из обзора работ миссия, в которой целью была демонстрация начальных возможностей информационного взаимодействия кластера малых спутников, описывается в работе [19].

В ближайшей перспективе следует ожидать продолжения активных исследований и появления новых результатов в области разработки указанных методов. В частности, в отмеченной выше работе [19] приводится достаточно большой список направлений исследований в части развития методов информационного взаимодействия между спутниками.

По мнению автора данной статьи, одним из критически важных следует рассматривать направление исследований, затронутое в работе [14], которое состоит в следующем. Развитие методов автономного

планирования и информационного взаимодействия до настоящего времени рассматривается вне зависимости друг от друга. В области автономного планирования пока еще превалирует подход, когда автономное планирование выполняется в комбинации с наземным планированием и рассматриваются ситуации, когда распределение целей наблюдения между спутниками выполняется исключительно при наземном планировании. В области же информационного взаимодействия, как правило, рассматриваются ситуации с переназначением целей наблюдения между спутниками без должного учета текущих оперативных планов спутников. В связи с этим комплексные исследования методов автономного планирования и методов информационного взаимодействия пока еще остаются вне фокуса внимания.

С точки зрения долгосрочного прогноза, следует выделить те технические возможности, развитие которых будет оказывать критически важное влияние на эффективность функционирования космических систем наблюдения целевых объектов на Земле и в космическом пространстве. Это возможности вычислительных бортовых устройств и возможности связи с космическими аппаратами. При обеспечении вычислительных возможностей, сопоставимых с наземными возможностями, создаются условия, позволяющие рассматривать полноценное автономное планирование. В частности, без необходимости выполнения каких-либо вспомогательных расчетов на Земле и, соответственно, без какой-либо комбинации с наземным планированием. Развитие технических возможностей связи с космическими аппаратами предполагает в идеале обеспечение связи в режиме реального времени или по крайней мере существенное увеличение пропускной способности каналов связи. Пути реализации таких возможностей рассматриваются в работе [18]. Обеспечение такого уровня связи позволит разрешить проблему «узкого горлышка», когда каналы связи не способны обеспечить передачу объема данных, которые могут накапливать космические аппараты в результате проведения съемок целевых объектов. При этом значимость решения этой проблемы в ближайшем будущем может только возрастать в связи с использованием малых космических аппаратов.

Литература

1. *Davis T.M.* Operationally Responsive Space – The Way Forward // Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–7–49.
2. *Chien S. et al.* A generalized timeline representation, services, and interface for automating space mission operations // Proceedings of the 12th International Conference on Space Operations, SpaceOps AIAA. 2012.
3. *Herz E.* EO and SAR Constellation Imagery Collection Planning // Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.

4. *Iacopino C., Harrison S., Brewer A*. Mission Planning Systems for Commercial Small-Sat Earth Observation Constellations // Proceedings of the 9th International Workshop on Planning and Scheduling for Space (IWPSS). 2015. pp. 45–52.
5. *Wörle M. et al*. The Incremental Planning System – GSOC's Next Generation Mission Planning Framework // Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
6. *Gottfert T. et al.* Robust Commanding // Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
7. *Michel J. et al.* A Portable Autonomous Ground Station to Support a Constellation of CubeSats // Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–6–39.
8. *Platzer P., Wake C., Gould L*. Smaller Satellites, Smarter Forecasts: GPS-RO Goes Mainstream // Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–7–53.
9. *Schwab T.* Implementing a Small Satellite Information Enterprise Using a Modular Open Architecture Approach Based on International Standards // Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–I–2.
10. *van der Horst J., Noble J.* Task allocation in networks of satellites with Keplerian dynamics // Acta Futura. 2012. vol. 5. pp 143–151.
11. *Maillard A. et al.* Ground and board decision-making on data downloads // Proceedings of 25th International Conference on Automated Planning and Scheduling. 2015.
12. *Lenzen C. et al.* Onboard Planning and Scheduling Autonomy within the Scope of the Fire Bird Mission // Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
13. *Kennedy A. et al.* Automated Resource-Constrained Science Planning for the MiRaTA Mission // Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–6–37.
14. *Herz E., George D., Esposito T., Center K*. Onboard Autonomous Planning System // Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
15. *Martin-Pimentel P. et al.* Laser Com in space, the operational concept // Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
16. *Israel D., Edwards B., Wilson K., Moores J*. An Optical Communications Pathfinder for the Next Generation Tracking and Data Relay Satellite // Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
17. European Data Relay System. URL: https://en.wikipedia.org/wiki/European_Data_Relay_System (дата обращения 01.06.2016)
18. *Королев Б.* Технология работы космической оптической линии связи для повышения оперативности управления и получения информации потребителем в процессе функционирования космических средств // Космическая техника и технология. 2014. Вып. 1(4). С. 39–47.
19. *Hanson J., Sanchez H., Oyadomari K.* The EDSN Intersatellite Communications Architecture // Proceedings of the AIAA/USU Conference on Small Satellites. 2014. SSC14-WS1.

Карсаев Олег Владиславович — к-т техн. наук, старший научный сотрудник лаборатории интеллектуальных систем, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: интеллектуальная поддержка принятия решений, транспортная логистика, многоагентные системы. Число научных публикаций — 90. karsaev@ips-logistic.com; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)3283570.

O.V. KARSAEV

REVIEW OF CONVENTIONAL AND INNOVATIVE SATELLITE MISSION PLANNING SYSTEMS

Karsaev O.V. **Review of Conventional and Innovative Satellite Mission Planning Systems.**

Abstract. The paper is a review of conventional and innovative planning systems of satellite operations in missions of observation of target objects on the ground and in space. In conventional planning systems satellites are considered executors of plans computed by ground control centers. This approach has some disadvantages that may significantly decrease efficiency of satellites operation. The paper includes a description and an analysis of these disadvantages. The existence of these disadvantages and challenges of small satellites mission planning are the reasons of re-search and development of innovative methods and planning systems that mainly assume adaptive autonomous on-board planning and information interaction between satellites. Development of the latter possibility is considered a basis that may provide adaptive group behavior of satellites.

The review includes a description of different innovative planning systems that are either already used in experimental modes in actual missions or so far being developed and investigated via simulation. The paper also contains a review of some prospective elaborations in the area of communication between satellites as these opportunities can significantly influence the mission planning problem statement.

Keywords: autonomous planning, information collaboration, group behavior.

Karsaev Oleg Vladislavovich — Ph.D., senior researcher of intelligent systems laboratory, St. Petersburg Institute for informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: intelligent decision support, transportation logistics, agent based systems. The number of publications — 90. karsaev@ips-logistic.com; 39, 14th line, St.Petersburg, 199178; office phone: +7(812)3283570.

References

1. Davis T.M. Operationally Responsive Space – The Way Forward. Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–7–49.
2. Chien S. et al. A generalized timeline representation, services, and interface for automating space mission operations. Proceedings of the 12th International Conference on Space Operations, SpaceOps AIAA. 2012.
3. Herz E. EO and SAR Constellation Imagery Collection Planning. Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
4. Iacopino C., Harrison S., Brewer A. Mission Planning Systems for Commercial Small-Sat Earth Observation Constellations. Proceedings of the 9th International Workshop on Planning and Scheduling for Space (IWPSS). 2015. pp. 45–52.
5. Wörle M. et al. The Incremental Planning System – GSOC's Next Generation Mission Planning Framework. Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
6. Gottfert T. et al. Robust Commanding. Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
7. Michel J. et al. A Portable Autonomous Ground Station to Support a Constellation of CubeSats. Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–6–39.
8. Platzer P., Wake C., Gould L. Smaller Satellites, Smarter Forecasts: GPS-RO Goes Mainstream. Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–7–53.

9. Schwab T. Implementing a Small Satellite Information Enterprise Using a Modular Open Architecture Approach Based on International Standards. Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–I–2.
10. van der Horst J., Noble J. Task allocation in networks of satellites with Keplerian dynamics. *Acta Futura*. 2012. vol. 5. pp 143–151.
11. Maillard A. et al. Ground and board decision-making on data downloads. Proceedings of 25th International Conference on Automated Planning and Scheduling. 2015.
12. Lenzen C. et al. Onboard Planning and Scheduling Autonomy within the Scope of the Fire Bird Mission. Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
13. Kennedy A. et al. Automated Resource-Constrained Science Planning for the MiRaTA Mission. Proceedings of the AIAA/USU Conference on Small Satellites. 2015. SSC15–6–37.
14. Herz E., George D., Esposito T., Center K. Onboard Autonomous Planning System. Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
15. Martin-Pimentel P. et al. Laser Com in space, the operational concept. Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
16. Israel D., Edwards B., Wilson K., Moores J. An Optical Communications Pathfinder for the Next Generation Tracking and Data Relay Satellite. Proceedings of the 14-th International Conference on Space Operations, SpaceOps AIAA. 2014.
17. European Data Relay System. Available at: https://en.wikipedia.org/wiki/European_Data_Relay_System (accessed 01.06.2016)
18. Korolev B. [Space optical communication technology aimed at a more responsive control and prompted delivery of data to the end user during space operations]. *Kosmicheskaya tehnika i tehnologiya – Space engineering and technology*. 2014. vol. 1(4). pp. 39–47. (In Russ.).
19. Hanson J., Sanchez H., Oyadomari K. The EDSN Intersatellite Communications Architecture. Proceedings of the AIAA/USU Conference on Small Satellites. 2014. SSC14–WS1.

УДК 629.7 **DOI** 10.15622/sp.48.9

Е.П. Минаков, Б.В. Соколов

ИССЛЕДОВАНИЯ ХАРАКТЕРИСТИК РАЗМЕЩЕНИЯ И ВАРИАНТОВ ПРИМЕНЕНИЯ МОНОБЛОЧНЫХ СТАЦИОНАРНЫХ НАЗЕМНЫХ СРЕДСТВ ПОРАЖЕНИЯ АСТЕРОИДОВ

Минаков Е.П., Соколов Б.В. **Исследования характеристик размещения и вариантов применения моноблочных стационарных наземных средств поражения астероидов.**

Аннотация. Представлены математические модели и результаты исследования характеристик трех вариантов размещения стартовых комплексов моноблочных стационарных наземных средств поражения астероидов, отличающихся друг от друга геоцентрическими координатами точек стояния, их количеством, а также вероятностями поражения астероидов для трех способов применения указанных средств: поражение астероидов на нисходящих участках траекторий движения специальных головных частей, их поражение на восходящих или нисходящих участках траекторий, при варьировании азимутов пусков рассматриваемых средств.

Ключевые слова: средство наземного базирования для поражения астероидов, специальная головная часть, область воздействия, характеристики размещения стартовых комплексов, способ поражения астероидов.

1. Введение. Падение на Землю астероидов типа Апофиса и таких метеоритов, как Тунгусский или Челябинский, ставят под угрозу существование человечества. В России и за рубежом предложено множество способов защиты Земли от астероидов, в числе которых [1-6] их контактное разрушение или отклонение их с орбит соударения с Землей, а также дистанционное воздействие на них в тех же целях. Работы в этом направлении ведутся в Государственном ракетном центре имени академика Макеева совместно с Уральским и Сибирским филиалами Российской академии наук, научно-производственном объединении имени С. А. Лавочкина, научно-исследовательском центре имени Г.Н. Бабакина, научно-производственном объединении «Молния» и в ряде других организаций [7-8]. Проведенные исследования показали, что один из способов устранения астероидной угрозы — поражение астероидов путем подрыва зарядов, доставляемых ракетами-перехватчиками [8, 9]. Считается, что в качестве указанных средств поражения могут выступать межконтинентальные баллистические ракеты, в частности тяжелая двухступенчатая жидкостная ампулизированная межконтинентальная баллистическая ракета SS-18 Mod.1,2,3 Satan (по классификации НАТО), оснащенная ядерной головной частью и запускаемая из шахт.

Перечисленные обстоятельства актуализируют проблематику технико-экономического обоснования возможности практического применения тех или иных способов применения наземных средств

поражения астероидов (СПА), к которым, помимо указанных, могут быть отнесены существующие и специально разработанные ракеты космического назначения (РКН), а также межконтинентальные баллистические ракеты, оснащенные специальными головными частями (СГЧ) [6-10]. Общими достоинствами указанных средств являются удобство их развертывания и эксплуатации, всегда высокая степень готовности и контроля их состояния, а также многочисленность этих средств. Основным их недостатком является возможность уничтожения астероидов только в непосредственной близости от Земли на расстоянии менее 2000 км, в результате чего могут возникнуть последствия двух типов: неконтролируемое падение частей астероида на поверхность Земли и радиационное заражение, «повреждение» озонного слоя атмосферы в случае применения ядерных СГЧ.

В тоже время падение на Землю челябинского метеорита выявило проблему, заключающуюся в практической непредсказуемости времени и траектории движения астероидов и метеоритов [11-16]. При этом сложной технической задачей является попадание СГЧ в астероид с максимальным линейным размером («диаметром»), летящим со скоростью более 12 км/с, когда «догнать» его не представляется возможным. Следовательно, воздействие на астероид должно происходить либо на «встречных курсах», что очень трудно обеспечить, либо в так называемых узловых точках (УТ) при очень высоких относительных скоростях движения и практически мгновенно [17-18].

Указанная проблема может быть решена созданием эффективно функционирующей системы контроля за астероидами и метеоритами, с одной стороны, а с другой стороны — расположением на поверхности Земли ракет-перехватчиков таким образом и в таком количестве, чтобы поразить любой движущийся к Земле объект за минимально возможное время при минимальной информации о параметрах его движения, то есть созданием наземного эшелона глобальной защиты Земли от астероидов и метеоритов. Очевидно, что система поражения астероидов НБ должна включать в себя совокупность стартовых комплексов (СК) наземного базирования (НБ) с готовыми к применению СПА, размещенными на поверхности Земли таким образом, чтобы зоны воздействия СГЧ полностью перекрывали заданный рубеж поражения астероидов (РПА). Важнейшими в настоящее время являются оценки характеристик размещения СК и применения СПА: их числа и положения на поверхности Земли, а также вероятностей поражения астероидов и метеоритов,

базирующиеся на строгих математических моделях, рассмотрению которых посвящена предлагаемая статья.

2. Модели и результаты оценивания характеристик размещения однотипных стационарных моноблочных СПА НБ. Приведенные в статье математические модели получены в предположении, что (рисунок1):

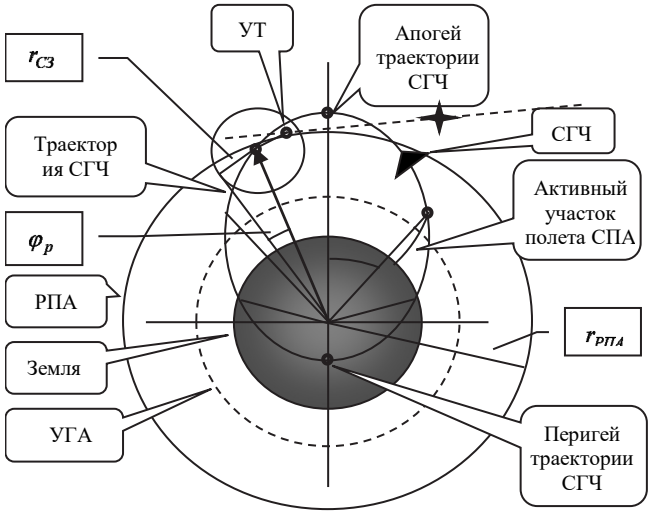


Рис. 1. Кинематические элементы применения СПА НБ (вид в плоскости движения СГЧ)

1) моделью поверхности Земли является сфера радиуса $R_3 = 6371$км;

2) РПА представляет собой сферу заданного радиуса — $r_{РПА}$ с центром, совпадающим с центром Земли;

3) все СПА обладают одинаковыми техническими характеристиками, имеют стационарное НБ и одно СПА доставляет на РПА только одну СГЧ;

4) зона воздействия СГЧ по астероиду имеет форму шара радиуса — $r_{СЗ}$;

5) параметры траекторий всех СПА (СГЧ) одинаковы и не зависят от азимута пуска СПА;

6) движение СГЧ описывается кеплеровской теорией, аппроксимируется эллипсом и происходит по возвратным траекториям;

7) движение астероидов аппроксимируется отрезками прямых линий;

8) воздействие на астероиды осуществляется выше условной границы атмосферы (УГА);

9) на относительную скорость движения СГЧ и астероида в момент воздействия на него СГЧ ограничений не наложено;

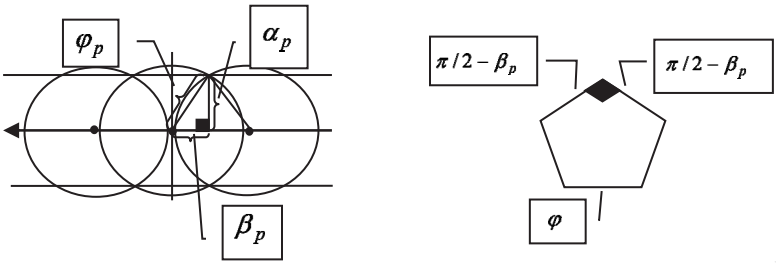
10)точность выведения СГЧ в УТ обеспечивается радиусом воздействия СГЧ.

