ISSN 1818-0442
DOI: 10.21293/1818-0442

ДОКЛАДЫ

Томского государственного университета систем управления и радиоэлектроники

2021 • Том 24, № 4

Министерство науки и высшего образования Российской Федерации

ДОКЛАДЫ ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

2021, том 24, № 4

Периодический научный журнал

Выходит 4 раза в год **ISSN 1818-0442**

Основан в 1997 г. **DOI: 10.21293/1818-0442**

Адрес редакции: 634050, г. Томск, пр. Ленина, 40, ТУСУР, тел. (382-2) 51-21-21

Свидетельство о регистрации МНС РФ № 1027000867068 от 13 октября 2004 г.

Подписной индекс 20648 в каталоге агентства «Роспечать»: газеты и журналы.

Издательство Томского государственного университета систем управления и радиоэлектроники

634050, Томск, пр. Ленина, 40, тел. (382-2) 51-21-21.

Верстка, техническое редактирование, подготовка оригинал-макета В.М. Бочкаревой.

Корректор В.Г. Лихачева.

Подписано в печать 25.12.2021. Формат 60×84 1/8. Печ. л. 5,25. Тираж 500. Заказ 26.

Editorial board

Содержание

ЭЛЕКТРОНИКА, РАДИОТЕХНИКА И СВЯЗЬ

УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

Contents

ELECTRONICS, RADIO ENGINEERING AND COMMUNICATIONS

CONTROL, COMPUTER SCIENCE AND INFORMATICS

ЭЛЕКТРОНИКА,
РАДИОТЕХНИКА И СВЯЗЬ

УДК 004.891

А.А. Квасников, С.П. Куксенко

Обзор экспертных систем по электромагнитной совместимости технических средств

Выполнен обзор экспертных систем по электромагнитной совместимости. Кратко изложены история развития и классификация современных экспертных систем. Указаны основные элементы и особенности построения программной архитектуры, а также примеры экспертных систем по электромагнитной совместимости технических средств различного назначения.

Ключевые слова: электромагнитная совместимость, экспертная система, техническое средство, радиоэлектронное средство, печатная плата, линия передачи.
DOI: 10.21293/1818-0442-2021-24-4-7-18

Различные радиоэлектронные средства (РЭС), в частности, и технические средства (ТС) в целом всё шире используются во всех сферах деятельности современного общества. При этом увеличение количества этих средств часто приводит к нарушению их совместной работы из-за возникновения взаимных электромагнитных помех (ЭМП). Поэтому обеспечение их электромагнитной совместимости (ЭМС) является актуальной проблемой.

Согласно ГОСТ Р 50397–2011, ЭМС технического средства – это его способность функционировать с заданным качеством в заданной электромагнитной обстановке и не создавать недопустимых ЭМП другим ТС. При этом под техническим средством подразумевается электротехническое, электронное и радиоэлектронное изделие, а также любое изделие, содержащее электрические и/или электронные составные части (оно может быть устройством, оборудованием, системой или установкой). Для решения проблемы обеспечения ЭМС ТС, связанной с дорогостоящими и длительными испытаниями, целесообразно на этапе проектирования использовать специализированное программное обеспечение (ПО). При этом решение задач ЭМС требует от проектировщика глубоких экспертных знаний. Поэтому разработка данного класса ПО ведется в направлении расширения его функциональных возможностей и внедрения элементов экспертных систем (ЭС), что позволяет разработчикам более эффективно и рационально использовать их ресурсы на этапе проектирования. Однако в научной литературе отсутствует актуальный обзор по особенностям разработки ЭС по ЭМС. Поэтому цель данной работы – выполнить обзор современного состояния исследований по разработке ЭС по ЭМС и выявить тенденции их развития на основании имеющихся открытых научных источников. При этом следует отметить, что авторы данной работы не претендуют на полноту выполненного обзора, поскольку рассматриваемая тематика весьма обширна, а ознакомительные версии ЭС в открытом доступе отсутствуют, что значительно осложняет выявление и обобщение особенностей заложенного в них математического и программного обеспечения.

История развития ЭС

История развития ЭС берет свое начало с середины XX в., что напрямую связано со стремительным развитием компьютерных технологий. Предпосылкой к созданию классических ЭС являлись попытки разработки интеллектуальных систем (ИС), автоматизирующих умственную деятельность человека. Первые ИС представляли собой программы, способные решать задачи с помощью эвристических методов и принципа обобщения, свойственного человеческому мышлению. В дальнейшем стало очевидно, что эффективность ИС зависит не только от заложенных в нее алгоритмов и методов, но и от знаний, которые она содержит. Также поскольку разработка универсальных ИС для решения широкого класса задач являлась трудозатратной, то была разработана общая концепция построения ИС. Такие ИС были названы ЭС. Целью разработки ранних ЭС было создание компьютерных систем, позволяющих решать задачи, выполнение которых требует наличия глубоких экспертных знаний в конкретной области. Так, были созданы ЭС, применимые в областях медицины, математики, образования, промышленности, химии, электроэнергетики и др. [1–6].

Архитектура ЭС

Современные ЭС условно делятся на классические, нейронные, нечеткие, нейро-нечеткие, веб-экспертные, мультиагентные, реального времени и принятия многокритериальных решений [7]. Программная архитектура классической ЭС, основанной на проверке правил проектирования, схематично представлена на рис. 1. Она состоит из: пользовательского интерфейса (инструмент взаимодействия пользователя с системой); модуля объяснения логических выводов (пояснения, как ЭС пришла к конкретному выводу); базы знаний (экспертные знания в конкретной предметной области); рабочей памяти (базы данных объектов и фактов, используемых системой для решения конкретных задач); механизма логического вывода (выводы на основе проверки правил проектирования и их приоритетов из базы знаний); модуля пополнения знаний (механизм пользовательского ввода новых данных в систему). При этом основными частями ЭС являются база

знаний и механизм логического вывода. Процесс наполнения базы знаний часто сопровождается затруднениями, связанными с преобразованием экспертных знаний в четкий набор логических правил [8]. Поэтому созданы специальные алгоритмы [9], а также подходы, основанные на применении нейронных сетей и методов поиска ассоциативных правил. Преимущество последних заключается в том, что базовый алгоритм обучения может автоматически генерировать базу знаний для ЭС [10, 11].