Угловой размер области воздействия СГЧ на РПА определяется по формуле (рисунок1):

$$\phi_p = \arcsin(r_{C3} / r_{PIIA}). \quad (1)$$

Угловое расстояние между точками задействования СГЧ в одной плоскости при создании полосы сплошного воздействия по астероидам на РПА определяется углом β_P (рисунок 2) по правилу Непера [14]:

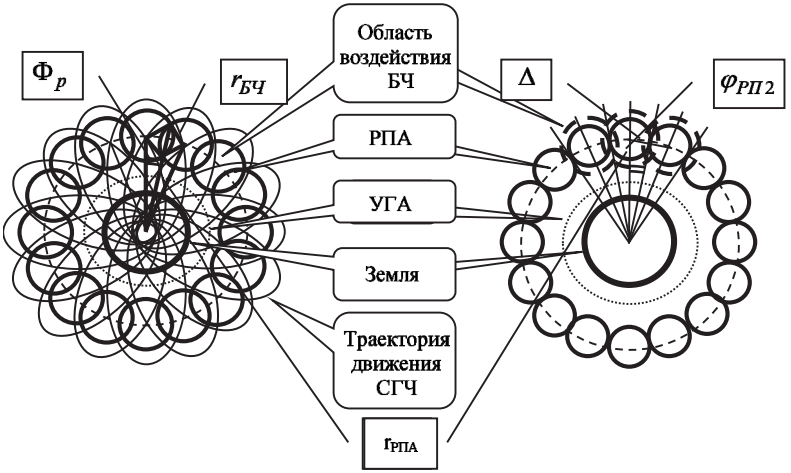
$$\cos\beta_p = \cos\varphi_p / \cos\alpha_p . \quad (2)$$



а) б)

Рис. 2. Связь между угловыми величинами области сплошного воздействия: а) угловые величины в плоскости движения СГЧ; б) пятиугольник Непера для определения углов β_p и α_p

Число СПА НБ, обеспечивающих одну плоскость сплошного воздействия (рисунок 3, а), определяется зависимостью:



а) б)

Рис. 3. Схема расположения траекторий движения и областей воздействия БЧ: а) в плоскости РПА; б) в плоскости экватора Земли

$$N_n = E[\pi / \beta_p] + 1 . \tag{3}$$

Уточненное угловое расстояние между точками задействования СГЧ в одной плоскости определяется по формуле:

$$\beta_p^* = \pi / N_n . \tag{4}$$

Угловой размер ширины полосы сплошного воздействия СГЧ в одной плоскости — α_p может быть вычислен по формуле:

$$\cos \alpha_p^* = \cos \varphi_p / \cos \beta_p^* . \tag{5}$$

Вероятность поражения астероида в случае независимого применения СПА НБ в каждой плоскости принимает значения [3]:

$$P_1 = \begin{cases} p, \text{когда области поражения СГЧ не пересекаются,} \\ 1-(1-p)^2, \text{когда области поражения СГЧ пересекаются,} \end{cases} \tag{6}$$

где p — вероятность успешного выполнения цикла подготовки и применения СПА НБ, включающая в себя вероятность точного предсказания времени пересечения РПА астероидом.

Число плоскостей сплошного воздействия СГЧ вычисляется в соответствии с зависимостью (рисунок 3.б):

$$M_n = E[\pi / \alpha_p^*] + 1. \quad (7)$$

Потребное число СПА НБ (СК), обеспечивающих сплошную область воздействия по астероидам, может быть вычислено по формуле:

$$Q = N_n M_n. \quad (8)$$

Для обеспечения сплошной области воздействия СК должны располагаться в одной из плоскостей, проходящих через центр Земли, а пуски СПА НБ — осуществляться с соответствующими азимутами.

3. Исследования вариантов размещения однотипных стационарных моноблочных СПА НБ. Возможны различные варианты размещения СК СПА НБ:

1) в плоскостях, проходящих через ось мира — SS^1 (рисунок 4);
2) с любой требуемой ориентацией линии пересечения плоскостей размещения СК СПА НБ;
3) с заданным расположением СК в соседних плоскостях;
4) с произвольным расположения СК в соседних плоскостях.

В первом варианте одним из способов применения СПА НБ является их пуск с одинаковыми азимутами, равными 0^0. При этом разность между широтами двух соседних СПА НБ определяется зависимостью:

$$\Delta\Psi = \Psi_i - \Psi_{i-1} = 2\beta_p^* = const, \quad (9)$$

а между долготами плоскостей:

$$\Delta\lambda = \lambda_i - \lambda_{i-1} = 2\alpha_p^* = const. \quad (10)$$

Эффективность поражения астероида оценивается по вероятности — P воздействия, которая в случае независимости применения [15] СПА, может быть оценена зависимостью (рисунок 5):

$$P = \begin{cases} P_1, \text{для областей однократного воздействия} \\ 1-(1-P_1)^2, \text{для областей двухкратного воздействия} \\ 1-(1-P_1)^3, \text{для областей трехкратного воздействия} \\ 1-(1-P_1)^{M_n}, \text{для областей } M_n \text{ - кратного воздействия} \end{cases}. \quad (11)$$

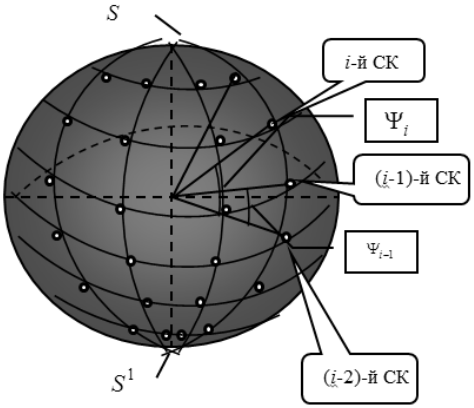


Рис. 4. Размещение СК в плоскостях, проходящих через ось мира

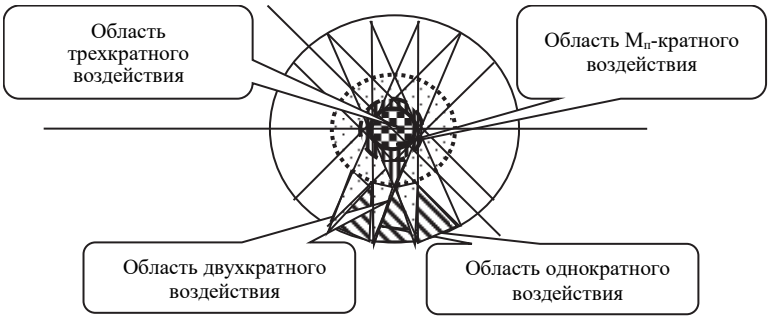


Рис. 5. Схема пересечения полос воздействия СГЧ
(вид на плоскость экватора)

Для оценивания Q для рассмотренной возможной схемы расположения СК были приняты исходные данные: $p = 0{,}8$; $r_{СЗ} = 5{,}10{,}15$ км ; $H_{РПА} = 200, 400, 500$ км . Результаты моделирования характеристик размещения СПА для каждого варианта исходных данных представлены в таблицах 1-3.

Таблица 1. Результаты оценивания величин N_n , M_n , Q , $p_{\min}$, $p_{\max}$, $\Delta\Psi$, $\Delta\lambda$ для $p = 0{,}8$; $H_{РПА} = 200$ км

$r_{СЗ}$, км	N_n	M_n	Q	$p_{\min}$	$p_{\max}$	$\Delta\Psi$, град	$\Delta\lambda$, град
5	6081	5625	34205625	0,8	1	0,0592105	0,0640083
10	3041	2813	8554333	0,8	1	0,1184211	0,1280168
15	1580	2808	4436640	0,8	1	0,2279924	0,1282427

Таблица 2. Результаты оценивания величин N_n, M_n, Q, $p_{\min}$, $p_{\max}$, $\Delta\Psi$, $\Delta\lambda$ для $p = 0{,}8$; $H_{РПА} = 400$ км

$r_{СЗ}$, км	N_n	M_n	Q	$p_{\min}$	$p_{\max}$	$\Delta\Psi$, град	$\Delta\lambda$, град
5	6505	5625	36590625	0,8	1	0,0553506	0,0640059
10	3253	2813	9150689	0,8	1	0,1107011	0,1280119
15	1644	2809	4617996	0,8	1	0,2191114	0,1281962

Таблица 3. Результаты оценивания величин N_n, M_n, Q, $p_{\min}$, $p_{\max}$, $\Delta\Psi$, $\Delta\lambda$ для $p = 0{,}8$; $H_{РПА} = 600$ км

$r_{СЗ}$, км	N_n	M_n	Q	$p_{\min}$	$p_{\max}$	$\Delta\Psi$, град	$\Delta\lambda$, град
5	6982	5625	39273750	0,8	1	0,0515685	0,0640012
10	3492	2813	9822996	0,8	1	0,1031223	0,1280143
15	1710	2809	4803390	0,8	1	0,2106495	0,1281642

Полученные результаты сведены в гистограммы зависимостей Q от $r_{СЗ}$ (рисунок 6).

Основным достоинством этого способа размещения СК и применения СПА НБ является необходимость знания только времени и ориентировочного места пересечения астероидом РПА, что позволяет гибко, оперативно и с высокой вероятностью их уничтожать. В то же время из полученных данных видно, что число СК с моноблочными СГЧ чрезвычайно велико. По ним можно оценить расстояние между СК по широте — $\Delta L_ш$ и по долготе — $\Delta L_д$:

$$\Delta L_ш = \Delta\Psi R_З; \Delta L_д = \Delta\lambda R_З. \qquad (12)$$

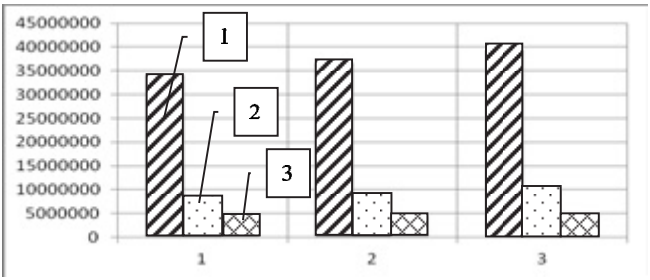
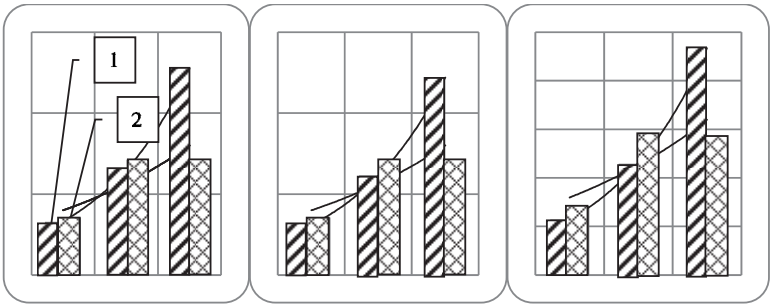


Рис. 6. Гистограммы зависимостей Q от $r_{СЗ}$ (для каждого варианта исходных данных: $H_{РПА} = 200$ км (1), $H_{РПА} = 400$ км (2), $H_{РПА} = 600$ км (3)

Соответствующие гистограммы представлены на рисунке 7.



а) б) в)

Рис. 7. Гистограммы зависимостей $\Delta L_ш$ (1) и $\Delta L_д$ (2) от $r_{СЗ}$

а) $H_{РПА} = 200$ км ; б) $H_{РПА} = 400$ км ; в) $H_{РПА} = 500$ км

На рисунке7 цифра 1 соответствует $\Delta L_ш$, цифра 2 — $\Delta L_д$.

Величина Q может быть уменьшена за счет сокращения числа СК, для СПА которых полосы сплошного воздействия взаимно перекрываются в приполярных областях. Для этого в $M_n - 1$ плоскости воздействия СГЧ число СК может быть сокращено до величины:

$$N_{n1} = E[(\pi - 2\alpha_p^*)/\beta_p] + 1. \qquad (13)$$

Общее число СК определяется тогда зависимостью:

$$Q_1 = N_n + (M_n - 1)N_{n1}, \qquad (14)$$

что обеспечивает вероятность:

$$p_{\min} = p \le P \le p_{\max} = P_1. \qquad (15)$$

Технически реализуем вариант поражения астероидов на РПА как на нисходящих, так и на восходящих участках траекторий движения СГЧ [1, 4], что также приводит к сокращению числа СК в одной плоскости до величины, определяемой зависимостью:

$$N_{n2} = E[\pi/(2\beta_p^*)] + 1. \qquad (16)$$

В этом случае выражение аналогичное (3) примет вид

$$N_{n3} = E[(\pi - 2\alpha_p^*)/(2\beta_p)] + 1. \qquad (17)$$

Общее число СК — Q_2 определяется тогда определяется по (14) при $N_n := N_{n2}$, $N_{n1} := N_{n3}$, а вероятность поражения астероида рассчитывается по формуле (15).

Результаты оценивания величин N_{n1} , Q_1 , N_{n2} , N_{n3} и Q_2 приведены в таблице 4.

Таблица 4. Результаты оценивания величин N_{n1}, Q_1, N_{n2} , N_{n3} и Q_2

$r_{СЗ}$, км	$H_{РПА}$, км	N_{n1}	Q_1	W_1	N_{n2}	N_{n3}	Q_2	W_2
5	200	3038	8545897	100,00	1521	1519	4272949	49,99
10	200	1578	4431026	48,20	790	789	2215513	50,00
15	200	1518	2135829	77,33	761	759	1067915	49,99
5	400	3250	9142253	100,00	1627	1625	4571127	49,99
10	400	1642	4612380	49,59	822	821	2306190	50,00
15	400	1624	2284971	100,00	814	812	1142486	49,99
5	600	3489	9814560	100,00	1746	1745	4908686	49,98
10	600	1708	4797774	51,15	855	854	2398887	50,00
15	600	1744	2452067	100,00	874	872	1226034	49,99

В этой же таблице приведены показатели сокращения числа СК $W_1 = (Q - Q_1)/Q$ и $W_2 = (Q_1 - Q_2)/Q_1$, выраженные в процентах. Предлагаемый последние два способа обеспечивают вероятность поражения астероида либо 0,8, либо 0,98.

Как видно из полученных данных, обладая практически теми же достоинствами, что и первый способ размещения СПА НБ, способ исключения СК для поражения астероидов в приполярных областях и на восходящих и нисходящих участках траекторий движения СГЧ позволяют существенно понизить их число, которое, однако, остается неприемлемо большим.

Технически реализуем способ поражения астероидов на РПА как на нисходящих, так и на восходящих участках траекторий движения СГЧ при азимутах пуска СПА, равных либо 0^0, либо 180^0, что приводит к сокращению числа СК в одной плоскости до величины, определяемой зависимостью:

$$N_{n4} = E[\pi/(4\beta_p^*)] + 1. \qquad (18)$$

В этом случае выражение аналогичное (3) примет вид:

$$N_{n5} = E[(\pi - 2\alpha_p^*)/(4\beta_p)] + 1. \quad (19)$$

Общее число СК — Q_3 определяется тогда определяется по (14) при $N_n := N_{n4}$, $N_{n1} := N_{n5}$, а вероятность поражения астероида оценивается по (15).

Результаты оценивания величин N_{n4} , N_{n5}, Q_3 и W_3 приведены в таблице5.

Таблица 5. Результаты оценивания величин N_{n4} , N_{n5}, Q_3 , W_3 , M_{n4} , Q_3 и W_3

$r_{СЗ}$, км	$H_{РПА}$, км	N_{n4}	N_{n5}	Q_3	W_3	M_{n4}	Q_4	W_4
5	200	761	760	2137881	49,96	704	535041	74,97
10	200	395	395	1109160	49,93	702	277290	75,00
15	200	381	380	534661	49,93	352	133761	74,98
5	400	814	813	2286970	49,96	704	572353	74,97
10	400	411	411	1154499	49,93	703	288933	74,97
15	400	407	406	571243	50,00	352	142913	74,98
5	600	873	873	2455749	49,97	704	614592	74,97
10	600	428	427	1199444	49,99	703	300182	74,97
15	600	437	436	613017	50,00	352	153473	74,96

Как видно из полученных данных, незначительное усложнение полетного задания СПА НБ дает положительные эффекты:

1) существенное сокращение (до приемлемых значений) числа СК;

2) повышение вероятности поражения астероидов за счет пусков СГЧ в одни и те же области РПА как при азимуте в 0^0, так и с азимутом 180^0 и вычисляемой по формулам:

$$P_1 = \begin{cases} 1-(1-p)^2, \text{когда области поражения СГЧ не пересекаются,} \\ 1-(1-p)^4, \text{когда области поражения СГЧ пересекаются.} \end{cases} \quad (20)$$

Возможность сокращения СК заложена в варьировании азимутами пусков СПА, что, однако, приводит к усложнению подготовки соответствующих полетных заданий. Пусть существует возможность пусков СПА с любым азимутом в диапазоне от 0^0 до 360^0 (рисунок 8).

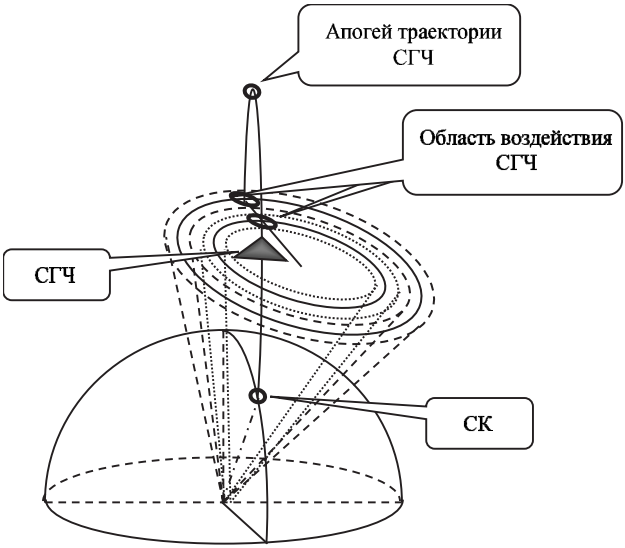


Рис. 8. Области воздействия СГЧ при любых азимутах пуска СПА

Это приводит к сокращению числа плоскостей размещения СК, которое в этом способе оценивается величиной

$$M_{п4} = E[\pi/(4\alpha_p^*)]+1, \qquad (21)$$

при тех же $N_{п4}$ и $N_{п5}$ и P_1, что и в последнем способе.

4. Заключение. Одним из основных результатов проведенных исследований следует считать тот факт, что впервые на основе использования математических моделей получены корректные численные значения характеристик размещения и применения моноблочных СПА НБ. Приведенные в статье оценки демонстрируют практически равную единице вероятность защиты Земли от летящих к ней астероидов и метеоритов, с одной стороны, а с другой стороны — потребность в огромном числе (сотни тысяч единиц) СПА для обеспечения этого. В связи с этим уместно привести высказывание Г. Гегеля о том, что «самая серьезная потребность есть потребность познания истины», которая в рассматриваемом случае состоит в полученные оценок, характеризующих предельные количества моноблочных СПА НБ, исчерпывающих их потенциальные возможности в борьбе с астероидной опасностью. Знание этой истины указывает так же на необходимость поиска альтернативных средств и способов решения проблемы защиты Земли, базирующихся прежде

всего на эффективном информационном обеспечении применения СПА. Особую актуальность в этой связи приобретают разработка и исследование характеристик применения СПА НБ с разделяющимися головными частями, мобильных СПА НБ, комбинированной пространственно-распределенной системы поражения астероидов и метеоритов, компонентами которой являются подсистема орбитального базирования, а также располагаемые в точках либрации и на поверхности Луны стационарные и мобильные СПА, базирующихся на фундаментальных и прикладных результатах, полученных отечественными учеными и инженерами в 80-е годы прошлого века в ответ на американскую программу «звездных войн» [6-8,12-16].

Отдельно следует подчеркнуть, что приведенные в статье модели и расчетные формулы (при их определенной доработке), а также полученные с их использованием результаты могут быть применены для исследования и оценивания сравнительных характеристик размещения и применения указанных СПА НБ различных типов.

Литература

1. *Соколов Л.Л. и др.*. Траектории соударения астероида Апофис с Землей в XXI веке // Астрон. вестн. 2012. Т. 46. № 4. С. 311–320.
2. *Шустов Б.М., Рыхлова Л.В.* О концепции комплексной программы «Создание российской системы противодействия космическим угрозам (2012-2020)» // Вестник Сиб. гос. аэрокосмического ун-та. Красноярск. 2011. Вып. 6(39). С.4–8.
3. Asteroid Impact Deflection Assessment AIDA study // ESA. 2015.
4. Asteroid deflection mission seeks smashing ideas // ESA. 2015.
5. *Пыжикова А.С., Фарафонтова Е.Л.* Проблема астероидно-кометной угрозы в рамках международного космического права // Актуальные проблемы авиации и космонавтики. 2012. Т. 2. Вып. 8. С. 355–357.
6. *Владимиров В.А., Рыхлова Л.В.* Угроза с неба (астероидно-кометная опасность) // Стратегия гражданской защиты: проблемы и исследования. 2014. Т. 4. Вып. 2. С. 591–602.
7. *Алексеев А.С., Величко И.И., Волков Ю.А., Ведерников Ю.А.* Ракетная концепция противометеоритной защиты Земли // Космическая защита Земли, Известия Челябинского научного центра, специальный выпуск. 1997. С. 55–77.
8. *Нечай В.З. и др.* Ядерный взрыв вблизи поверхности астероидов и комет // Космическая защита Земли, Известия Челябинского научного центра, специальный выпуск. 1997. С. 179–182.
9. *Бурков В.Д. и др.* Проблема противодействия астероидной опасности космическими средствами // Вестник Московского государственного университета леса – Лесной вестник. 2011. Вып. 5. С. 157–169.
10. *Соколов Л.Л., Кутеева Г.А.* О характеристиках возможных соударений астероидов с Землей // Вестник Санкт-Петербургского университета. Серия 1. Математика. Механика. Астрономия. 2012. Вып. 4. С. 133–138.
11. *Park S.-Y., Ross I.M.* Two-Body Optimization for Deflecting Earth-Crossing Asteroids // Journal of Guidance, Control and Dynamics. 1999. vol. 22. no. 3. pp. 415–420.

12. *Hall C.D., Ross I.M.* Dynamics and Control Problems in the Deflection of Near-Earth Objects // Advances in the Astronautical Sciences, Astrodynamics. 1997. vol. 97. Part I. pp. 613–631.
13. *Ross I.M., Park S.-Y., Porter S.E.* Gravitational Effects of Earth in Optimizing Delta-V for Deflecting Earth-Crossing Asteroids // Journal of Spacecraft and Rockets. 2001. vol.38. no. 5. pp. 759–764.
14. *Dwayne A.* Giant bombs on giant rockets: Project Icarus // The Space Review. 2004. vol. 5.
15. Сайт «Фактрум». URL: http://www.factroom.ru/facts/13802 (дата обращения 11.09.2013).
16. *Dillow C.* How it Would Work: Destroying an Incoming Killer Asteroid With a Nuclear Blast // Bonnier. URL: https://www.flightglobal.com/news/articles/nasa-plans-armageddon-spacecraft-to-blast-asteroid-215924 (дата обращения 26.09.2016).
17. *Вентцель Е.С., Овчаров Л.А.* Теория случайных процессов и ее инженерные приложения. М.: Высшая школа. 2000. 383 с.
18. *Аверкиев Н.Ф., Богачев С.А., Васьков С.А. и др.* Основы теории полета летательных аппаратов. СПб.: ВКА имени А.Ф. Можайского, 2013. 242 с.

Поддержка исследований. Исследование выполнено за счет гранта Российского научного фонда (проект № 16-19-00199).

Минаков Евгений Петрович — д-р техн. наук, профессор, профессор, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: системный анализ, баллистическое обеспечение полетов космических аппаратов, эффективность применения космических комплексов и систем. Число научных публикаций — 150. ep.minakov12345@mail.ru; ул. Ждановская, 13, Санкт-Петербург, 197198; р.т.: +7(812)552-6341.

Соколов Борис Владимирович — д-р техн. наук, профессор, Заслуженный деятель науки РФ, заместитель директора по научной работе, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: разработка научных основ теории управления структурной динамикой сложных организационно-технических систем. Число научных публикаций — 450. sokol@iias.spb.su; 14-я линия В.О., д. 39, Санкт-Петербург, 199178; р.т.: +7-812-328-3311.

E.P. MINAKOV, B.V. SOKOLOV

INVESTIGATION OF ALLOCATION CHARACTERISTICS AND DEPLOYMENT VARIANTS OF GROUND-BASED MISSILES FOR ASTEROID DESTRUCTION

Minakov E.P, Sokolov B.V. **Investigation of Allocation Characteristics and Deployment Variants of Ground-Based Missiles for Asteroid Destruction.**

Annotation. The paper presents mathematical models and investigation results of three variants of allocation of ground-based missiles for destroying asteroids. These missiles differ from each other by geocentric coordinates of control points, their amount and the probabilities of hitting the asteroid in three ways: hitting the asteroid on the descending parts of the trajectory of motion of special warheads; on ascending or descending parts of trajectories; at varying firing azimuths of the considered means.

Keywords: ground-based missiles for asteroid destruction, special warhead, impact area, allocation characteristics of missiles, way of hitting asteroids.

Minakov Evgeniy Petrovich — Ph.D., Dr. Sci., professor, professor, Mozhaisky Military Space Academy. Research interests: system analysis, provision of ballistic spacecraft, effectiveness of space complexes and systems. The number of publications — 150. ep.minakov12345@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812)552-6341.

Sokolov Boris Vladimirovich — Ph.D., Dr. Sci., professor, Honored scientist of Russian Federation, deputy director for research, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: development of research fundamentals for the control theory by structural dynamics of complex organizational-technical systems. The number of publications — 450. sokol@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-812-328-3311.

Acknowledgements. This research is supported by RSF (grant 16-19-00199).

References

1. Sokolov L.L., et al. [Trajectories of impact of an asteroid Apofis with Earth in the 21st century]. *Astronomical bulletin — Astronomicheskii vestnik.* 2012. vol. 46. no. 4. pp. 311–320.
2. Shustov B.M., Ryhlova L.V. [About the concept of the comprehensive program "Creation of the Russian system of counteraction to space threats (2012-2020)"]. *Vestnik Sib. gos. ajerokosmicheskogo un-ta. Kasnojarsk — Bulletin of the Siberian state space university.* 2011. vol. 6(39). pp. 4–8.
3. Asteroid Impact Deflection Assessment AIDA study. ESA. 2015.
4. Asteroid deflection mission seeks smashing ideas. ESA. 2015.
5. Pyzhikova A.S., Farafontova E.L. [Problem of asteroid and cometary threat within the international space law]. *Aktual'nye problemy aviacii i kosmonavtiki — Urgent problems of aircraft and astronautics.* 2012. vol. 2. no. 8. pp. 355–357.
6. Vladimirov V.A., Ryhlova L.V. [Threat from the sky (asteroid and cometary danger)]. *Strategija grazhdanskoj zashhity: problemy i issledovanija — Strategy of civil protection: problems and researches.* 2014. vol. 4. no. 2. pp. 591–602.
7. Alekseev A.C., Velichko I.I., Volkov Y.A., Vedernikov Y.A. [Rocket concept of antimeteoric protection of Earth]. *Kosmicheskaja zashhita Zemli, Izvestija*

Cheljabinskogo nauchnogo centra, special'nyj vypusk – Space protection of Earth, News of the Chelyabinsk scientific center, special release. 1997. pp. 55–77.
8. Nechay V.Z., et al. [Nuclear explosion near a surface of asteroids and comets]. *Kosmicheskaja zashhita Zemli, Izvestija Cheljabinskogo nauchnogo centra, special'nyj vypusk – Space protection of Earth, News of the Chelyabinsk scientific center, special release*. 1997. pp. 179–182.
9. Burkov V.D., et al. [Problem of counteraction of asteroid danger space means]. *Vestnik Moskovskogo gosudarstvennogo univer-siteta lesa – Lesnoj vestnik — Bulletin of Moscow State University of the wood – Wood bulletin.* 2011. vol. 5. pp. 157–169.
10. Sokolov L.L., Kuteeva G.A. [About characteristics of possible impacts of asteroids with Earth]. *Vestnik Sankt-Peterburgskogo universiteta. Serija 1. Matematika. Mehanika. Astronomija — Bulletin of the St. Petersburg university. Series 1. Mathematics. Mechanics. Astronomy.* 2012. vol. 4. pp. 133–138.
11. Park S.-Y., Ross I.M. Two-Body Optimization for Deflecting Earth-Crossing Asteroids. *Journal of Guidance, Control and Dynamics*. 1999. vol. 22. no. 3. pp. 415–420.
12. Hall C.D., Ross I.M.. Dynamics and Control Problems in the Deflection of Near-Earth Objects. *Advances in the Astronautical Sciences, Astrodynamics*. 1997. vol. 97. Part I. pp. 613–631.
13. Ross I.M., Park S.-Y., Porter S.E. Gravitational Effects of Earth in Optimizing Delta-V for Deflecting Earth-Crossing Asteroids. *Journal of Spacecraft and Rockets*. 2001. vol. 38. no. 5. pp. 759–764.
14. *Dwayne A.* Giant bombs on giant rockets: Project Icarus. The Space Review. 2004. vol. 5.
15. Sajt «Faktrum» [Factrum]. Available at: http://www.factroom.ru/facts/13802 (accessed 11.09.2013).
16. Dillow C. How it Would Work: Destroying an Incoming Killer Asteroid With a Nuclear Blast. Bonnier (9 April 2012). Available at: https://www.flightglobal.com/news/articles/nasa-plans-armageddon-spacecraft-to-blast-asteroid-215924 (accessed 26.09.2016).
17. Ventcel' E.S., Ovcharov L.A. *Teorija sluchajnyh processov i ee inzhenernye prilozhenija* [Theory of casual processes and its engineering applications]. M.: Vysshaja shkola, 2000. 383 p.
18. Averkiev N.F., Bogachev S.A., Vas'kov S.A. et al. *Osnovy teorii poleta letatel'nyh apparatov* [Bases of the aircraft flight theory]. SPb.: VKA imeni A.F. Mozhajskogo, 2013. 242 p.

УДК 006.72 **DOI** 10.15622/sp.48.10

А.А. Воевода, Д.О. Романников

АСИНХРОННЫЙ АЛГОРИТМ СОРТИРОВКИ МАССИВА ЧИСЕЛ С ИСПОЛЬЗОВАНИЕМ ИНГИБИТОРНЫХ СЕТЕЙ ПЕТРИ

Воевода А.А., Романников Д.О. **Асинхронный алгоритм сортировки массива чисел с использованием ингибиторных сетей Петри.**

Аннотация. В настоящее время задачи ускорения вычислений и/или их оптимизация является достаточно актуальной задачей. Среди направлений решения вышеприведенной задачи в статье рассматривается применение подхода распараллеливания и асинхронизации алгоритма сортировки. Предлагается метод сортировки, основанный на принципе разбиения всего массива на множество независимых пар чисел и их параллельное и асинхронное сравнение, что отличает предлагаемый алгоритм от традиционных алгоритмов сортировки (таких как быстрая сортировка, сортировка слиянием, вставками и другие). Алгоритм реализован с использованием сетей Петри как наиболее подходящего инструмента для описания асинхронных систем, а также приведен пример его работы. В статье выполнена оценка быстродействия алгоритма для наилучшего и наихудших случаев. В наилучшем случае алгоритм выполняется за 2 или 3 условных такта в зависимости от разбиения массива на пары соседних элементов. В наихудшем случае – за n или за 3n/2, где n – число элементов. Принципы распараллеливания и асинхронизации, использованные при построении алгоритма, также могут быть применены для других алгоритмов.

Ключевые слова: алгоритмы сортировки, пузырьковая сортировка, сети Петри, асинхронность, параллельные вычисления.

1. Введение. В настоящее время решение большинства современных задач требует больших вычислительных ресурсов. При этом развитие вычислительных ресурсов выполняется по многим направлениям: аппаратный уровень, где, например, увеличивают число ядер процессора; программное обеспечение, где применяют различные виды распараллеливания; и архитектурный уровень, где вычислительные системы проектируются из расчета распределения вычислительной нагрузки на многие независимые вычислительные ресурсы [1-3]. Стоит отметить, что для всех вышеприведенных направлений развития чаще всего применяются синхронные схемы их работы.

Одной из частных задач, которая решается при оптимизации использования вычислительных ресурсов и их ускорения, является задача сортировки. Для решения данной задачи разработано множество алгоритмов (сортировка пузырьком (*bubble sorting*), сортировка слиянием (*merge sorting*), быстрая сортировка (*quick sorting*), чет-нечет сортировка (*odd-even sorting*) и др.) [4-5]. В частности, в [5] приводится многопоточная реализация чет-нечет сортировки (*odd-even sorting*), заключающаяся в разбиении и параллельном сравнении и перестанов-

ке элементов массива на пары, начинающиеся с четных и не четных элементов. Битонная сортировка (*bitonic sorting*) [5, 6], основанная на последовательном приведении массива к парам битонных последовательностей и дальнейшем их слиянии, является популярным алгоритмом часто применяемая в GPU (*Graphics Processing Unit*). В [5] ранг сортировка (*rank sorting*), в основе которой лежит подсчет количества элементов с меньшим и большим значениями и последующая их расстановка по пред рассчитанным позициям. В [6] предлагается *AA-sort* алгоритм, основанный на сортировке расческой (*comb sorting*), разбиении всего массива элементов на множество подгрупп и их параллельной сортировке с последующим слиянием. В [7] приводится сравнение различных видов сортировок на современных вычислительных устройствах (в том числе и на GPU).

Стоит отметить попытки решить задачу сортировки при помощи машинного обучения [8], в частности, в [9] предлагается нейронная машина Тьюринга, с помощью которой алгоритмом сортировки пирамидой (*heap sorting*) сортируется массив из 20 элементов, а в [10] показана возможность сортировки массива из 10 элементов с использованием только нейронной сети.

При распараллеливании процессов дополнительные возможности возникают в случае их асинхронности. Для создания асинхронных систем с целью максимального использования существующих вычислительных ресурсов применяются сети Петри. Так в [11] рассмотрено решение задач организации связи между таксофонами и центром дистанционного контроля, в [12, 13] решаются задачи автоматики, среди которых есть задачи управления оборудованием водонапорных станций [13] и задача управления обжигом печи [13], а в [14] приводится пример решения задачи управления роботом-манипулятором, которая далее была развита в [13, 15, 16].

В связи с этим задача адаптации существующих алгоритмов для возможности их исполнения в параллельном и асинхронном режиме является актуальной.

Распараллеливание [1-3] и асинхронность могут быть применены и к задаче сортировки. В статье предлагается асинхронный алгоритм сортировки массива чисел, основывающийся на разбиении всего множества чисел массива на независимые пары и их сравнении. Можно рассматривать предлагаемый метод как адаптацию пузырьковой сортировки (*bubble sorting*) [4] к «многопузырьковому виду».

В отличие от традиционных алгоритмов сортировки, к которым можно отнести алгоритмы быстрой сортировки, сортировку вставками, слиянием и другие [4-6], предлагаемый алгоритм способен эффективно

исполняться за счет возможности максимального распараллеливания вычислений, то есть основным требованием к разрабатываемому алгоритму сортировки является эффективное использование возможности современных устройств, а именно – сортировка массивов в параллельном асинхронном режиме с целью непосредственного ускорения самой сортировки и более рационального использования ресурсов.