Классические ЭС являются наиболее применимыми на практике. Тем не менее разработке ЭС, имеющих отличные от них программные архитектуры, посвящены усилия многих исследователей. Так, известен пример разработки веб-экспертной системы для сбора уплаты за регистрацию транспортных средств [12]. ЭС реализована с использованием возможностей системы управления бизнес-правилами Blaze Advisor и развернута на сервере приложений Java. Также предложен метод динамического планирования для ЭС реального времени, пригодный для управления или мониторинга сложными промышленными процессами, использование которого обеспечивает высокоэффективное применение ресурсов [13]. В работе [14] приведены особенности разработки нейро-нечеткой ЭС, в которой используется база знаний, сгенерированная с помощью правил машинного обучения, а не содержащая статические правила. Подобная реализация механизма наполнения базы знаний ЭС делает возможным получение контекстно-зависимого персонализированного набора правил, который может быть использован, например, для повышения эффективности работы мобильных приложений, предоставляющих персонализированные услуги пользователям. В работе [15] представлен обзор алгоритмов машинного обучения и возможных сфер их применения при разработке ЭС различного назначения.

Важным этапом создания ЭС является разработка требований к их функционалу. Так, выполнен анализ атрибутов ЭС, процесса разработки требований ЭС и возможных методов, которые могут быть использованы при создании ЭС [16, 17]. В качестве основных критериев оценки эффективности ЭС выступают интеллектуальность (способность ЭС решать задачи аналогично человеку-эксперту), экономичность (генерация решений за минимальное время) и удобство в её использовании. Процесс разработки требований делится на пять этапов: выявление требований; моделирование (создание абстрактного описания системы с использованием ER- и/или UML-диаграмм); анализ требований (формирование списка функций, вида представления данных и интерфейса системы, выявление ошибок, связанных с возможной неполнотой, непоследовательностью или неконкретностью требований); валидация и верификация (проверка того, что заложенные ЭС правильны и адекватны); управление требованиями (обеспечение постоянного соответствия результатов работы ЭС её требованиям и документирование требований).

Особенности современных ЭС по ЭМС ТС

Как известно, проблема обеспечения ЭМС ТС связана с генерацией, передачей и приёмом электромагнитной энергии [18]. Так, эмиттер (источник) генерирует ЭМП, которые через кондуктивную, гальваническую или электромагнитную связь поступают на рецептор (приёмник).

На практике принято выделять три уровня ЭМС: внутриаппаратная, внутрисистемная и межсистемная. Первая определена на уровне блока, узла и пр., вторая – системы или комплекса, а третья – между системами и комплексами. Эта специфика обусловливает особенности разработки используемого программного и математического обеспечения и требуемого объема входных данных. Так, при решении задач внутриаппаратной и внутрисистемной ЭМС используются проекционные и конечно-разностные численные методы, а при межсистемной – асимптотические. При этом альтернативные аналитические методы разработаны только для первых двух [19, 20].

Преимуществом их использования являются быстродействие и простота в использовании, а недостатком – ограниченный круг задач, который может быть решен (отсутствие универсальности). Также их использование подразумевает, что разработчик должен самостоятельно оценить возможность применения этих методов для решения поставленной задачи. Использование численных методов позволяет рассчитывать поля и токи в конфигурациях, геометрия которых достаточно сильно приближена к реальным устройствам. Однако эффективность их использования напрямую зависит от вычислительной мощности используемой рабочей станции.

Помимо различий в архитектурах, ЭС различаются организацией баз знаний. В работе [21] рассмотрены различные схемы представления знаний, а также предложен подход к формированию блоков данных (фреймов) для базы знаний по ЭМС. Фрейм является структурой организации знаний, состоящей из ряда слотов. Каждый слот идентифицируется отдельным именем и соответствует определенному свойству объекта, представленного фреймом.

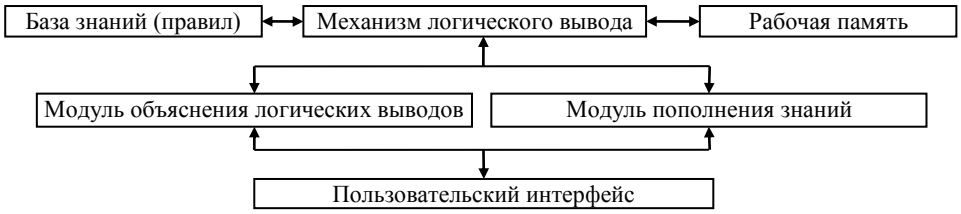

Рис. 1. Программная архитектура классической ЭС [7]

Такое представление базы знаний позволяет описывать как поведение компонентов, так и их взаимосвязи. Преимуществами подхода являются отсутствие ограничений на число слотов в фрейме, возможность использования сложных структур данных, простота в описании и возможность обработки и представления неполных знаний.

Несмотря на имеющиеся различия в реализации современных ЭС, в целом функционально они схожи. Так, из-за необходимости большого числа вычислений, особенно при использовании численных методов, их рекомендуется интегрировать в системы или среды автоматизированного проектирования. Тогда ЭС являются, по сути, программными надстройками к этим системам и средам проектирования, существенно расширяющими их функционал.

Для наглядности изложения далее приведены краткие обзоры функциональных возможностей и примеры реализации известных ЭС по ЭМС ТС.

ЭС по внутриаппаратной ЭМС ТС

В работах [22, 23] предложен подход к организации ЭС по ЭМС печатных плат (ПП), основанный на применении аналитических и численных методов с последующей проверкой правил проектирования. Так, процесс работы ЭС состоит из четырех этапов: ввод данных, анализ, оценка и вывод результатов (рис. 2). Каждому этапу соответствуют отдельные модули, выполняющие определенные задачи. На этапе ввода происходит сбор и классификация информации об анализируемой ПП, а также загрузка файла, содержащего конкретные требования по ЭМС в соответствии с наработками компании производителя или отрасли в целом. После завершения работы этапа ввода данные из считанных файлов используются для классификации цепей за счет анализа свойств, распространяемых по ним сигналов и их назначения.