2. Алгоритм многопузырьковой сортировки. Основной принцип предлагаемого метода сортировки заключается в том, что из массива случайным образом выбираются пары соседних чисел, которые затем сравниваются (к примеру, в массиве из 100 элементов на одном условном такте (в силу того, что алгоритм является асинхронным, понятие тактов к нему не применимо, но под условным тактом тут и далее подразумевается исполнение возможных операций сравнения без сравнения повторяющихся пар чисел) одновременно могут сравниваться от 33 до 50 пар). После сравнения данная пара чисел блокируется для того, чтобы избежать их повторного сравнения. Если числа были переставлены в результате сравнения, то снимается блокировка с соседних чисел (слева и справа), так как имеет смысл выполнять сравнение для измененных пар. В случае если сравниваемая пара чисел не была переставлена, то есть левый элемент меньше, чем правый, то блокировка чисел соседних с рассматриваемой парой не снимается. Алгоритм заканчивает свою работу в случае запрета на сравнение для всех пар соседних чисел массива.

Схематичное представление алгоритма сортировки массива из четырех трехразрядных чисел приведено на рисунке 1. Числа массива на рисунке 1 изображены вертикальной последовательностью разрядов, представленных в виде окружностей. Секции сравнения, нарисованные на рисунке прямоугольниками, выполняют сравнение *i*-тых разрядов соседних чисел. Каждый разряд числа имеет левого и правого соседей и так как сравнение происходит попарно между соседними разрядами, каждый разряд числа (кроме крайних) относится к двум секциям сравнения, что представлено на рисунке как окружность, разделенная вертикальной чертой между двумя секциями сравнения.

В начальном состоянии метки находятся только в месте *start* и в местах представляющих разряды чисел в массиве. Работа приведенной системы начинается со срабатывания самого верхнего перехода, при котором метка из места *start* переходит в каждое из мест *c1-c4,* которые показывают доступность для сравнения соответствующих элементов массива. Изначально переходы, ведущие к местам *d1-d3*, показывающие, что соответствующие секции сравнения могут начать работу, доступны для срабатывания из-за того, что места *b1-b3* не содержат

меток. В начальных условиях места *a1-a3* также не содержат меток. Остальная логика работы части схемы с блокировками раскрывается ниже в процессе описания ее работы.

Все секции сравнения имеют одинаковое строение и отличаются лишь тем, какие разряды они представляют на рисунке 1.

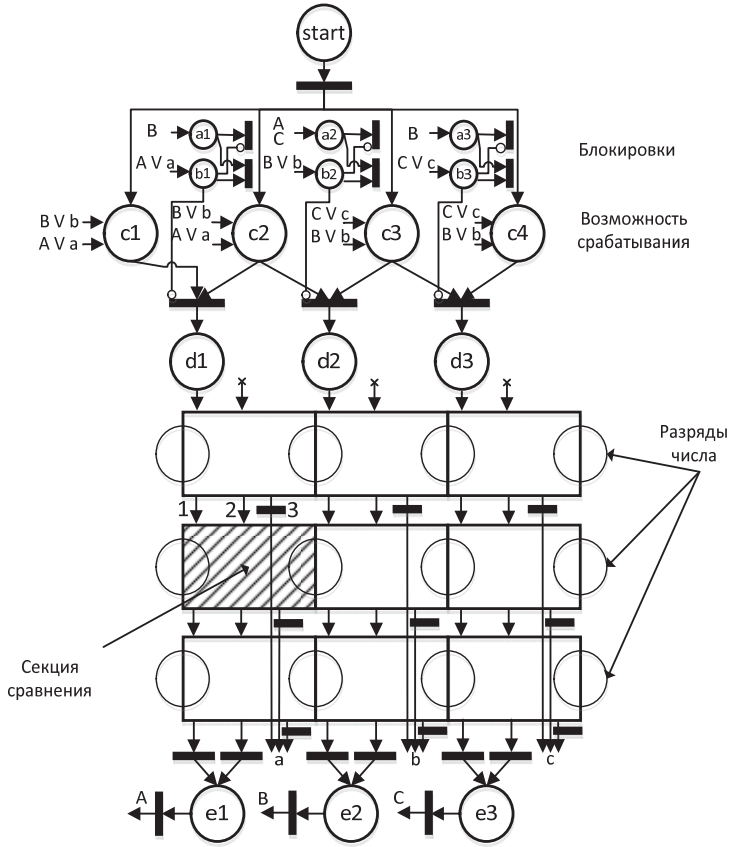


Рис. 1. Асинхронный алгоритм сортировки четырех трехразрядных чисел методом всплывающих пузырьков

Каждая секция сравнения содержит два входа – команду сравнения и команду перестановки разрядов. Самые верхние секции сравнения также содержат по два входа, но вход перестановки не соединен ни с каким местом из-за отсутствия необходимости смены всех чисел без предварительного сравнения (на рисунке изображен крестиком). Результатом сравнения двух разрядов могут быть не-

сколько исходов (изображены в виде переходов, исходящих из секции сравнения, и отмеченные цифрами 1-3): стрелка, отмеченная единицей, соответствует необходимости продолжения сравнения следующих разрядов. И она срабатывает при условии, что сравниваемые значения равны; двойка – поменять нижестоящие значения разрядов местами. Срабатывает при условии, что значение разряда слева больше чем значение разряда справа; тройка – закончить сравнение данной пары чисел. Срабатывает при условии, что левое число меньше правого. Результатом сравнения двух чисел является наличие меток в местах *e1-e3*. В вышеприведенных местах метки могут оказаться при равенстве сравниваемых чисел (срабатывание левого перехода) или перестановки чисел (правый переход). Далее метки из мест *e1-e3* переходят в места *a1-a3, b1-b3, c1-c4*. Рассмотрим работу переходов, связанных с местами *a1-a3, b1-b3,* на примере срабатывания переходов *a*, *A*.

Из места *e1* (переход *A*) метка переходит в места *c1*, *c2,* показывающие, что соответствующие числа массива не заняты (выполнено сравнение: числа равны или левое меньше правого), а также в место *b1* – для блокировки повторного срабатывания сравнения только что сравниваемых чисел, и в *a2* для снятия блокировки с соседних элементов (для мест, у которых есть левый и правый соседние элементы, также есть переходы для снятия блокировки с левого элемента).

При срабатывании перехода *a* (правое число больше левого) метка выполняет аналогичные переходы за исключением снятия блокировки с соседних элементов. Это связано с тем, что переход *a* означает, что числа упорядочены и не было выполнено перестановки. Окончанием работы приведенного алгоритма является блокировка переходов, ведущих к местам *d1-d3*, то есть наличие меток в местах *b1-b3*. Данного условия достаточно, так как метки из мест *b1-b3* могут быть удалены только при сравнении пар чисел, что не может быть из-за их блокировки. Переходы от меток *a1-a3*, *b1-b3* необходимы для того, чтобы снять блокировку с пар чисел. Возможны несколько вариантов: 1) место *b1* содержит метку, запрещающую сравнение первой пары чисел. Тогда она может быть снята, если в результате сравнения второй пары чисел сработал переход *B* и метка перешла в место *a1*. При этом срабатывает «нижний» переход для уничтожения блокирующей сравнение метки; 2) место *b1* не содержит метки, но в результате сравнения второй пары чисел сработал переход *B* и метка перешла в место *a1*. При этом срабатывает «верхний» переход (место *a1* содержит метку, а *b1* соединено ингибитор-

ной – запрещающей дугой с переходом) для уничтожения блокирующей сравнение метки.

На рисунке 2 приведена секция сравнения (на рисунке 1 она обозначена прямоугольником) двух *i*-тых разрядов. Входами для секции являются два перехода: команда сравнения чисел показана переходом *t1*, команда перестановки разрядов – переходом *t2*. Изначально метки со значениями разрядов чисел содержаться в местах *p1*, *p2*. Для большей наглядности на данном рисунке двунаправленной дугой показана пара дуг, идущих в противоположные направления.

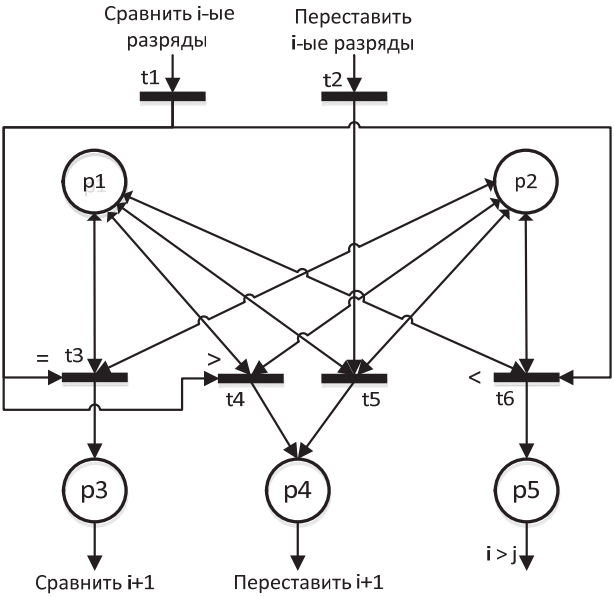


Рис. 2. Секция сравнения *i*-тых разрядов соседних чисел

При команде сравнения становится доступным для срабатывания один из переходов: *t3*, при условии, что значения в местах *p1* и *p2* одинаковы; *t4*, если значение в *p1* больше, чем в *p2*; *t6*, если значение в *p2* больше, чем в *p1*. При команде перестановки срабатывает переход *t5*, при котором метки меняются местами. В место *p3* метка попадает при условии, что значения в *p1* и *p2* одинаковы, в *p4* – если значение в *p1* больше чем в *p2* или при команде перестановки и в *p5* при условии, что значение в *p1* меньше чем в *p2*.

3. Реализация алгоритма сортировки. В качестве программного пакета для реализации приведенного алгоритма с использованием сетей Петри был выбран CPN Tools 4.0.1.

Реализация основной схемы (рисунок 1) разбита на несколько частей из-за громоздкости схемы и приведена на рисунке 3 и 4 (причем часть 2 на рисунке 4 является расширением части 1 на рисунке 3 и должна находиться вместо многоточия на рисунке 3). На рисунке 4 представлена часть схемы с набором секций сравнения для сортировки массива из четырех трехразрядных разрядов, на рисунке 3 часть с логикой блокировок.

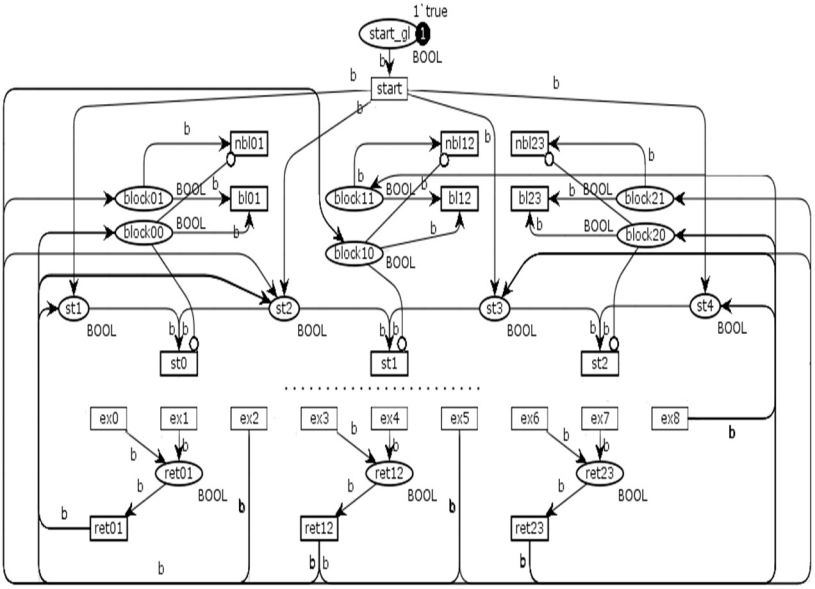


Рис. 3. Реализация алгоритма сортировки в сетях Петри: часть 1

Рассмотрим работу приведенной схемы. Работа алгоритма начинается с срабатывания перехода *start* (дуги, соединяющие переходы и метки, снабжены переменными, которые «переносят» значения меток) и перехода меток в места *st1-st4*. Переходы *st0-st2* при этом становятся доступными для срабатывания из-за того, что места *block00-block20* соединены ингибиторными дугами с переходами и не содержат меток. Через переходы *st0-st2* метки попадают в места *st0_in-st2_in* на рисунке 4.

На рисунке 4 приведена часть сети Петри предлагаемого алгоритма, изображенного на рисунке 1.

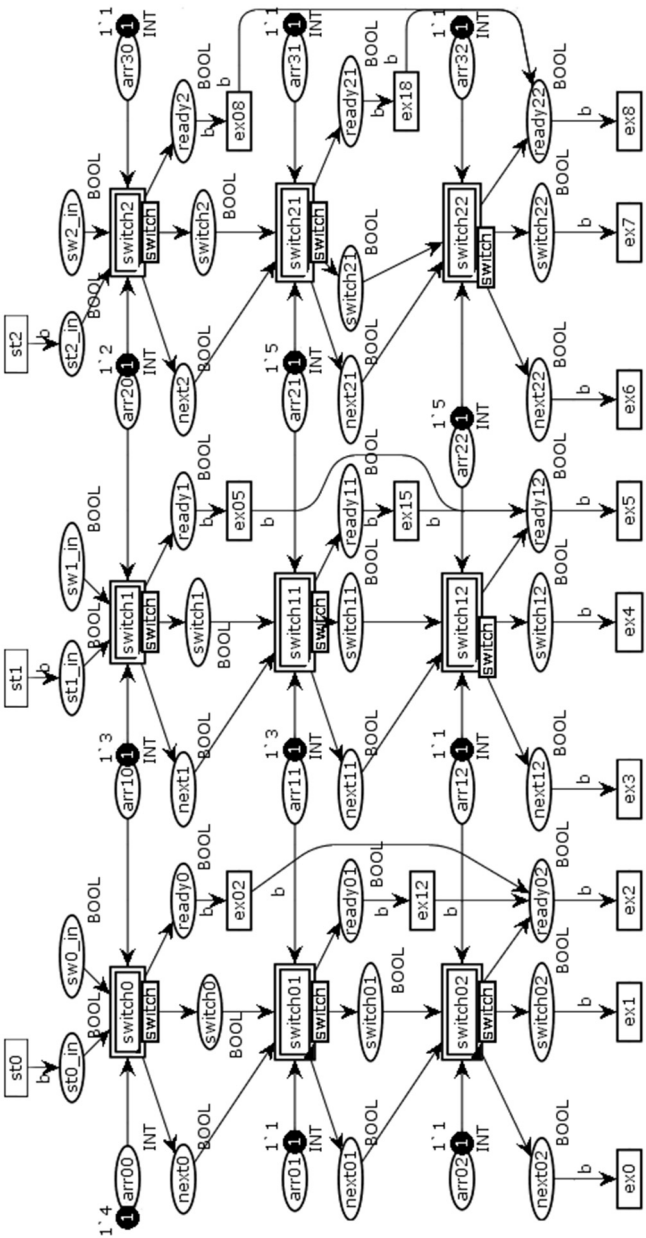


Рис. 4. Реализация алгоритма сортировки в сетях Петри: часть 2

В данной конкретной реализации использованы иерархические сети Петри, и переходы, отмеченные надписью *switch* в прямоугольнике, являются подсетью основной сети Петри, содержащие секции сравнения. Для реализации иерархических сетей Петри в CPN Tools необходимо соединить места в основной сети с входными/выходными местами в подсети. Таким образом, все места на рисунке 4 соединены с аналогичными местами с соответствующими секциями сравнения (рисунок 5). Например, для перехода *switch0* входные места *st0_in* и *sw0_in* соединены с местами *start* и *switch* соответственно, места *arr00* и *arr10* с *p1*, *p2* соответственно, а места *next0*, *switch0* и *ready0* с местами *next_out, switch_out* и *ready_out* соответственно. Остальные секции имеют аналогичное строение. Сами разряды чисел содержатся в местах *arr00-arr32 (array)* и представлены метками (в CPN Tools метки обозначаются записью «1`2», где 1 – число меток, 2 – их значение).

После последнего слоя секций сравнения метки могут находиться либо в местах *ret01-ret23*, либо в *ready02-ready22*, что соответствует тому, что сравниваемые элементы равны или были переставлены (*ret**), либо упорядочены (*ready**). При любом исходе метки переходят в места *st1-st4* (в зависимости от секции) и блокируют сравнение. Если метка оказалась в местах *ret01-ret23*, то дополнительно снимается блокировка для соседних элементов путем перехода метки в места *block01-block21* и срабатывания переходов *bl01-bl23*. Если в результате работы секции сравнения оказалось, что элементы упорядочены, то разблокировка соседних элементов не выполняется. Остановка работы приведенной сети выполняется, когда все пары соседних чисел заблокированы для сравнения, то есть метки находятся в местах *b1-b3*.

4. Реализация секции сравнения. На рисунке 5 представлена реализация секции сравнения двух разрядов (рисунок 2) соседних чисел. Данная схема является детализацией перехода *switch* на рисунке 4, а именно *switch0*. Места *p1*, *p2* связаны с местами *arr01*, *arr11*. Места *start* и *switch* показывают наличие команды на начало сравнения и перестановки соответственно. Выходные места *next_out, switch_out* и *ready_out* показывают результаты исполнения секции сравнения, два из которых (*next_out, switch_out*) передаются в следующие секции сравнения, а *ready_out* «собирается» в *ex2* в зависимости от секции.