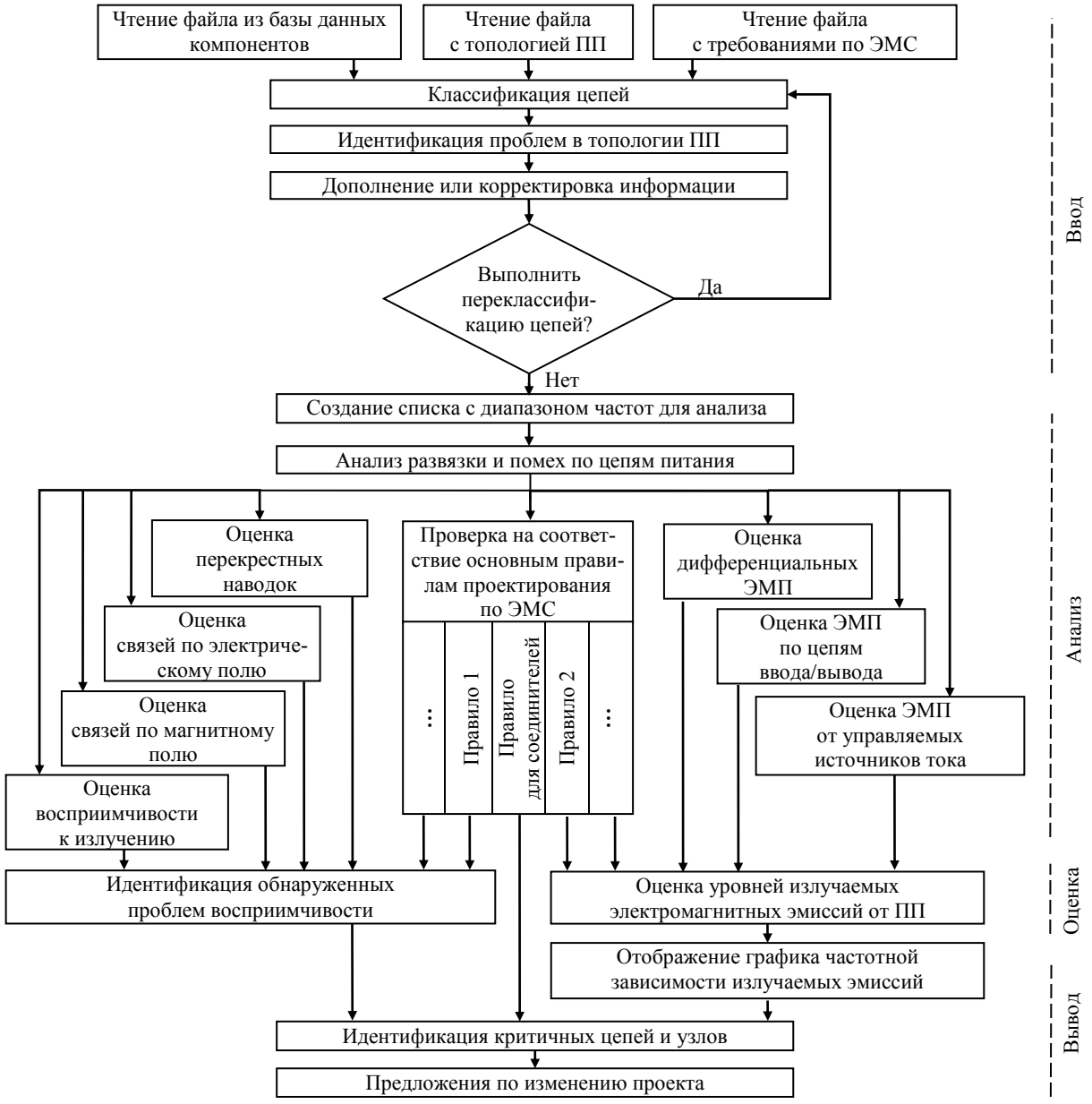

Рис. 2. Структура ЭС по ЭМС ПП [23]

Далее происходит поиск возможных проблем компоновки и трассировки, например, связанных с подключением цепей к нескольким источникам питания или, наоборот, отсутствием электрического контакта, и предупреждение пользователя об этом. Затем пользователь может внести правки, добавить недостающую информацию и перезапустить алгоритм классификации цепей. На этапе анализа выполняется подробный анализ ПП на предмет наличия потенциальных проблем, связанных с её излучением и восприимчивостью, а также выполнить проверку на соответствие основным рекомендациям по проектированию. Для этого предварительно формируется список тактовых частот, используемых в схеме, их гармоник, а также всех частот узкополосных аналоговых сигналов, на которых затем производятся вычисления. Далее на основе полученных результатов формируется общая оценка излучаемых электромагнитных эмиссий от ПП. На этапе вывода пользователю доступен график частотной зависимости излучаемых эмиссий, а также список узлов и компонентов ПП, вносящих наиболее существенный вклад в эти эмиссии. Помимо этого, предлагаются варианты конструктивных решений, направленные на снижение уровня эмиссий и повышение помехоустойчивости ПП.

Известна ЭС EMC Expert, которая ориентирована на выявление проблем ЭМС ПП (рис. 3) [24]. Система состоит из 5 основных компонентов: генераторов промежуточного формата и базы данных, пользовательского интерфейса, базы знаний и анализатора ЭМС. Генератор промежуточного формата предназначен для преобразования файлов анализируемой ПП, созданных с помощью системы автоматизированного проектирования (САПР), в форму, пригодную для дальнейшей генерации базы данных, реализованной в соответствии с принципами объектно-ориентированного программирования и содержащей список элементов ПП и их параметров. База знаний содержит правила и рекомендации по проектированию ПП. Используя эти базы, система находит имеющиеся недостатки в реализации ПП и отображает их, подсвечивая соответствующие области в графическом интерфейсе пользователя.

В работе [25] обсуждается совместное применение ЭС и электродинамических САПР, а также представлены перспективы развития ЭС в области ЭМС. Также представлен краткий обзор программных средств и подходов к обеспечению ЭМС и предложена обобщенная структура ЭС по ЭМС ПП, функциональные модули которой обеспечивают выполнение 4 этапов работы системы: ввод, классификация, оценка (проверка правил проектирования и оценка ЭМС), формирование отчета. Структурная схема ЭС приведена на рис. 4.

Известен алгоритм автоматического размещения компонентов на ПП, ориентированный на уменьшение уровня ЭМП [26]. Вначале компоненты автоматически делятся на группы по списку межсоединений, затем эти группы помещаются на схему, используя специальный алгоритм. После этого на схему помещаются межсоединения с ограничениями по их длине. Также разработаны алгоритмы для быстрой оценки электромагнитного излучения от ПП, которые позволяют ЭС работать с ограниченным количеством информации о корпусе, кабелях или точном характере сигналов, оценивать различные структуры ПП посредством поиска потенциально сильных источников электромагнитного излучения [27]. Кроме того, предложены алгоритмы, разработанные для ЭС по ЭМС, для оценки конструкций ПП [28]. Так, максимальные значения излучаемых эмиссий, оцененные алгоритмами, сравниваются с измеренными данными различных конфигураций ПП. Алгоритмы определяют наиболее важные механизмы формирования ЭМП, используя информацию о конструктивных особенностях ПП, которые оказывают наиболее существенное влияние на излучаемые эмиссии.