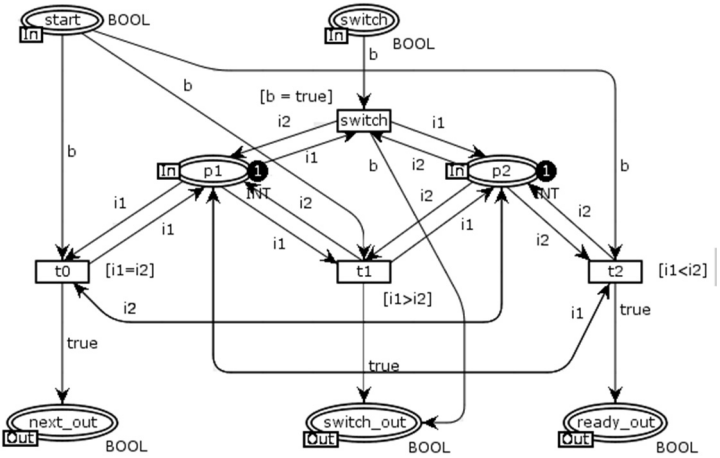


Рис. 5. Реализация секции сравнения алгоритма сортировки в сетях Петри

Переход *t0* срабатывает при условии, что метки в местах *p1* и *p2* равны (проверка осуществляется с помощью защитного условия «*i1=i2*» на переходе). При этом переменные *i1, i2* (с помощью которых выполняется «перенос» меток с места к переходу) не меняют местами исходные метки. При переходе *t1*, который срабатывает, если значение метки в *p1* больше, чем в *p2* (защитное условие «*i1>i2*»), исходные метки меняются местами (переменные *i1* и *i2* возвращаются в разные места). Переход *t2* срабатывает, если значение в *p1* меньше, чем в *p2* (защитное условие «*i1<i2*»).

5. Пример работы алгоритма. Рассмотрим работу полученной реализации алгоритма на примере сортировки следующего массива:

$$\{13, 12, 16, 15, 14, 1\},$$

который состоит только лишь из шести элементов для компактности изложения. В сетях Петри в случае возможности срабатывания нескольких переходов срабатывание любого из доступных является равновероятным событием. Поэтому при сортировке массива предложенным алгоритмом нет однозначной последовательности перестановок. Для вышеприведенного массива результат работы алгоритма приведен в таблице 1, где в левой колонке показан номер условных тактов (номеров срезов состояния массива) от начального до того момента как массив будет отсортирован. Сравниваемые пары на условных тактах выделены. В запуске, приведенном в средней колонке, на первом условном такте сравниваются пары чисел {12, 16} и {14, 15} (далее по

номерам индексов элементов массива считая с нулевого индекса). Так как в результате первого такта 1–4 элементы массива заблокированы, то на втором условном такте доступными для сравнения остаются пары {0, 1}, {2, 3} и {4, 5}. Третий условный такт сравнения совпадает с первым. На четвертом такте пара с индексами {0, 1} – заблокирована, остальные доступны для сравнения. На пятом такте сравниваются 1 и 2 элементы, и далее на шестом сравнение завершается парой {0, 1}.

Таблица 1. Сортировка массива из шести элементов методом всплывающих пузырьков

Номер условного такта	Состояние массива (запуск 1)	Состояние массива (запуск 2)
0	13 12 16 15 14 1	13 12 16 15 14 1
1	13 **12 16 14 15** 1	**12 13 15 16 1 14**
2	**12 13 14 16 1 15**	12 **13 15 1 16** 14
3	12 **13 14 1 16** 15	12 13 **1 15 14 16**
4	12 13 **1 14 15 16**	12 **1 13 14 15** 16
5	12 **1 13** 14 15 16	**1 12 13 14 15 16**
6	**1 12** 13 14 15 16	-

В данном примере сортировка массива выполнена за 6 условных тактов. В виду случайности выбора пар при различных запусках количество условных тактов может меняться. К примеру, тот же самый массив может быть отсортирован за другое количество условных тактов (таблица 1, запуск 2). В худшем случае сортировка будет выполнена за девять условных тактов.

6. Оценка быстродействия алгоритма. Рассмотрим оценку быстродействия приведенного алгоритма. Асимптотическая сложность классического алгоритма пузырьковой сортировки $O(n^2)$ [4], параллельный вариант чет-нечет сортировки $O(log(2n))$. Рассмотрим наилучший и наихудший возможные случаи оценки.

В наилучшем случае массив уже отсортирован, тогда после сравнения соседних элементов массива будут заблокированы непосредственно сравниваемые элементы, а метки для снятия блокировки с соседних элементов не будут переходить в места для снятия блокировок. Иллюстрация вариантов разбиения массива на пары соседних элементов на примере массива из шести элементов приведена на рисунке 6. В верхней его части представлены два варианта, когда весь массив разбивается через один элемент. В таких случаях для разбиения на пары всего массива требуется по три условных такта. В нижней части рисунка представлено разбиение, в котором нет пропусков элементов. В данном случае для полного разбиения массива требуется всего

два условных такта. Таким образом, для полной сортировки всего массива требуется 3 и 2 тактов соответственно.

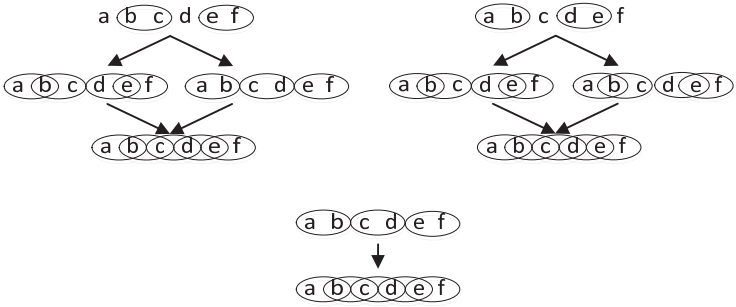


Рис. 6. Возможные варианты разбиения массива на пары чисел

В наихудшем случае массив отсортирован в обратном порядке, если учитывать, что в реализации пузырьковой сортировки необходимо совершить $n\text{-}1 + n\text{-}2 + n\text{-}3 \ldots + 1 = (n + 1 - 1)*n/2 = n^2/2$ сравнений [4]. Учитывая, что в предлагаемом алгоритме в среднем одновременно может выполняться $n/2$ или $n/3$ действий (перестановка или сравнение), то общее количество действий будет $(n^2/2)/(n/2) = n$ или $(n^2/2)/(n/3) = 3n/2$ в зависимости от разбиения массива на пары соседних элементов.

Для оценки быстродействия в среднем следует оценить математическое ожидание функции распределения возможного количества пар соседних элементов. Например, для массива из 16 элементов 8 пар возможны в 1 комбинации, 7 пар – 28 комбинаций, 6 пары – 32 комбинации, 5 пар – 1 комбинация. Тогда математическое ожидание примерно соответствует шести парам. То есть на одном условном такте выполняется анализ шести пар чисел, что лежит между худшим и лучшим случаями.

7. Заключение. В статье продемонстрирована возможность использования сетей Петри с целью распараллеливания процессов обработки информации, что в данном случае выполнено на примере классической задачи сортировки массивов. Приводится обобщенный алгоритм пузырьковой сортировки, который позволяет выполнять параллельную асинхронную сортировку массива элементов. В приведенной в работе реализации алгоритма с использованием сети Петри используется представление числа в поразрядном виде, и, в частности, возможна обработка чисел в двоичном виде. При необходимости числа могут быть свернуты и тогда они будут представлены в виде одного

слоя секций сравнения (рисунок 1). Приведен иллюстративный пример работы сортировки массива.

Принципы, примененные для построения алгоритма, могут быть применены к другим типам сортировки, например, сортировки слиянием или быстрой сортировки, что и является целью дальнейших исследований.

Выполнена оценка быстродействия приведенного алгоритма для наилучшего и наихудших случаев. В наилучшем случае, когда массив уже отсортирован, рассматриваемый алгоритм выполняется за 2 или 3 условных такта в зависимости от разбиения массива на пары соседних элементов. В наихудшем случае – за n или за $3n/2$, где n – число элементов.

Литература

1. *Wilkinson B., Allen M.* Parallel Programming: Techniques and Applications Using Networked Workstations and Parallel Computers (2nd Edition) // Pearson Education. 2005. 431 p.
2. *Kirk D.B., Hwu W.W.* Programming Massively Parallel Processors, Second Edition: A Hands-on Approach // Morgan Kaufmann. 2012. 496 p.
3. *Малышкин В. Э., Корнеев В. Д.* Параллельное программирование мультикомпьютеров // Издательство НГТУ. 2011. 296 с.
4. *Cormen T., Leiserson C., Rivest R., Stein C.* Introduction to Algorithms: 3rd Edition // The MIT Press. 2009. 1328 p.
5. *Jan B., Montrucchio B., Ragusa C., Khan F. G., Khan O.* Fast parallel sorting algorithms on GPUs // International Journal of Distributed and Parallel Systems (IJDPS). 2012. pp. 107–118.
6. *Inoue H., Moriyama T., Komatsu H., Nakatani T.* AA-Sort: A New Parallel Sorting Algorithm for Multi-Core SIMD Processors // Proceedings on 16th International Conference on Parallel Architecture and Compilation Techniques (PACT 2007). 2007. pp. 189–198.
7. *Capannini, G., Silvestri F., Baraglia R.* Sorting on GPUs for large scale datasets: A thorough comparison // Information Processing and Management. 2011. vol. 48(5). pp. 903–917.
8. *Haykin S.* Neural Networks and Learning Machines, 3rd Edition // Pearson Education. 2009. 938 p.
9. *Graves A. Wayne G., Danihelka I.* Neural Turing Machines // The Computing Research Repository 1410. 5401. 2014. pp. 1–24.
10. *Воевода А.А., Полубинский В. Л., Романников Д.О.* Сортировка массива целых чисел с использованием нейронной сети // Научный Вестник НГТУ. 2016. №2(63). С. 151–157.
11. *Коротиков С.В., Саркенов Д.О.* Применение спецификации эквивалентности в моделировании сеанса связи таксофона и центра дистанционного контроля и управления таксофонами раскрашенной сетью Петри // Сб. науч. тр. НГТУ. 2007. № 3 (49). С. 97–104.
12. *Марков А.В.* Автоматизация проектирования и анализа программного обеспечения с использованием языка UML и сетей Петри: дисс. канд. техн. наук // Новосибирск. 2015. 176 с.

13. *Воевода А.А., Марков А.В., Романников Д.О.* Разработка программного обеспечения: проектирование с использованием UML диаграмм и сетей Петри на примере АСУ ТП водонапорной станции // Труды СПИИРАН. 2014. №3(34). С. 218–232.
14. *Марков А.В.* Поиск манипулятором кратчайшего пути в лабиринте // Сб. науч. тр. НГТУ. 2011. №4(66). С. 75–90.
15. *Марков А.В., Воевода А.А.* Развитие системы “Перемещение манипулятора в пространстве с препятствиями” при помощи рекурсивных функций // Автоматика и программная инженерия. №2(4). 2013. С. 35–41.
16. *Марков А.В.* Свойства инверсии сетей Петри // Сб. науч. тр. НГТУ. 2014. №4(78). С. 139–152.

Воевода Александр Александрович — д-р техн. наук, профессор, профессор кафедры автоматики, Новосибирский государственный технический университет. Область научных интересов: полиномиальный синтез, сети Петри, UML диаграммы. Число научных публикаций — 200. voevoda@ucit.ru; пр. Карла Маркса 20, Новосибирск, 630073; р.т.: +79139223092.

Романников Дмитрий Олегович — к-т техн. наук, доцент, доцент кафедры автоматики, Новосибирский государственный технический университет. Область научных интересов: машинное обучение, нейронные сети, сети Петри. Число научных публикаций — 45. dmitry.romannikov@gmail.com; пр. Карла Маркса 20, Новосибирск, 630073; р.т.: +7 961 223 8567.

Поддержка исследований. Работа выполнена при финансовой поддержке Министерства образования и науки РФ (проект № 2014/138).

A.A. VOEVODA, D.O. ROMANNIKOV

ASYNCHRONOUS SORTING ALGORITHM FOR ARRAY OF NUMBERS WITH THE USE OF INHIBITORY PETRI NETS

Voevoda A.A., Romannikov D.O. **Asynchronous Sorting Algorithm for Array of Numbers With the use of Inhibitory Petri Nets.**

Abstract. Currently the tasks of computations speed-up and/or their optimization are actual ones. Among the ways to solve these tasks is a method of parallelization and asynchronization of a sorting algorithm, which is considered in the article. We offer a sorting method that is based on the principle of dividing an array into a set of independent pairs of numbers and their parallel and asynchronous comparison, which distinguishes the offered method from the traditional sorting algorithms (like quick sorting, merge sorting, insertion sorting and others). The algorithm is realized with the use of Petri nets as the most suitable tool for describing asynchronous systems. Examples of its work are given. The performance of the algorithm is evaluated for the best and the worst cases. In the best case the algorithm is executed for 2 or 3 conditional tacks depending on an array partition into the pairs of adjacent elements. In the worst case –for n or 3n/2, where n is the number of elements. Parallelization and asynchronization principles, used during the algorithm construction, can also be used for different algorithms.

Keywords: sorting algorithms, bubble sorting, Petri nets, asynchronous, parallel processing.

Voevoda Alexandr Aleksandrovich — Ph.D., Dr. Sci., professor, professor of automation department, Novosibirsk State Technical University. Research interests: polynomial synthesis, UML diagrams, Petri nets. The number of publications — 200. voevoda@ucit.ru; 20, Karl Marx Avenue, Novosibirsk, 630073; office phone: +79139223092.

Romannikov Dmitry Olegovich — Ph.D., associate professor, associate professor of automation department, Novosibirsk State Technical University. Research interests: machine learning, neural networks, Petri nets.. The number of publications — 45. dmitry.romannikov@gmail.com; 20, Karl Marx Avenue, Novosibirsk, 630073; office phone: +7 961 223 8567.

Acknowledgements. This research is supported by RFBR (grant 2014/138).

References

1. Wilkinson B., Allen M. Parallel Programming: Techniques and Applications Using Networked Workstations and Parallel Computers (2nd Edition). Pearson Education. 2005. 431 p.
2. Kirk D.B., Hwu W.W. Programming Massively Parallel Processors, Second Edition: A Hands-on Approach. Morgan Kaufmann. 2012. 496 p.
3. Malyshkin V.Je., Korneev V.D. *Parallel'noe programmirovanie mul'tikomp'juterov* [Parallel programming of multicomputers]. Izdatel'stvo NGTU. 2011. 296 p. (In Russ.).
4. Cormen T., Leiserson C., Rivest R., Stein C. Introduction to Algorithms: 3rd Edition. The MIT Press. 2009. 1328 p.
5. Jan B., Montrucchio B., Ragusa C., Khan F. G., Khan O. Fast parallel sorting algorithms on GPUs. *International Journal of Distributed and Parallel Systems (IJDPS)*. 2012. pp. 107–118.
6. Inoue H., Moriyama T., Komatsu H., Nakatani T. AA-Sort: A New Parallel Sorting Algorithm for Multi-Core SIMD Processors. Proceedings on 16th International Con-

ference on Parallel Architecture and Compilation Techniques (PACT 2007). 2007. pp. 189–198.
7. Capannini, G., Silvestri F., Baraglia R. Sorting on GPUs for large scale datasets: A thorough comparison. *Information Processing and Management*. 2011. vol. 48 (5). pp. 903–917.
8. Haykin S. Neural Networks and Learning Machines: 3rd Edition. Pearson Education. 2009. 938 p.
9. Graves A. Wayne G., Danihelka I. Neural Turing Machines. The Computing Research Repository 1410.5401. 2014. pp. 1–24.
10. Voevoda A.A., Polubinskij V. L., Romannikov D.O. Array of integers sorting with a using of a neural network. *Nauchnyj Vestnik NGTU – Science Bulletin of NSTU*. 2016. vol. 2 (63). pp. 151–157. (In Russ.)
11. Korotikov S.V., Sarkenov D.O. Application Specification equivalence in the modeling session payphone and remote monitoring and control center payphones colored Petri net. *Sb. nauch. tr. NGTU – Collection of scientific works of NSTU*. 2007. № 3 (49). pp. 97–104. (In Russ.).
12. Markov A.V. *Avtomatizacija proektirovanijai analiza programmnogo obespechenijas ispol'zovaniem jazyka UML i setej Petri diss. kand. tehn. nauk* [Design automation and the analysis of the software with use of the UML language and Petri nets. Ph.D. thesis]. Novosibirsk: 2007. 176 p. (In Russ.).
13. Voevoda A.A., Markov A.V., Romannikov D.O. Software development: design using UML diagrams and Petri nets on the example of PCS pumping station. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2014. vol. 3 (34). pp. 218–232. (In Russ.).
14. Markov A.V. Search manipulator shortest path in a maze. *Sb. nauch. tr. NGTU – Collection of scientific works of NSTU*. 2011. vol. 4(66). pp. 75–90.
15. Markov A.V. Voevoda A.A. Development of the system "manipulator move in space with obstacles" with recursive functions. *Avtomatika i programmnaja inzhenerija – Automation and Software Engineering*. 2013. no. 2(4). pp. 35–41.
16. Markov A.V. Properties of Petri nets inversion. *Sb. nauch. tr. NGTU – Collection of scientific works of NSTU*. 2014. vol. 4(78). pp. 139–152.