Рис. 3. Структурная схема ЭС EMC Expert [24]

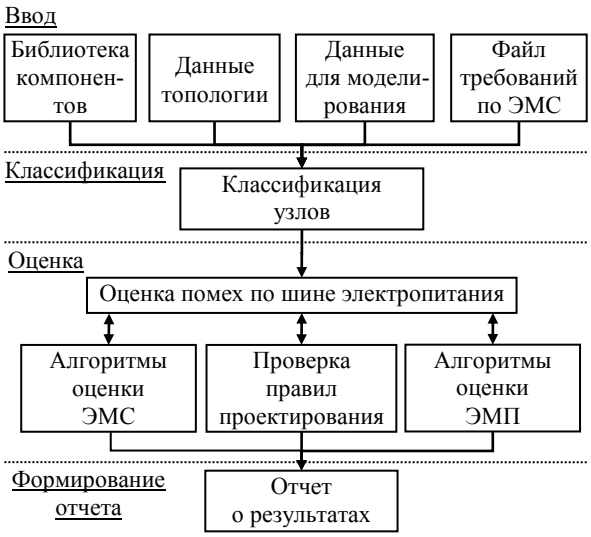

Рис. 4. Структурная схема ЭС по ЭМС ПП [25]

Для удаленных испытаний ТС на ЭМС предложена система, содержащая инструменты сетевого взаимодействия для передачи и управления данными в режиме реального времени (рис. 5) [29]. Она предоставляет эксперту результаты испытаний удаленных ТС, что существенно экономит финансовые и временные ресурсы.

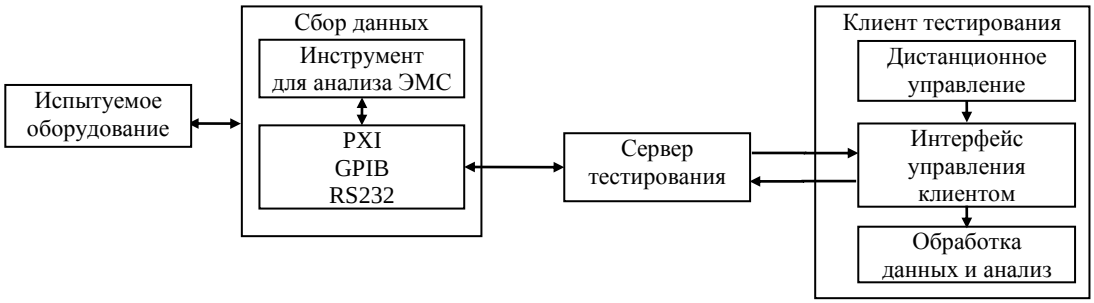

Рис. 5. Структура системы для удаленного тестирования ТС на ЭМС [29]

При разработке баз знаний, содержащих рекомендации по проектированию ПП, кабелей и экранирующих корпусов с учетом ЭМС, широко используются различные лабораторные макеты [30].

В работе [31] представлена ЭС, предназначенная для анализа, синтеза и исследований микрополосковых полосно-пропускающих фильтров. Система содержит базу готовых конструкций фильтров и оригинальный алгоритм оптимизации.

В работе [32] предложена модульная архитектура прототипа ЭС по ЭМС линий передачи (ЛП). Связанные ЛП и устройства на их основе являются основными элементами РЭС, при автоматизированном проектировании которых часто используется квазистатический подход. Стандартная процедура проектирования состоит из пяти этапов: задание входных данных, анализ, оптимизация, прогнозирование и вывод результатов (рис. 6).

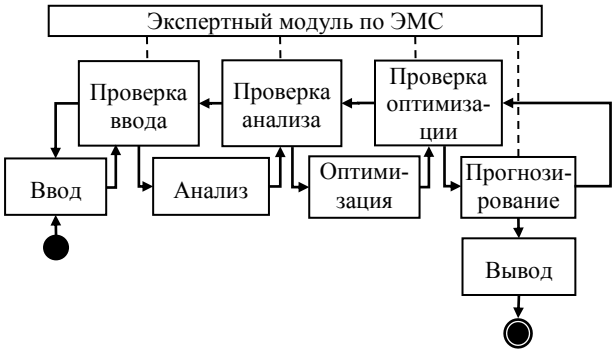

Рис. 6. Диаграмма рабочего процесса ЭС по ЭМС ЛП [32]

Для прямой автоматизации процесса проектирования система содержит экспертный модуль по ЭМС, основанный на базе знаний, содержащей правила проектирования, и позволяющий анализировать результаты каждого этапа и управлять общим процессом работы системы. Если модуль обнаруживает нарушения правил, то в зависимости от выбранного режима работы ЭС либо автоматически возвращается к предыдущим этапам для получения приемлемых результатов, либо сообщает пользователю об ошибках и предоставляет список возможных решений.

ЭС по внутрисистемной ЭМС ТС

На данный момент предложено несколько подходов к созданию ЭС, направленных на решение задач внутрисистемной ЭМС. Так, для решения задач многокритериальной оптимизации и оптимального проектирования военных кораблей с учетом ЭМС предложена ЭС, основанная на применении метода анализа иерархий трехмерных моделей [33]. Трехмерную модель корабля условно представляют в виде куба, каждая ось которого соответствует определенному критерию оценки. Критериями выступают эксплуатационные и технологические требования, электромагнитное излучение и его влияние на персонал/топливо/боеприпасы, стоимость производства и др. При использовании более трёх критериев требуется несколько таких моделей. При этом отмечено, что изменение одного параметра в соответствии с выбранными критериями может оказать как положительное, так и отрицательное влияние на результат, полученный по другим критериям.

Декомпозиция модели позволяет рационально расположить новое оборудование в системе корабля согласно установленным критериям. При этом каждая ось трехмерной модели ограничена значениями, которые соответствуют эксплуатационным требованиям и ограничениям на это оборудование. В случае выхода тестируемого оборудования за пороговые значения может быть поэтапно применена последовательность действий: изменение технических характеристик рассматриваемого оборудования; изменение характеристик всей системы оборудования корабля; частичная замена частей системы новым оборудованием с учетом эксплуатационных требований; подбор нового оборудования. Основная идея такого подхода к реализации ЭС состоит в получении результата, при котором результирующая трехмерная модель нового оборудования удовлетворяет идеальной ситуации по ЭМС всей системы. В случае если это оказывается невозможным, то ЭС предлагает наиболее близкий к ней вариант.

Возможности применения ЭС по ЭМС различных ТС в современной рабочей среде рассмотрены в работе [34]. В работе отмечено, что, несмотря на разработанные ЭС для проектирования ПП, автомобильных конструкций или других предметных областей, большинство из них – улучшенные системы контроля правил проектирования, включающие в себя аналитические или численные методы моделирования, позволяющие получить прогнозируемый результат. При этом применение ЭС по ЭМС после завершения этапа проектирования может привести к затратам временных и денежных ресурсов на перепроектирование. Поэтому целесообразно использо-

вание ЭС на всех этапах проектирования ТС. Для этого синтезирован алгоритм разработки ТС с применением ЭС по ЭМС (рис. 7).