УДК 004.93; 004.932 **DOI** 10.15622/sp.48.11

А.Ю. Каплин, А.А. Коротин, А.В. Назаров, В.Л. Якимов

АЛГОРИТМ КЛАССИФИКАЦИИ ГРУППОВЫХ ТОЧЕЧНЫХ ОБЪЕКТОВ С НЕУПОРЯДОЧЕННЫМИ ЭЛЕМЕНТАМИ НА ОСНОВЕ ВЕРОЯТНОСТНОЙ МЕРЫ БЛИЗОСТИ

Каплин А.Ю., Коротин А.А., Назаров А.В., Якимов В.Л. **Алгоритм классификации групповых точечных объектов с неупорядоченными элементами на основе вероятностной меры близости.**

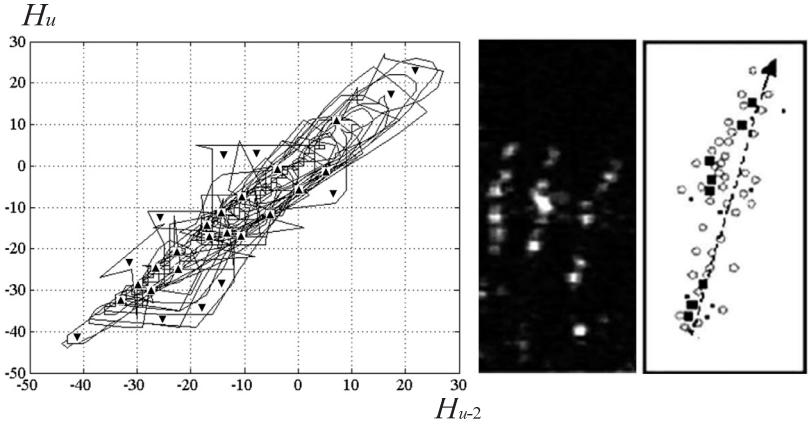
Аннотация. Представлен алгоритм классификации групповых точечных объектов (ГТО), основанный на сравнительном анализе фрагментов искаженных образов и шаблонов ГТО. В качестве фрагментов использованы последовательности элементов ГТО различной длины. В качестве признаков классификации выступают попарные и угловые межточечные расстояния. При решении задачи классификации используется вероятностная мера близости, задаваемая экспертом с помощью функции принадлежности и закона распределения вероятности дискретных значений признаков классифицируемых объектов. Алгоритм включает следующие этапы: поиск и сравнение состава фрагментов искаженных образов и шаблонов ГТО; формирование вероятностной оценки близости искаженного образа ГТО и каждого шаблона в пространстве рассматриваемых признаков по результатам анализа каждого фрагмента; накопление полученных вероятностей по результатам анализа всех фрагментов искаженного образа; ранжирование полученных вероятностей отнесения искаженного образа к шаблонам ГТО; определение наиболее вероятного шаблона. В алгоритме предусмотрена возможность уточнения класса искаженного образа ГТО за счет использования логических правил и аналитических выражений рассматриваемой предметной области. Приведены пример и результаты применения данного алгоритма для решения задачи классификации реальных ГТО на основе анализа их фрагментов в виде последовательностей из двух и трех элементов.

Ключевые слова: групповой точечный объект, классификация, вероятностная мера близости.

1. Введение. Широкий класс задач обработки информации в современных информационных системах может быть связан с извлечением информации из изображений, представленных в виде компактного множества изолированных друг от друга точечных отметок — групповых точечных объектов (ГТО), обладающих формой и внутренней структурой, причем точки ГТО могут быть объектами различного типа [1, 2]. Одной из таких задач является идентификация ГТО, для решения которой необходимо разработать алгоритм классификации, позволяющий принять решение о классе ГТО с требуемой достоверностью [3].

На рисунке 1 представлены два различных примера ГТО для которых решение задачи идентификации имеет схожий характер и элементами которых являются: а) набор точек одной из проекций фазового пространства динамической системы ориентации малого космического аппарата, характеризующий ее техническое состояние и полученный на основе значений временного ряда H_u телеметрируемого па-

раметра ориентации на Землю, где *и* — номер отсчета телеметрируемого параметра3[4]; б) набор точек, образующий точечную модель одного из трех кораблей, полученный в результате обработки радиолокационного изображения [5, 6]. Для указанных примеров точки ГТО соответствовали: областям высокой и низкой плотности фазовых траекторий (рисунок 1а); областям радиолокационного изображения с различными уровнями яркости (рисунок 1б). В первом случае объект ГТО образован точками двух типов («▲», «▼»), а во втором — точками трех типов («■», «●»,«○»).



а) б)

Рис. 1. Примеры ГТО из области: а) технической диагностики [4]; б) радиолокации [5, 6]

В общем случае решение задачи классификации ГТО может быть затруднено вследствие различного рода искажений, отсутствия ключевых точек (элементов ГТО), ложного определения типа элементов, неупорядоченности элементов и т. д.

Существуют различные подходы к определению ключевых элементов ГТО, формированию множества признаков классификации и решению задачи их распознавания. Наиболее обширной является категория алгоритмов обработки и распознавания объектов на изображении [3, 5, 7, 8]. При этом важнейшей задачей, предшествующей распознаванию ГТО на изображении, является задача достоверного обнаружения ключевых элементов ГТО. Для ее решения используются подходы на основе преобразований исходного изображения, позволяющих получить инвариантные признаки обнаруживаемых объектов; на основе алгоритмов детекции границ и различных фильтров и т. д. [9].

Большой класс методов обработки изображений и сигналов для классификации ГТО предлагает контурный анализ и его приложения [10]. Рассмотрение ГТО в виде квантернионных сигналов позволяет эффективно решать задачу их обнаружения на основе согласованной фильтрации [2, 10]. Так как ГТО представляют собой геометрические объекты, то в качестве признаков их классификации обычно используют различные межточечные и угловые расстояния [11, 12, 13]. После обнаружения элементов ГТО и определения множества признаков их классификации для решения задачи распознавания ГТО могут быть использованы различные методы, которые можно разделить на две большие группы, определяемые как геометрический (дискриминантный) и синтаксический (структурный) подходы [10].

В разработанном алгоритме для решения задачи классификации используется информация о сформированных моделях (шаблонах) ГТО в пространстве рассматриваемых признаков (межточечных и угловых расстояний), а основными критериями при его разработке были следующие: простота реализации и возможность использования современных технологий поиска в базах данных большой размерности, возможность получения именно вероятностной оценки отнесения текущего искаженного образа к каждому из множества шаблонов ГТО, удобная возможность использования при классификации дополнительной априорной информации в виде уточняющих экспертных правил.

2. Постановка задачи классификации ГТО. Решение задачи классификации ГТО можно разбить на три этапа:

– выделение признаков классификации ГТО, формирование базы шаблонов с массивами значений рассмотренных признаков;

– поиск в базе и соотнесение текущего искаженного образа ГТО со множеством шаблонов в пространстве рассматриваемых признаков;

– формирование вероятностной оценки для каждого претендента из базы шаблонов, ранжирование претендентов в соответствии с полученной вероятностной оценкой, принятие решения о наиболее вероятном претенденте.

В ходе решения задачи классификации необходимо синтезировать алгоритм *f*:

$$\mathbf{Y} = f(\hat{\mathbf{S}}, \mathbf{S}_1, \mathbf{S}_2, ... \mathbf{S}_N), \tag{1}$$

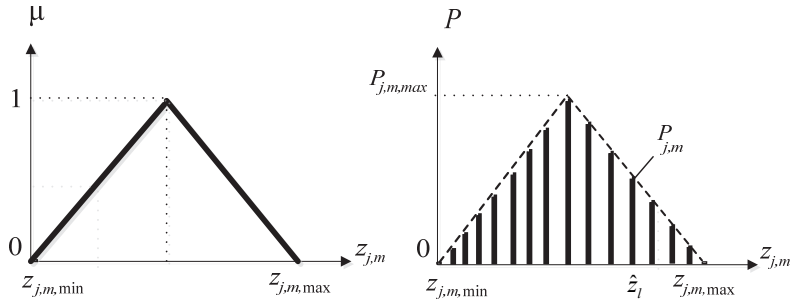
где $\hat{\mathrm{S}} = (\hat{z}_1, \hat{z}_2, ..., \hat{z}_L)$ — входной искаженный образ ГТО; $\hat{z}_l$ — признаки искаженного образа ГТО; l=1…L — номер признака искаженного ГТО; L — количество признаков искаженного образа ГТО;

$\mathbf{S}_j = (z_{j,1}, z_{j,2}, ..., z_{j,N_j})$ — j-й шаблон ГТО; $z_{j,m}$ — признак j-го шаблона ГТО; $m = 1 \ldots N_j$ — номер признака j-го шаблона ГТО; N_j — количество признаков j-го шаблона ГТО; N — количество шаблонов ГТО; $\mathbf{Y}$ — код шаблона ГТО (номер класса), поставленный в соответствие искаженному образу $\hat{\mathbf{S}}$. При этом алгоритм классификации $\boldsymbol{f}$ реализуется на основе вычисления меры близости между искаженным образом и шаблонами ГТО в пространстве указанных признаков [3, 10].

В общем случае признаки ГТО могут быть не равноценны и вносить различный вклад в значение вероятности отнесения искаженного образа $\hat{\mathbf{S}}$ к шаблонам $\mathbf{S}_j$ [14]. Так как образы ГТО искажены, а имеющиеся в базе шаблоны ГТО пересекаются в пространстве рассматриваемых признаков и зачастую имеют, одинаковые фрагменты, используем вероятностную меру для оценки близости искаженного образа и множества шаблонов [15, 16]. В отсутствии статистической информации о распределении значений признаков, зависимости этих распределений от внешних факторов (например, для наземных ГТО размещение элементов может сильно зависеть от рельефа и характера местности) и их статистической независимости, для выполнения такой процедуры можно использовать функции принадлежности, задаваемые экспертом [17]. Вероятностный метод построения функций принадлежности основан на сходстве понятий нечеткости и вероятности [17, 18]. При формировании функции принадлежности необходимо учесть, что маловероятное и наиболее вероятное событие должно иметь соответственно малую и максимальную степень принадлежности [17, 18, 19]. Будем считать признаки ГТО $z_{j,m}$ и $\hat{z}_l$ дискретными случайными величинами.

На рисунке 2 представлены функция принадлежности и закон распределения дискретной случайной величины $z_{j,m}$ — одного из m признаков j-го шаблона ГТО. Вероятность $P_{j,m}$ является условной вероятностью отнесения искаженного образа ГТО к j-му шаблону при условии, что значение его признака $\hat{z}_l$ равно некоторому дискретному значению на шкале признака $z_{j,m}$. Так как случайная величина $z_{j,m}$ дискретная и принимает строго фиксированные значения в пределах от $z_{j,m,\min}$ до $z_{j,m,\max}$, то ее закон распределения и максимальное значение вероятности $P_{j,m,\max}$ должны быть одинаковы для всех признаков шаблонов ГТО, а сумма вероятностей $P_{j,m}$ по всем возможным дискретным

значениям величины $z_{j,m}$ должна быть равна 1, что позволит обеспечить равнозначность признаков классификации (рисунок 2).



а) б)

Рис. 2. Функция принадлежности (а) и закон распределения дискретной случайной величины $z_{j,m}$ (б)

Элементы ГТО, в общем случае, не упорядочены, а номера признаков ГТО l и m — могут не совпадать [1]. Это требует процедуры сравнения искаженного образа ГТО по каждому признаку $\hat{z}_l$ с каждым j-м шаблоном по каждому признаку $z_{j,m}$ и получения вероятностей $P_{j,l,m}$ отнесения искаженного образа ГТО по признакам $\hat{z}_l$ к j-м шаблонам по признакам $z_{j,m}$. Анализируя вероятности $P_{j,l,m}$, найдем максимальное значение вероятности $P_{j,l}$ отнесения искаженного образа ГТО по каждому признаку $\hat{z}_l$ к каждому j-му шаблону, используя следующее правило:

$$P_{j,l} = \max_{m} \left\{ P_{j,l,m} \right\}. \tag{2}$$

Допуская статистическую независимость признаков $\hat{z}_l$, оценим вероятности P_j отнесения искаженного образа ГТО к j-м шаблонам по совокупности L признаков:

$$P_j = \frac{1}{L} \sum_{l=1}^{L} P_{j,l}. \tag{3}$$

Решением задачи классификации (1) будет номер шаблона ξ, соответствующий значению максимальной вероятности P_j:

$$\mathbf{Y} = \xi \left| P_\xi = \max_j \left\{ P_j \right\} \right. \tag{4}$$

Для оценки качества классификации используем показатель достоверности G:

$$G = \frac{\sum_{g=1}^{N_p} \delta(\mathbf{Y}_g^*, \mathbf{Y}_g)}{N_p}, G \geq G_{\text{зад.}};$$
$$\delta(\mathbf{Y}_g^*, \mathbf{Y}_g) = \begin{cases} 1, \mathbf{Y}_g = \mathbf{Y}_g^*; \\ 0, \mathbf{Y}_g \neq \mathbf{Y}_g^*, \end{cases} \quad (5)$$

где $\mathbf{Y}_g^*$ — код (номер) шаблона ГТО на выходе классификатора при подаче на его вход искаженного образа ГТО $\hat{\mathbf{S}}_g$; $\mathbf{Y}_g$ — истинное значение кода шаблона ГТО при подаче на его вход искаженного образа $\hat{\mathbf{S}}_g$; g — номер тестового примера ГТО, g=1…N_p; N_p — количество примеров ГТО, используемых для тестирования; $G_{\text{зад.}}$ — заданное значение достоверности классификации; $\delta(\mathbf{Y}_g^*, \mathbf{Y}_g)$ — символ Кронекера.

Рассмотрим в качестве признаков ГТО попарные расстояния между элементами (эвклидовы расстояния), а также углы, вычисляемые на основе теоремы косинусов с использованием полученных расстояний [12, 13].

3. Формирование базы шаблонов ГТО. В качестве шаблонов ГТО будем рассматривать наборы элементов различного типа: 1, 2, 3… (рисунок 3). Положение элементов ГТО задано координатами x_i, y_i, i=1…n, i — номер элемента, n — количество элементов. Величина n для различных шаблонов ГТО может различаться. Количество шаблонов N определяется требованиями к задаче классификации. Каждый шаблон можно представить в виде совокупности признаков, размещенных, к примеру, в виде таблицы.

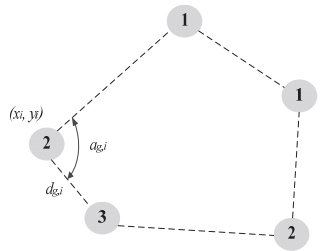


Рис. 3. Шаблон ГТО

Для формирования базы шаблонов выполним следующую последовательность действий:

Шаг 1. Сформируем шаблоны ГТО $\mathbf{S}_j$ в виде набора элементов различного типа: 1, 2, 3, ... (рисунок 3).

Шаг 2. Выбираем шаблон ГТО $\mathbf{S}_j$ и формируем последовательности элементов различной длины: «11232», «1122», «123»,… Для каждого i-го элемента вычисляем расстояния $d_{j,i}$ и углы $a_{j,i}$, а также ставим в соответствие минимальную и максимальную границу признаков $d_{j,i,\min}$, $\alpha_{j,i,\min}$, $d_{j,i,\max}$, $\alpha_{j,i,\max}$, используя дополнительные экспертные знания о предметной области [13]. Например: $d_{j,i,\min} = 0$, $\alpha_{j,i,\min} = \alpha_{j,i} - 45^0$, $d_{j,i,\max} = 2d_{j,i}$, $\alpha_{j,i,\max} = \alpha_{j,i} + 45^0$. Углы $\alpha_{j,i}$ определяем на основе сторон образованных элементами ГТО треугольников по теореме косинусов. Таким образом, описываем каждый шаблон $\mathbf{S}_j$ последовательностями элементов и соответствующих им строк в массиве значений признаков: ($d_{j,i}$, $\alpha_{j,i}$, $d_{j,i,\min}$, $\alpha_{j,i,\min}$, $d_{j,i,\max}$, $\alpha_{j,i,\max}$).

Шаг 3. Выполним шаг 2 для каждого j-го шаблона и пополним данными таблицу 1.

Таблица 1. Пример базы шаблонов ГТО

Шаблоны ГТО $\mathbf{S}_j$	Последовательности i-х элементов ГТО		Признаки $d_{j,i}$	Признаки $\alpha_{j,i}$	Граничные значения признаков				Доп. эксперт. правила $\Lambda_{j,q}$
	Номер послед. q	Послед.			$d_{j,i,\min}$	$\alpha_{j,i,\min}$	$d_{j,i,\max}$	$\alpha_{j,i,\max}$	
$\mathbf{S}_1$	1	123123	5,5,5…	30,40,23,…	0,0,0,…	α-45	10,10,10,…	α+45	$\Lambda_{1,1}$
	2	1231	10,3,5…	30,50,23,…	0,0,0,…	α-45	20,6,10,…	α+45	$\Lambda_{1,2}$
	…		…	…	…	…	…	…	….
$\mathbf{S}_2$	1	122122	10,5,5…	10,40,25,…	0,0,0,…	α-45	20,10,10,…	α+45	$\Lambda_{2,1}$
	2	2212	10,4,5…	20,50,2,…	0,0,0,…	α-45	20,8,10,…	α+45	–
	3	1221	10,2,5…	30,60,8,…	0,0,0,…	α-45	20,4,10,…	α+45	$\Lambda_{2,3}$
	…		…	…	…	…	…	…	…
…	…		…	…	…	…	…	…	…
$\mathbf{S}_N$	…		…	…	…	…	…	…	…

Количество последовательностей $N_{\text{посл.}}$ по каждому шаблону связано с количеством элементов ГТО n следующим образом:

$$N_{\text{посл.}} = \sum_{i=2}^{n} \frac{n!}{i!(n-i)!} = 2^n - n - 1. \quad (6)$$

Классификация ГТО на основе представленной в таблице информации сводится к решению задачи оптимального поиска в базе данных большой размерности. С учетом возможностей современных ПЭВМ осуществить поиск оптимального решения в представленной таблице за приемлемое время при использовании небольших ГТО ($n \leq 20$) не представляет большого труда. Учитывая, что при описании сложных ГТО ($n > 100$) можно ограничиться рассмотрением небольшого количества ключевых объектов, данный подход может быть применим для решения широкого класса задач. Тем не менее при больших n, значимой проблемой может стать низкая оперативность решения задачи классификации.