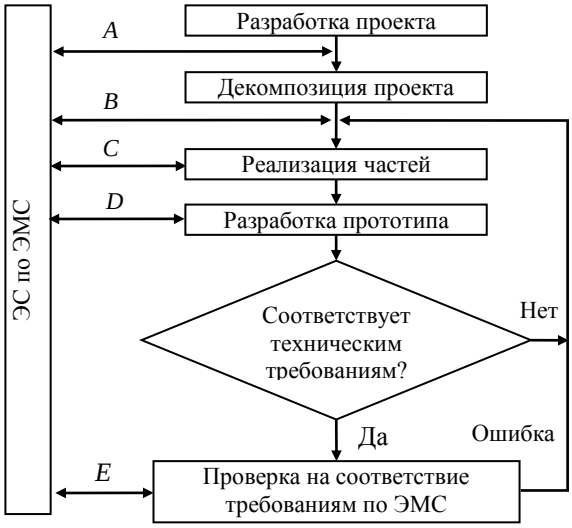

Рис. 7. Блок-схема алгоритма разработки ТС с применением ЭС по ЭМС [34]

На уровне *A* ЭС позволяет выявить потенциальные общесистемные проблемы по ЭМС. На уровне *B* происходит декомпозиция проекта на функциональные части и поиск возможных проблем по ЭМС в них. На уровнях *C* и *D* ЭС предлагает возможные изменения в компоновке составных частей, непосредственно взаимодействуя с соответствующими САПР. Последний уровень *D* предназначен для выдачи рекомендаций по решению оставшихся проблем по ЭМС.

Вопросам интеграции ЭС в существующие среды проектирования ТС посвящена работа [35]. Вариант такой интеграции на примере РЭС приведен на рис. 8. Так, на основании технического задания на разработку формируются проектные ограничения и критерии обеспечения ЭМС. Далее производится проектирование РЭС при помощи САПР. Взаимодействие между САПР и ЭС осуществляется с помощью модуля подготовки технической информации. На основе результатов проектирования ЭС генерирует рекомендации по обеспечению ЭМС, на основе которых в проект вносятся необходимые изменения.

Для оценки рисков возникновения проблем ЭМС ТС системы высокоскоростных железных дорог при её эксплуатации предложена четырехуровневая иерархическая модель, представленная на рис. 9 [36]. Так, возможные причины возникновения проблем ЭМС могут быть обусловлены множеством различных факторов, каждому из которых соответствует конкретное значение риска. При этом каждая из проблем в общем виде обусловлена наличием связи между источником и рецептором ЭМП. Процесс оценки риска с использованием модели состоит из нескольких этапов (рис. 10). Сначала выполняется определение рецептора ЭМП, после чего происходит построение его модели анализа риска. Далее с использованием значений риска каждого уровня и их весов рассчитывается общее значение риска ЭМС всей системы.

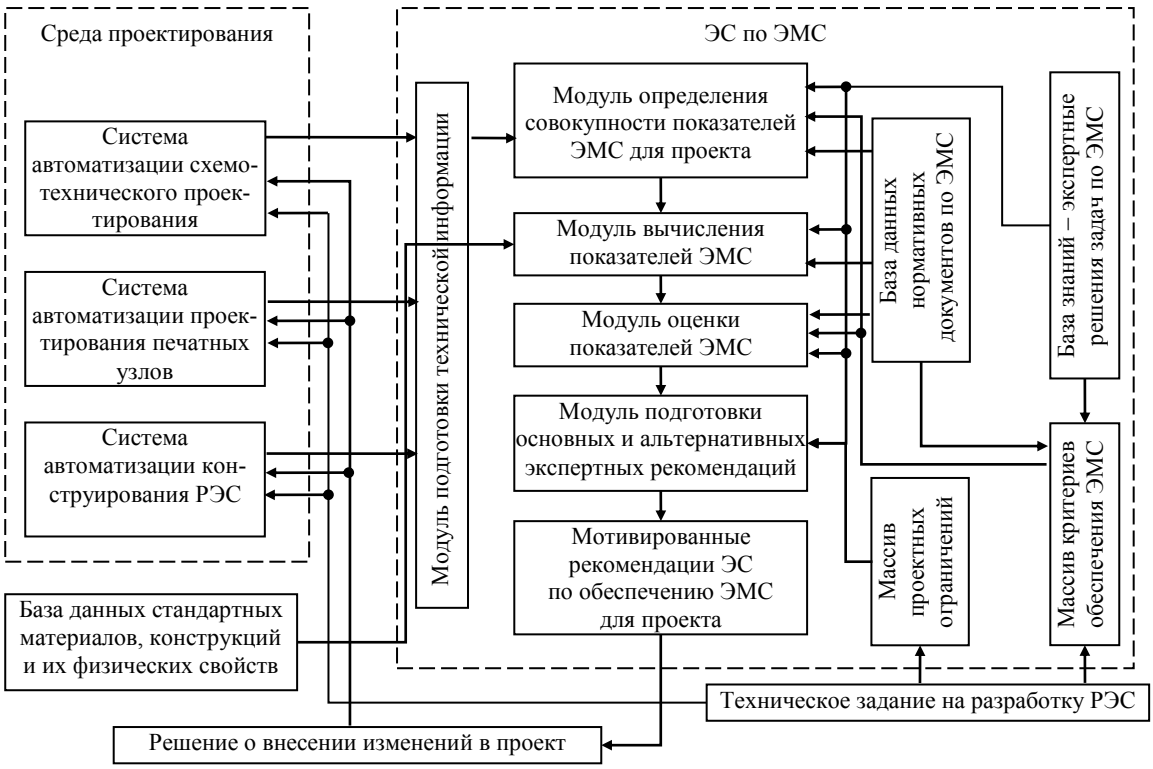

Рис. 8. Структурная схема интеграции ЭС по ЭМС в среду проектирования [35]

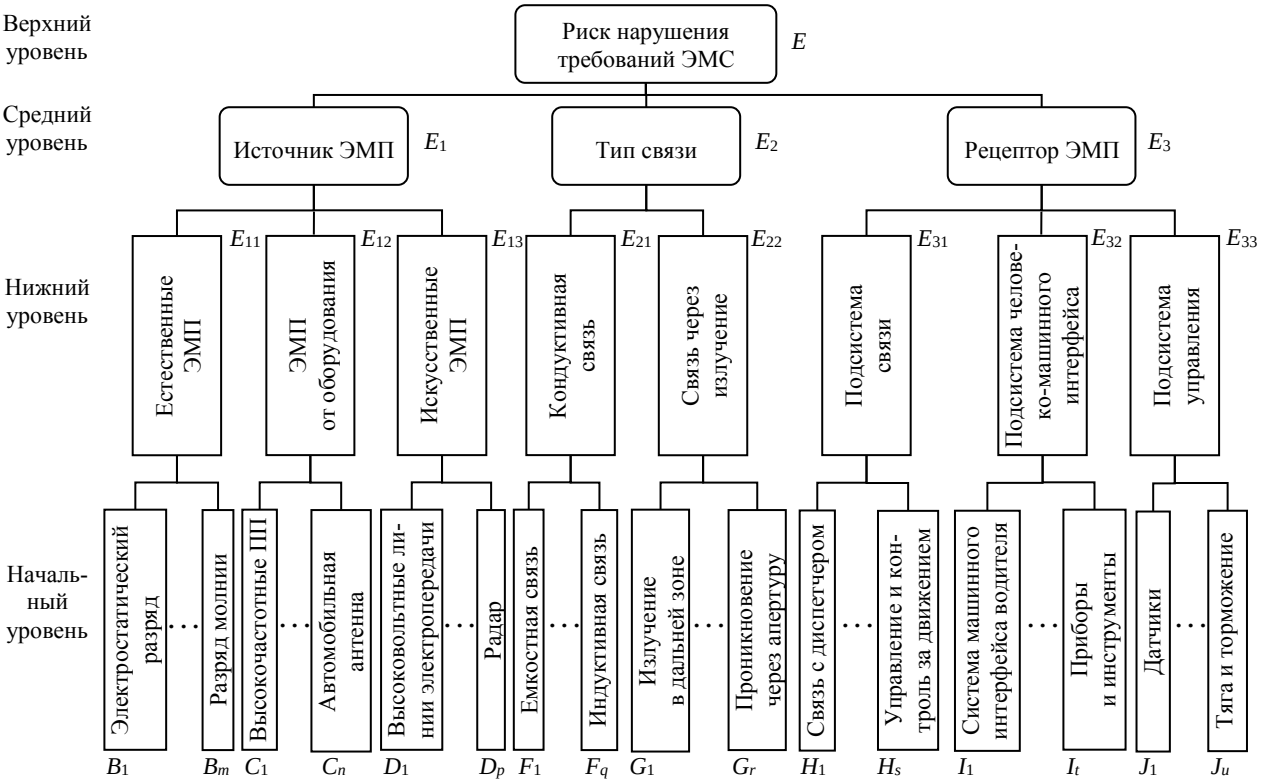

Рис. 9. Модель для анализа риска возникновения проблем ЭМС системы высокоскоростных железных дорог [36]

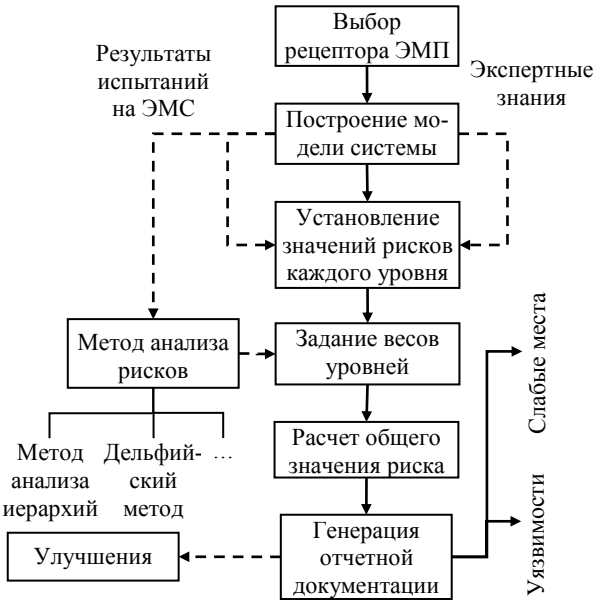

Рис. 10. Диаграмма процесса оценки риска возникновения проблем ЭМС системы железных дорог [36]

Отдельные значения рисков определяются на основе экспертных знаний, результатов испытаний или имеющейся статистики, а значения весов рассчитываются, например, с помощью метода анализа иерархий или аналогичных ему. На последнем этапе производится формирование отчетной документации, на основании которой могут быть выявлены уязвимости и предложены подходы к их устранению.

В работе [37] предложена ЭС по ЭМС автомобилей, которая позволяет выявить проблемы, связанные с излучением и помехоустойчивостью, перекрестными наводками, размещением модулей, заземлением компонентов и последующими испытаниями на ЭМС (рис. 11). В работе [38] выполнено сопоставление точности результатов вычисления перекрестных наводок, полученных с использованием алгоритмов оценки индуктивной и емкостной связей, с экспериментальными результатами на примере ТС автомобиля и предложены алгоритмы прогнозирования потенциальных проблем, обусловленных перекрестными наводками. В результате предлагается сравнивать полученные оценки уровня наводок, полученные в «наихудших случаях» работы алгоритма, со значениями, полученными из измерений или статистической обработки.

Методика разработки эффективной ЭС, которая используется для анализа, прогнозирования и проектирования ТС с учетом ЭМС на системном уровне, предложена в работе [39]. Так, в систему интегрированы базы данных и модули технических характеристик, проектирования и анализа ЭМС. Отличительной особенностью системы является то, что она разработана с использованием архитектуры клиент-сервер и поэтому может быть одновременно использована разработчиками через локальную компьютерную сеть (рис. 12).

ЭС по межсистемной ЭМС ТС

Вопросам разработки ЭС HardSys по ЭМС военной техники, в которой представление знаний основано на нечеткой логике, посвящена работа [40]. На примере боевого вертолета показано, что классификация электромагнитных характеристик в нечетком виде при использовании ЭС оказывается эффективным средством для определения его наиболее уязвимых мест по ЭМС.