Оперативность можно повысить, ограничившись рассмотрением последовательностей из двух и трех элементов ГТО. Причем, если в первом случае в качестве признаков классификации ГТО могут быть использованы лишь попарные расстояния между элементами (таблица 2), то во втором случае их количество можно расширить за счет рассмотрения углов между образованными сторонами треугольников (таблица 3), что должно благоприятно отразиться на достоверности классификации.

Количество последовательностей $N_{\text{посл.}}$ по каждому шаблону в таблице 2 связано с количеством элементов ГТО n следующим образом:

$$N_{\text{посл.}} = \frac{n!}{2!(n-2)!}, \quad (7)$$

а в таблице 3 соответственно:

$$N_{\text{посл.}} = \frac{n!}{3!(n-3)!}. \quad (8)$$

Таблица 2. Пример базы шаблонов ГТО

Шаблоны ГТО $\mathbf{S}_j$	Последовательности i-х элементов ГТО		Признаки $d_{j,i}$	Граничные значения признаков		Доп. эксперт. правила $\Lambda_{j,q}$
	Номер послед. q	Послед.		$d_{j,i,\min}$	$d_{j,i,\max}$	
$\mathbf{S}_1$	1	12	5	0	10	$\Lambda_{1,1}$
	2	13	10	0	20	$\Lambda_{1,2}$
	3	23	10	0	20	–
	4	14	5	0	10	–
	…		…	…	…	….
$\mathbf{S}_2$	1	12	6	0	12	$\Lambda_{2,1}$
	2	13	16	0	32	–
	…		…	…	…	…
…	…		…	…	…	…
$\mathbf{S}_N$	…		…	…	…	…

Таблица 3. Пример базы шаблонов ГТО

Шаблоны ГТО $\mathbf{S}_j$	Последовательности элементов ГТО		Признаки $d_{j,i}$	Признаки $\alpha_{j,i}$	Граничные значения признаков				Доп. эксперт. правила $\Lambda_{j,q}$
	Номер послед. q	Послед.			$d_{j,i,\min}$	$\alpha_{j,i,\min}$	$d_{j,i,\max}$	$\alpha_{j,i,\max}$	
$\mathbf{S}_1$	1	123	5,5,5	30	0,0,0	α-45	10,10, 10	α+45	$\Lambda_{1,1}$
	2	124	10,3,5	50	0,0,0	α-45	10,6, 10	α+45	$\Lambda_{1,2}$
	…		…	…	…	…	…	…	….
$\mathbf{S}_2$	1	123	10,5,5	40	0,0,0	α-45	20,10, 10	α+45	$\Lambda_{2,1}$
	2	134	10,4,5	25	0,0,0	α-45	20,8, 10	α+45	0
	…		…	…	…	…	…	…	…
…	…		…	…	…	…	…	…	…
$\mathbf{S}_N$	…		…	…	…	…	…	…	…

Учитывая значительный размер представленных таблиц, в базе шаблонов ГТО могут храниться лишь координаты их элементов и экспертные правила, а все представленные в таблицах 1-3 последовательности элементов различной длины, попарные расстояния, углы, а так-

же граничные значения признаков могут быть вычислены в процессе реализации алгоритма классификации.

В качестве экспертных правил могут выступать различные логические условия, позволяющие улучшить решение задачи классификации. К примеру, если элементы ГТО представляют собой разнотипные объекты, размещенные на местности, то в качестве таких правил могут быть использованы логические условия размещения данных объектов взависимости от характера местности, что позволит уточнить координаты элементов ГТО и улучшить решение задачи классификации.

4. Последовательный алгоритм распознавания искаженного образа и формирования вероятностной оценки отнесения его к множеству шаблонов ГТО. Рассмотрим одну из реализаций алгоритма классификации ГТО в пространстве перечисленных выше признаков с учетом (1-5).

Шаг 1. Формируем набор искаженных неполных образов ГТО с ложными элементами из имеющейся базы шаблонов при различных среднеквадратичных отклонениях координат их элементов σ и углах поворота φ, задаваемых в пределах, указанных экспертом.

Шаг 2. Вводим переменную g – номер искаженного образа ГТО, $g = 1$. Выбираем $\hat{\mathbf{S}}_g$ (рисунок 4).

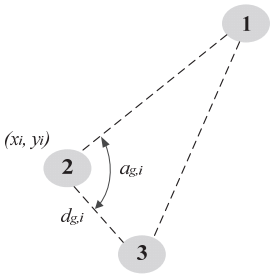


Рис. 4. Пример искаженного образа ГТО

Шаг 3. Вводим переменную j — номер анализируемого шаблона, $j = 1$. Выбираем шаблон $\mathbf{S}_j$ из базы шаблонов.

Шаг 4. Вводим переменные: r — номер анализируемой последовательности искаженного образа ГТО, $r=1\ldots N_r$, где N_r — количество последовательностей искаженного образа, присваиваем $r=0$; q — номер анализируемой последовательности шаблона $\mathbf{S}_j$, $q=1\ldots N_{j,q}$, где $N_{j,q}$ — количество последовательностей шаблона $\mathbf{S}_j$, присваиваем $q=1$; $P_{j,r}$ — максимальную вероятность отнесения g-го искаженного образа $\hat{\mathbf{S}}_g$ к шаблонам $\mathbf{S}_j$ по результатам анализа последовательности $\mathbf{A}$ и

всех последовательностей шаблона $\mathbf{S}_j$; $P_{\max}$ — промежуточное значение вероятности $P_{j,r}$, присваиваем $P_{\max}$=0. Выбираем r-ю последовательность элементов искаженного образа ГТО, обозначаем ее **A**, определяем признаки $(d_{g,i},\alpha_{g,i})$ последовательности **A**.

Шаг 5. Выбираем q-ю последовательность из множества последовательностей шаблона $\mathbf{S}_j$, обозначаем ее **B**.

Шаг 6. Сравниваем состав последовательностей **B** и **A**. Если они различаются, то увеличиваем q и переходим на шаг 5, иначе — переходим на шаг 7.

Шаг 7. Определяем для каждого перехода последовательности **A** вероятности $(P_{d,j,r,q,i}, P_{\alpha,j,r,q,i})$ — отнесения его к шаблону $\mathbf{S}_j$ по каждому из признаков $(d_{g,i}, \alpha_{g,i})$ на основе треугольных функций распределения вероятностей (рис. 2). Вероятности $(P_{d,j,r,q,i}, P_{\alpha,j,r,q,i})$ могут быть уточнены путем использования корректирующих экспертных правил $\Lambda_{j,q}$.

Шаг 8. Определяем вероятности $P_{j,r,q}$ отнесения образа $\hat{\mathbf{S}}_g$ к шаблону $\mathbf{S}_j$ по результатам анализа последовательностей **A** и **B**:

$$\begin{aligned} P_{j,r,q} &= \min_i \min_{d,\alpha} \left\{ P_{d,j,r,q,i}, P_{\alpha,j,r,q,i} \right\}, \\ P_{j,r,q,\max} &= \max \left\{ P_{j,r,q}, P_{\max} \right\}, \\ P_{\max} &= P_{j,r,q,\max}, \end{aligned} \tag{9}$$

где $P_{j,r,q,\max}$ — промежуточное значение вероятности $P_{\max}$. Если рассмотрены не все $N_{j,q}$ последовательностей шаблона $\mathbf{S}_j$, то увеличиваем q и переходим на шаг 5, иначе — определяем вероятность отнесения образа $\hat{\mathbf{S}}_g$ к шаблону $\mathbf{S}_j$ по результатам анализа последовательности **A** и всех $N_{j,q}$ последовательностей шаблона:

$$P_{j,r} = P_{\max}. \tag{10}$$

Шаг 9. Если рассмотрены не все N_r последовательностей искаженного образа $\hat{\mathbf{S}}_g$, то увеличиваем r и переходим на шаг 4, иначе — определяем вероятность отнесения искаженного образа $\hat{\mathbf{S}}_g$ к шаблону $\mathbf{S}_j$ по результатам анализа всех N_r последовательностей $\hat{\mathbf{S}}_g$ и $N_{j,q}$ последовательностей шаблона $\mathbf{S}_j$:

$$P_j = \frac{1}{N_r} \sum_{r=1}^{N_r} P_{j,r}. \tag{11}$$

Шаг 10. Если рассмотрены не все N_j шаблонов, то увеличиваем j и выполняем шаги 3–9, иначе — нормируем, при необходимости, полученные вероятности $\{P_j\}$:

$$P_j = \frac{P_j}{\sum_{j=1}^{N_j} P_j}, \forall j, \tag{12}$$

ранжируем множество вероятностей $\{P_j\}$, принимаем решение о наиболее вероятном шаблоне с номером ξ:

$$\mathbf{Y}_g = \xi \left| P_\xi = \max_j \{P_j\}. \right. \tag{13}$$

Шаг 11. Выполняем шаги 2-10 для всех искаженных образов $\hat{\mathbf{S}}_g$ из сформированной выборки примеров. Оцениваем достоверность классификации G в соответствии с (5).

Шаг 12. Если $G \geq G_{зад}$, то заканчиваем выполнение алгоритма. Сформированная база шаблонов таблицы 2-3 с признаками и представленный алгоритм могут быть использованы для автоматической классификации новых искаженных образов. Иначе, если $G < G_{зад}$, осуществляем коррекцию таблиц 2-3.

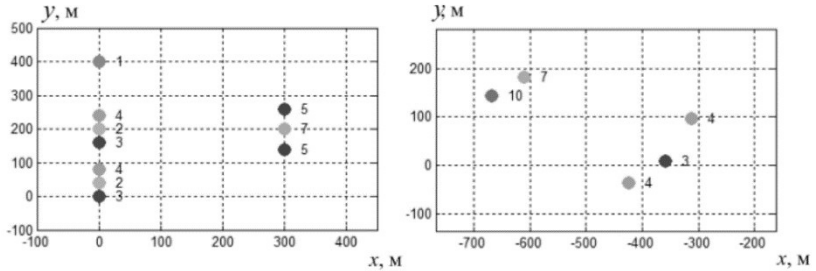
Функцию принадлежности, а следовательно, и закон распределения вероятностей можно аппроксимировать полиномиальной зависимостью и набором коэффициентов. Используя статистические данные, можно получить коэффициенты этих полиномов с помощью метода наименьших квадратов таким образом, чтобы результат классификации был наиболее достоверным [20, 21].

При накоплении вероятностей (11) необходимо учесть различие шаблонов по количеству элементов: если имеется два шаблона ГТО с разным количеством элементов и одинаковой вероятностью отнесения P_j к искаженному образу ГТО, то нужно отдать предпочтение шаблону с меньшим количеством элементов. Реализовать данное логическое условие можно путем умножения значения вероятности отнесения P_j на множитель $(n_j / n_ш)$, где n_j — количество элементов в искаженном образе ГТО, $n_ш$ — количество элементов в анализируемом шаблоне. С другой стороны, данный множитель можно рассматривать как априорную вероятность того, что обнаруженные элементы искаженного ГТО

являются элементами именно *j*-го шаблона. Данное условие является одним из примеров экспертных правил $\Lambda_{j,q}$, используемых в алгоритме.

5. Результаты моделирования. Рассмотренный алгоритм использован для решения задачи классификации искаженных образов наземных ГТО в виде набора элементов различного типа с прямоугольными координатами, полученных по результатам наблюдения в оптическом диапазоне. Элементы ГТО представляли собой объекты 12 типов, причем каждый тип кодировался числом от 1 до 12. Всего имелось 11 шаблонов ГТО, образующих базу шаблонов. Количество элементов в шаблонах ГТО составляло от 2 до 14. Особенностью некоторых шаблонов являлось наличие одинаковых фрагментов из нескольких элементов. Предъявлялись следующие требования к достоверности классификации ГТО: $G \geq G_{зад.}$, $G_{зад.}=0.75$.

На рисунке 5 представлены изображения одного из шаблонов ГТО под номером «6» и соответствующего ему искаженного образа при наличии 40% элементов ГТО, из которых 20 % — ложных, среднеквадратическом отклонении координат элементов ГТО σ=30 м и угле поворота φ=140 град.



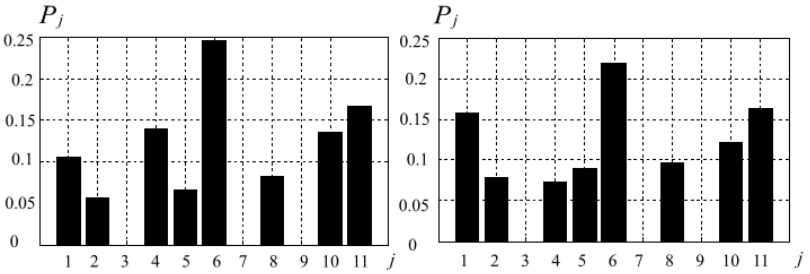
а) б)

Рис. 5. Изображение ГТО: а) шаблона; б) искаженного образа

Анализ рисунка 6 показывает, что увеличение количества признаков ГТО часто позволяет получить более выраженный пик зависимости вероятности P_j от номера шаблона *j*, что, в конечном итоге, положительным образом отражается на повышении достоверности классификации *G* в широком диапазоне варьируемых параметров наблюдения.

В качестве признаков классификации были использованы: а) попарные расстояния между каждыми тремя элементами ГТО и один из углов образованного треугольника; б) попарные расстояния между элементами ГТО. В результате работы рассмотренного алгоритма получен набор вероятностей P_j – отнесения искаженного образа под номером «6» к каждому из 11 шаблонов (рисунок 6).

Данный вывод подтверждают зависимости, представленные на рисунках 7 и 8, полученные по результатам статистических экспериментов на всей базе шаблонов при изменении относительного количества пропущенных v и ложных элементов w в искаженных образах ГТО из базы, а также среднеквадратического отклонения координат элементов σ.



а) б)

Рис. 6. Зависимость вероятности отнесения искаженного образа ГТО под номером «6» к каждому из 11 базовых шаблонов с использованием в качестве признаков: а) попарных расстояний между каждыми тремя элементами ГТО и одного из углов образованного треугольника (таблица 2); б) попарных расстояний между элементами ГТО (таблица 3)

Параметры v и w определяются следующим образом:

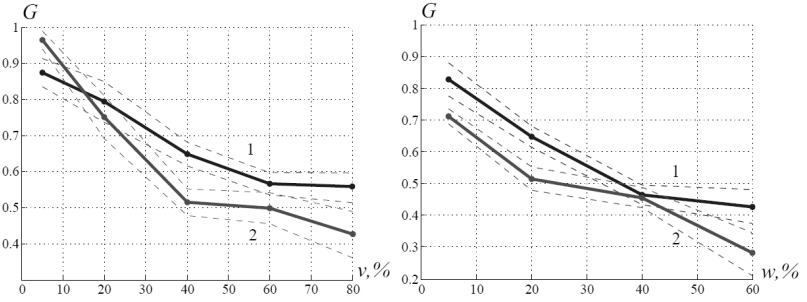
$$v = \frac{n_{\text{ш}} - n_j}{n_{\text{ш}}} \times 100\%,$$

$$w = \frac{n_{\text{л}}}{n_j} \times 100\%,$$

где n_j — количество элементов в искаженном образе ГТО, $n_{\text{л}}$ — количество ложных элементов в искаженном образе ГТО, $n_{\text{ш}}$ — количество элементов в шаблоне ГТО, из которого синтезирован искаженный образ. Для указанных зависимостей определен доверительный интервал на значение достоверности G с доверительной вероятностью 0.99 по результатам 1000 экспериментов (отмечен на рисунках пунктиром).

Как показывают результаты, достоверность классификации значимо ухудшается, если в искаженном образе ГТО одновременно имеются пропущенные и ложные элементы, а также существует значимый разброс их координат. Тем не менее заданное значение достоверности

классификации $G_{зад.}$=0.75 было достигнуто в «плохих» ситуациях и достаточно широком диапазоне варьируемых параметров v и w.