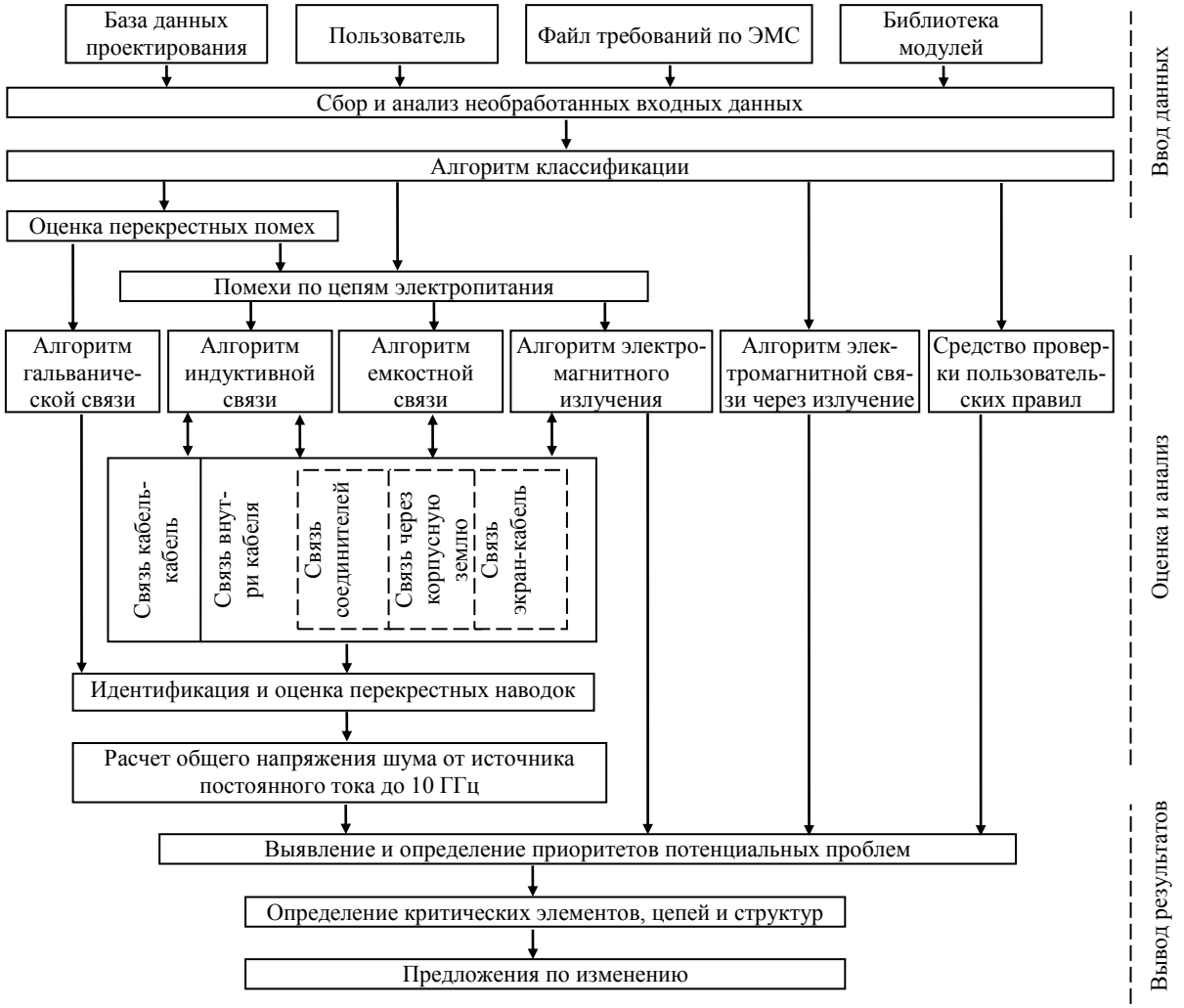

Рис. 11. Архитектура ЭС по ЭМС автомобилей [37]

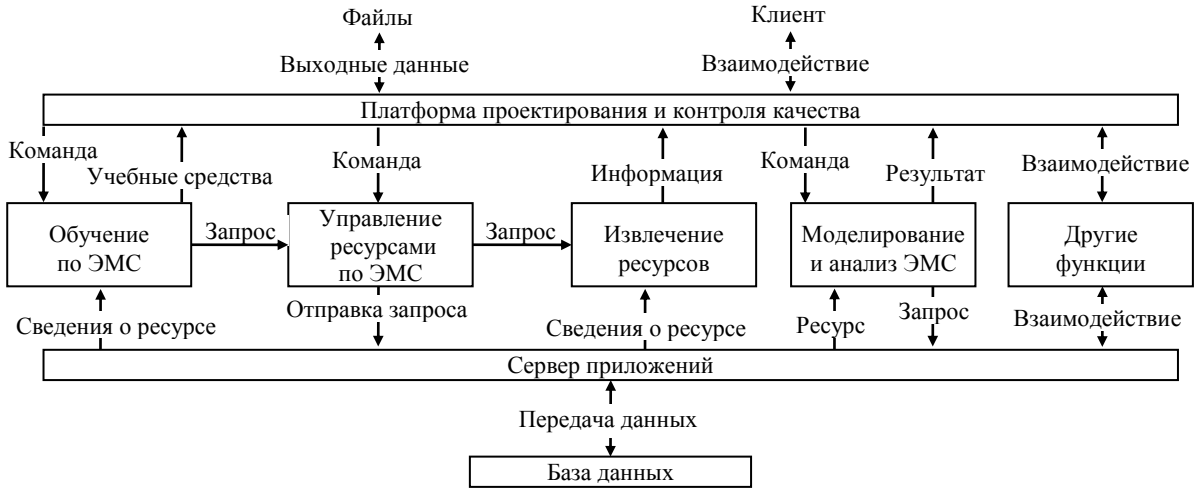

Рис. 12. Архитектура ЭС по ЭМС, основанная на сетевых взаимодействиях [39]

Рассмотрению результатов применения эвристического подхода, использующего базу знаний, к анализу ЭМС радиочастотных приемопередатчиков, близкорасположенных на платформе беспилотного летательного аппарата, посвящена работа [41]. Так, при постановке задачи обеспечения доступности корректной геометрической модели анализируемой системы используется ЭС предварительной обработки. База знаний построена таким образом, чтобы содержать основные правила моделирования и сценарии, описывающие шаги, задействованные в утвержденной нисходящей/восходящей методологии анализа ЭМС. Далее ЭС используется для мониторинга сигнальной обстановки во временной области

и выбора схем, подходящих для смягчения последствий влияния ЭМП, наводящихся на входные порты приемного устройства.

В работе [42] обсуждается применение подхода, основанного на знаниях, к задаче анализа ЭМС ТС в частотной и временной областях, а также представлены результаты использования ЭС E^{3}EXPERT, использующей методику валидации геометрических моделей анализируемых ТС. Система позволяет прогнозировать, ранжировать и устранять ЭМП, используя выбор схемы подавления помех, основанный на информации из базы знаний.

В работе [43] обсуждается применение ЭС EMC-Analyzer для решения задач ЭМС бортовых и наземных группировок радиотехнических систем в условиях жесткой электромагнитной обстановки. В ходе анализа линейные компоненты радиоприемников (входные цепи, фильтры, изоляция) моделируются в частотной области, а нелинейные с использованием их дискретных моделей и полиномиальных моделей высокого порядка – во временной области. При этом имеющийся функционал ЭС позволяет её использовать для моделирования как межсистемной, так и внутрисистемной ЭМС, а также систем заземления промышленных предприятий.

В работах [44, 45] использован подход к подавлению ЭМП систем расширения спектра по принципу прямой последовательности. Подход основан на использовании ЭС комплексной обработки сигналов при мониторинге среды для определения параметров помеховых сигналов с заданной точностью. После мониторинга окружающей среды система выбирает из специализированной библиотеки наиболее подходящий фильтр для подавления внешних ЭМП.