а) б)

Рис. 7. Зависимости достоверности классификации ГТО на всей базе шаблонов G: а) от относительного количества пропущенных элементов в искаженных образах ГТО v при заданном среднеквадратическом отклонении σ = 30м и относительном количестве ложных элементов w = 20%; б) от относительного количества ложных элементов w в искаженных образах ГТО при заданном σ = 30м и v = 40% и использовании в качестве признаков попарных расстояний между каждыми тремя элементами и одного из углов образованных треугольников (кривая 1) и попарных расстояний между элементами ГТО (кривая 2)

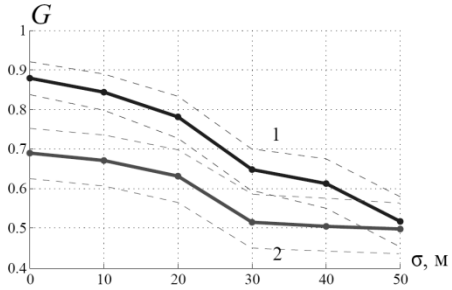


Рис. 8. Зависимость достоверности классификации ГТО на всей базе шаблонов G от среднеквадратического отклонения координат элементов σ при заданном относительном количестве пропущенных v =40% и ложных w = 20% элементов с доверительными интервалами при использовании в качестве признаков попарных расстояний между каждыми тремя элементами и одного из углов образованных треугольников (кривая 1) и попарных расстояний между элементами ГТО (кривая 2)

При решении рассмотренной задачи применение в качестве признаков попарных расстояний между каждыми тремя элементами и одного из углов образованных треугольников позволяет получить лучший результат, чем при использовании только попарных расстоя-

ний. Второй подход может быть использован в тех случаях, когда в искаженном образе ГТО имеется в наличии лишь два элемента, а также в «хороших» ситуациях, характеризующихся малым количеством пропущенных и ложных элементов ГТО, а также малым значением среднеквадратического отклонения координат его элементов. Представленные результаты получены при значениях σ, v и w, которые характерны для «плохих» ситуаций, что подтверждает возможность использования разработанного алгоритма и выбранных признаков классификации сложных ГТО в различных реальных применениях.

6. Заключение. Достоинством представленного алгоритма является возможность удобного включения в процедуру поиска не только дополнительных признаков, позволяющих уточнить класс ГТО, но и различных логических или эвристических правил, а также аналитических выражений, описывающих данную предметную область и позволяющих скорректировать нужным образом оценку значений признаков ГТО и повысить достоверность решения задачи классификации (1). Кроме того, имеется возможность встраивания в алгоритм адаптивных процедур, позволяющих уточнить результат классификации на множестве получаемых статистических данных. Основными направлениями совершенствования данного алгоритма являются: поиск эффективных признаков классификации ГТО; оценка влияния длины анализируемых последовательностей ГТО на достоверность классификации; оптимизация параметров используемых функций принадлежности; исследование различных способов получения оценок P_j и принятия решения о наиболее вероятном шаблоне.

Литература

1. *Фурман Я.А., Роженцов А.А., Евдокимов А.О.* Распознавание групповых точечных объектов с неупорядоченными отметками // Автометрия. 2005. Т. 41. №1. С. 19–28.
2. *Фурман Я.А., Егошина И.Л., Ерусланов Р.В.* Согласованная фильтрация зашумленных дискретных кватернионных сигналов // Журнал радиоэлектроники. 2012. № 3. С. 1–35.
3. *Роженцов А.А., Евдокимов А.О., Григорьев А.В.* Распознавание плоских изображений групповых точечных объектов при наличии ошибок обнаружения // Изв. высш. учебн. заведений: Приборостроение. 2006. Т. 49. № 4. С. 59–64.
4. *Мальцев Г.Н., Назаров А.В., Якимов В.Л.* Алгоритм реконструкции фазового пространства и его применение для создания прогнозных моделей // Информационно-управляющие системы. 2014. № 2. С. 33–39.
5. *Неронский Л.Б. и др.* Формирование точечных моделей объектов по комплексным РСА - изображениям // Современные проблемы дистанционного зондирования Земли из космоса. 2010. Т. 7. № 4. С. 158–164.
6. *Sharp R.* Jane's Fighting Ships, 1999-2000 // Jane's Information Group. 1990. 800 p.
7. *Дзенчарский Н.Л., Медведев М.В., Шлеймович М.П.* Поиск изображений с выделением особых точек на основе вейвлет-преобразования // Вестник Казанского государственного технологического университета. 2011. № 1. С. 131–135.
8. *Ипатов Ю.А., Кревецкий А.В.* Методы обнаружения и пространственной локализации групп точечных объектов // Кибернетика и программирование. 2014. № 6. С.17–25.
9. *Szeliski R.* Computer Vision: Algorithms and Applications // Springer. 2011. 812 p.

10. *Фурман Я.А.* Точечные поля и групповые объекты // М.: Физматлит. 2015. 440 с.
11. *Furman Y.A., Eruslanov R.V., Egoshina I.L.* Iterative Algorithm for angular matching of group point objects with apriori uncertainty of parameters // Pattern recognition and image analysis. 2013. vol. 23. no. 3. pp. 381–388.
12. *Воробьев С.Н., Лазарев И.В.* Алгоритм распознавания конфигураций звезд // Информационно-управляющие системы. 2008. №2. С. 2–8.
13. *Дубровкина М.В.* Векторно-нормализованный метод распознавания групповых точечных объектов произвольной формы // Вестник Сумского государственного университета. 2009. № 4. С. 32–38.
14. *Варшавский П.Р., Еремеев А.П.* Моделирование рассуждений на основе прецедентов в интеллектуальных системах поддержки принятия решений // Искусственный интеллект и принятие решений. 2009. №1. С. 45–57.
15. *Уздин Д.З.* О новом подходе в теории распознавания образов (состояний). Новые методы математической диагностики // М.: МАКС Пресс. 2012. 232 с.
16. *Осипов Г.С.* Методы искусственного интеллекта // М.: Физматлит. 2011. 296 с.
17. *Kandel A., Byatt W.* Fuzzy sets, fuzzy algebra, and fuzzy statistics // Proceedings of the IEEE. 1978. vol. 66. no. 12. pp. 1619–1639.
18. *Зак Ю.А.* Принятие решений в условиях нечетких и размытых данных: Fuzzy-технологии // М.: Книжный дом «Либроком». 2013. 352 с.
19. *Смагин В.А., Парамонов И.Ю.* Вероятностный критерий оценивания нечеткой энтропии // Информация и космос. 2015. №2. С. 42–46.
20. *Бураков М.В., Брунов М.С.* Структурная идентификация нечеткой модели // Труды СПИИРАН. 2014. Вып. 3. С. 232–246.
21. *Ходашинский И. А.* Построение компактных и точных нечетких моделей на основе статистических информационных критериев // Информатика и системы управления. 2014. № 1(39). С. 99–107.

Каплин Александр Юрьевич — к-т техн. наук, заместитель генерального директора-генеральный конструктор, ОАО «Радиоавионика». Область научных интересов: системы управления и связи специального назначения, человеко-машинные систе-мы, бортовая радиолокация и радионавигация. Число научных публикаций — 50. a.kaplin@list.ru; Троицкий пр., д. 4 лит. Б, Санкт-Петербург, 190103; р.т.: +7(812) 251-3875, Факс: +7(812)251-2743.

Коротин Андрей Анатольевич — к-т техн. наук, директор научно-исследовательского центра, ОАО «Радиоавионика». Область научных интересов: системы управления и связи специального назначения, человеко-машинные системы, аппаратно-программные комплексы, защита космических аппаратов от радиации. Число научных публикаций — 30. kaa2805@mail.ru; Троицкий пр., д. 4 лит. Б, Санкт-Петербург, 190103; р.т.: +79119107595, Факс: +7(812) 251-2743.

Назаров Андрей Вячеславович — д-р техн. наук, доцент, начальник кафедры космической радиолокации и радионавигации, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: распознавание образов, нейросетевые технологии, моделирование распределенных систем, обработка сигналов в оптико-электронных информационных системах. Число научных публикаций — 100. naz-av@mail.ru; ул. Ждановская, 13, Санкт-Петербург, 197198; р.т.: +7(812)347-95-33.

Якимов Виктор Леонидович — к-т техн. наук, доцент, заместитель начальника кафедры приемных устройств и радиоавтоматики, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: моделирование сложных систем, нейросетевые технологии, техническая диагностика. Число научных публикаций — 40. yakim78@yandex.ru; ул. Ждановская, 13, Санкт-Петербург, 197198; р.т.: +7(812)347-95-36.

A.Y. KAPLIN, A.A. KOROTIN, A.V. NAZAROV, V.L. YAKIMOV

CLASSIFICATION ALGORITHM OF GROUP POINT OBJECTS WITH UNORDERED ELEMENTS BASED ON CLOSENESS PROBABILITY MEASURE

Kaplin A.Y., Korotin A.A., Nazarov A.V., Yakimov V.L. **Classification Algorithm of Group Point Objects with Unordered Elements based on Closeness Probability Measure.**

Abstract. The paper presents a classification algorithm of group point objects (GPO) based on the comparative analysis of fragments of distorted images and the GPO templates. The sequences of the GPO elements of different lengths are used as fragments. The paired and angular interdot distances are used as classification signs. The probability measure of closeness, set by the expert by means of the membership function and the distribution law of probability of discrete values of classified objects signs, is used in solving a classification task.

The algorithm includes the following stages: search and comparison of fragments composition of distorted images and the GPO templates; formation of a probable assessment of closeness of GPO distorted image and each template in space of the considered signs according to the analysis of each fragment; accumulation of the received probabilities on the basis of analysis results of all distorted image fragments; ranging of the received probabilities of classifying the distorted image as the GPO template; determination of the most probable template. The algorithm provides the possibility of specifying a GPO distorted image class using logical rules and analytical expressions of the considered data domain. The example and results of the algorithm application for solving a classification task of real GPO on the basis of the analysis of their fragments in the form of sequences from two and three elements are given.

Keywords: group point object, classification, probability measure of closeness.

Kaplin Alexander Yurievich — Ph.D., deputy director-general, general designer, Joint Stock Venture «Radioavionika». Research interests: control and communication systems of a special purpose, human - machine systems, on-board radar and navigation. The number of publications — 50. a.kaplin@list.ru; P.O.B. 111, St. Petersburg, 190103; office phone: +7(812) 251-3875, Fax: +7(812) 251-2743.

Korotin Andrey Anatolievich — Ph.D., director of research center, Joint Stock Venture «Radioavionika». Research interests: control and communication systems of a special purpose, human-machine systems, hardware-software complexes, protection of spacecraft from the radiation. The number of publications — 30. kaa2805@mail.ru; P.O.B. 111, St. Petersburg, 190103; office phone: +79119107595, Fax: +7(812) 251-2743.

Nazarov Andrey Vyacheslavovich — Ph.D., Dr. Sci., associate professor, head of space radiolocation and a radio navigation department, Mozhaisky Military Space Academy. Research interests: pattern recognition, neural nets, modeling of distributed systems, signal processing in optical-electronic information systems. The number of publications — 100. nazav@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812)347-95-33.

Yakimov Victor Leonidovich — Ph.D., associate professor, deputy head of receiving devices and radio automatic equipment department, Mozhaisky Military Space Academy. Research interests: simulation of difficult systems, neural network technologies, technical diagnostics. The number of publications — 40. yakim78@yandex.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812)347-95-36.

References

1. Furman Ja.A., Rozhencov A.A., Evdokimov A.O. [Recognition of group point objects with ordered marks]. *Avtometrija – Avtometriya.* 2005. vol. 41. no. 1. pp. 19–28. (In Russ.).

2. Furman Ja.A., Egoshina I.L., Eruslanov R.V. [Matched filtering of noisy discrete quaternion signals]. *Zhurnal radiojelektroniki – Magazine of radio electronics*. 2012. no. 3. pp. 1–35. (In Russ.).
3. Rozhencov A.A., Evdokimov A.O., Grigor'ev A.V. [Recognition of flat images of group point objects in the presence of error detection]. *Izv. vyssh. uchebn. zavedenij: Priborostroenie – Proceedings of the higher educational institutions: Instrumentation*. 2006. vol. 49. no. 4. pp. 59–64. (In Russ.).
4. Maltsev G.N., Nazarov A.V., Yakimov V.L. [A reconstruction algorithm for a dynamic system phase space and its application for development of predictive models]. *Informacionno-upravljajushhie sistemy – Information and control systems.* 2014. vol. 2(69). pp. 33–39 (In Russ.).
5. Neronskiy L.B. et al. [Generation of object point models by SAR complex images]. *Sovremennye problemy distantsionnogo zondirovaniia Zemli iz kosmosa – Actual problems of remote sensing of the Earth from space.* 2010. vol. 7. no. 4. pp. 158–164. (In Russ.).
6. Sharp R. Jane's Fighting Ships, 1999-2000. Jane's Information Group. 1990. 800 p.
7. Dzencharskii N.L., Medvedev M.V., Shleimovich M.P. [Image search with the release of specific points on the basis of wavelet transform]. *Vestnik Kazanskogo gosudarstvennogo tekhnologicheskogo universiteta – Vestnik of the Kazan state technological university*. 2011. vol. 1. pp. 131–135. (In Russ.).
8. Ipatov Iu.A., Krevetskii A.V. [Methods of detection and spatial localization of groups of point objects]. *Kibernetika i programmirovanie – Cybernetics and programming*. 2014. vol. 6. pp. 17–25. (In Russ.).
9. Szeliski R. Computer Vision: Algorithms and Applications. Springer. 2011. 812 p.
10. Furman Ja.A. *Tochechnye polia i gruppovye ob"ekty* [Point field and group objects]. Moscow: Fizmatlit Publ. 2015. 440 p. (In Russ.).
11. Furman Y.A., Eruslanov R.V., Egoshina I.L. [Iterative algorithm for angular matching of group point objects with apriori uncertainty of parameters]. *Pattern recognition and image analysis*. 2013. vol. 23. vol. 3. pp. 381–388.
12. Vorob'ev S.N., Lazarev I.V. [Configurations recognition algorithm stars]. *Informacionno-upravljajushhie sistemy –Information and control systems*. 2008. vol. 2. pp. 2–8. (In Russ.).
13. Dubrovkina M.V. [Vector-normalized method for detection of group point objects of arbitrary shape]. *Vestnik Sumskogo gosudarstvennogo universiteta – Bulletin of the Sumy state university.* 2009. vol. 4. pp. 32–38. (In Russ.).
14. Varshavskij P.R., Eremeev A.P. [Modelling of reasoning based on precedents in intelligent decision support systems]. *Iskusstvennyj intellekt i prinjatie reshenij – Artificial intelligence and decision-making*. 2009. no. 1. pp. 45–57 (In Russ.).
15. Uzdin D.Z. *O novom podkhode v teorii raspoznavaniia obrazov (sostoianii). Novye metody matematicheskoi diagnostiki* [A New Approach to the Theory of Pattern Recognition (States). New Methods of Mathematical Diagnostics]. Moscow: MAKS Press Publ. 2012. 232 p. (In Russ.).
16. Osipov G.S. *Metody iskusstvennogo intellekta* [Methods of artificial intelligence]. Moscow: Fizmatlit Publ. 2011. 296 p. (In Russ.).
17. Kandel A., Byatt W. Fuzzy sets, fuzzy algebra, and fuzzy statistics. Proceedings of the IEEE. 1978. vol. 66. no. 12. pp. 1619–1639.
18. Zak Ju.A. *Prinjatie reshenij v uslovijah nechetkih i razmytyh dannyh: Fuzzy-tehnologii* [Decision-making in a fuzzy and blurry data: Fuzzy-technology]. Moscow: Knizhnyj dom «Librokom» Publ. 2013. 352 p. (In Russ.).
19. Smagin V.A., Paramonov I.Ju. [Probabilistic estimation of fuzzy entropy criterion] // *Informacija i kosmos – Information and Space*. 2015. no. 2. p. 42–46. (In Russ.).
20. Burakov M.V., Brunov M.S. [Structure identification of fuzzy model]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2014. vol. 3. pp. 232–246. (In Russ.).
21. Khodashinskii I. A. [Building compact and powerful fuzzy models based on statistical information criteria]. *Informatika i sistemy upravleniia – Information and control systems*. 2014. vol. 1(39). pp. 99–107. (In Russ.).

РУКОВОДСТВО ДЛЯ АВТОРОВ

Взаимодействие автора с редакцией осуществляется через личный кабинет на сайте журнала «Труды СПИИРАН» http://www.proceedings.spiiras.nw.ru. При регистрации авторам рекомендуется заполнить все предложенные поля данных.

Подготовка статьи ведется с помощью текстовых редакторов MS Word 2007 и выше. Объем основного текста – от 15 до 25 страниц включительно. Формат страницы документа – A5 (148 мм ширина, 210 мм высота); ориентация – портретная; все поля – 20 мм. Верхний и нижний колонтитулы страницы – пустые. Основной шрифт документа – Times New Roman, основной кегль (размер) шрифта – 10 pt. Переносы разрешены. Абзацный отступ устанавливается размером в 10 мм. Межстрочный интервал – одинарный. Номера страниц не проставляются.

В основную часть допускается помещать рисунки, таблицы, листинги и формулы. Правила их оформления подробно рассмотрены на нашем сайте в разделе «Руководство для авторов».

AUTHOR GUIDELINES

Interaction between each potential author and the Editorial board is realized through the personal account on the website of the journal "Proceedings of SPIIRAS" http://www.proceedings.spiiras.nw.ru. At the registration the authors are requested to fill out all data fields in the proposed form.

The submissions should be prepared using MS Word 2007 text editor or higher versions, at that, only manuscripts in *.docx format will be considered. The text of the paper in the main part of it should be from 15 – 25 pages of A5 size that is 210 X 148 mm; orientation – portrait; all margins – 20 mm. The font of the main paper text is Times New Roman of 10 pt font size. The pages' headers and footers should be empty; indention – 10 mm; line spacing – single; pages are not numbered; hyphenations are allowed.

Certain figures, tables, listings and formulas are allowed in the main section, and their typography is considered by the paper template in more detail in journal web.

ISSN 2078-9181

Вып. 5(48)

ТРУДЫ СПИИРАН
proceedings.spiiras.nw.ru

С-Пб
2016