Заключение

В работе освещено современное состояние исследований по созданию ЭС. Из-за отсутствия в свободном доступе ознакомительных версий ЭС их сравнительный анализ не был выполнен. Поэтому акцент в работе был сделан на систематизацию информации, доступной в открытых научных источниках. Так, приведены краткие сведения об истории создания ЭС и их классификация. Указаны особенности построения современных ЭС по внутриаппаратной, внутрисистемной и межсистемной ЭМС. Показано, что одной из главных тенденций развития этих ЭС является их интегрирование со средами проектирования. Для полноты изложения приведены краткие сведения о функциональных возможностях и примеры построения известных ЭС по ЭМС ТС различного назначения.

Авторы благодарят рецензента за ценные замечания, благодаря которым статья была значительно улучшена.

Литература

1. Haider K.A. Development of expert systems methodologies and applications / K.A. Haider, Z.K. Rafiqul // International journal of information technology & management information system. – 2015. – Vol. 6. – P. 49–59.

2. Liao S. Expert system methodologies and applications – a decade review from 1995 to 2004 // Expert systems with applications. – 2005. – Vol. 28. – P. 93–103.

3. Automated identification of insulation faults using electro magnetic interference methods / J. Slater, I. Mitiche, A. Nesbitt, G. Morison, P. Boreham // Proc. of IEEE Electrical insulation conference. – Calgary, Canada: IEEE publ., 2019 – P. 473–476.

4. Jain M.B. A web based expert system shell for fault diagnosis and control of power system equipment / M.B. Jain, A. Jain, M.B. Srinivas // Proc. of International conference on condition monitoring and diagnosis. – Beijing, China: IEEE publ., 2008. – P. 1310–1313.

5. Jain M.B. A novel web based expert system architecture for on-line and off-line fault diagnosis and control (FDC) of power system equipment / M.B. Jain, M.B. Srinivas, A. Jain // Proc. of Joint International conference on power system technology and IEEE Power India conference. – Hyderabad, India: IEEE publ., 2008. – P. 1–5.

6. The application of fuzzy mathematics to transformer diagnosis expert system / Q. Ning, Y. Quan, D. Wang, J. Chen, W. Gao // Proc. of 9th IEEE International Conference on the properties and applications of dielectric materials. – Harbin, China: IEEE publ., 2009. – P. 161–164.

7. Tolun M.R. Expert systems / M.R. Tolun, S. Sahin, K. Oztoprak // Kirk-Othmer encyclopedia of chemical technology. – 2016. – P. 1–12.

8. Маренко В.А. Способы представления данных в экспертных системах // Математические структуры и моделирование. – 2001. – № 8. – С. 34–39.

9. Пат. 8 356 002 США, МПК G 06 F 17/00. Learning apparatus and method of intelligent system / R. Kim (KR), A. Moon (KR), T. Kang (KR), H. Kim (KR), H. Cho (KR). – № 12 / 123 039; заявл. 05.03.09; опубл. 15.01.13. – 8 с.

10. Agrawal R. Fast algorithms for mining association rules in large databases / R. Agrawal, R. Srikant // Proc. of 20th International conference on very large data bases. – Santiago, Chile: Morgan Kaufmann publ., 1994. – P. 487–499.

11. Agrawal R. Mining association rules between sets of items in large databases / R. Agrawal, T. Imieliński, A. Swami // Proc. of International conference on management of data (ACM SIGMOD). – Washington, USA: Association for computing machinery publ., 1993. – P. 207–216.

12. Demmin A.T. A web-based expert system for vehicle registration / A.T. Demmin, D.A. Zhang // Proc. of IEEE International conference of information reuse and integration. – Las Vegas, USA: IEEE publ., 2003. – P. 420–427.

13. Campos A.M. A real-time expert system architecture based on a novel dynamic task scheduling technique / A.M. Campos, D. Garcia // Proc. of IEEE International conference on industrial electronics, control and instrumentation (IECON02). – Seville, Spain: IEEE publ., 2002. – P. 1893–1898.

14. Mobile expert system: exploring context-aware machine learning rules for personalized decision-making in mobile applications / I.H. Sarker; A.I. Khan, Y.B. Abushark, F. Alsolami // Symmetry. – 2021. – Vol. 13, No. 10. – P. 1–10.

15. Sarker I.H. Machine learning: algorithms, real-world applications and research directions // SN computer science. – 2021. – Vol. 2, No. 160. – P. 1–20.

16. Requirement engineering techniques in developing expert systems / J.K. Ang, S.B. Leong, C.F. Lee, U.K. Yusof // Proc. of IEEE Symposium on computers & informatics. – Kuala Lumpur, Malaysia: IEEE publ., 2011. – P. 640–645.

17. Agarwal M. Expert system and it's requirement engineering process / M. Agarwal, S. Goel // Proc. of International

conference on recent advances and innovations in engineering. – Jaipur, India: IEEE publ., 2014. – P. 1–4.

18. Paul C.R. Transmission lines in digital systems for EMC practitioners. – Hoboken, New Jersey: John Wiley & Sons, 2012. – 270 p.

19. Computer-based design tools for EMC / M.D. Ganley, S.J. Porter, J.F. Dawson, A.C. Marvin, M.P. Ro-binson // Proc. of IEEE Colloquium on circuit design and tools for EMC. – London, UK: IET publ., 1995. – P. 1–7.

20. Hubing T. EMC Expert systems for evaluating automotive designs // Proc. of IEEE International symposium on electromagnetic compatibility. – Portland, USA: IEEE publ., 2006. – P. 840–841.

21. Frame based knowledge systems for EMC analysis / M. Surekha, A.B. Patki, G. Radha, A.V. Sudha, G.S. Sekhar, P. Shanthi // Proc. of IEEE International symposium on electromagnetic compatibility. – Washington, USA: IEEE publ., 1990. – P. 170–174.

22. Hubing T. An expert system approach to EMC modeling / T. Hubing, J. Drewniak, T. Van Doren, N. Kashyap // Proc. of Symposium on electromagnetic compatibility. – Santa Clara, USA: IEEE publ., 1996. – P. 1–4.

23. Expert system algorithms for EMC analysis / T. Hubing, N. Kashyap, J. Drewniak, T. Van Doren // Proc. of 14th Annual review of progress in applied computational electromagnetics. – Monterey, USA: ACES publ., 1998. – P. 905–910.

24. EMC analysis in PCB designs using an expert system / K.N. Rao, P. Venkata Ramana, M.V. Krishnamurthy, K. Srinivas // Proc. of International conference on electromagnetic interference and compatibility (INCEMIC). – Madras, India: IEEE publ., 1995. – P. 59–62.

25. Lai S. Progress of expert systems in electromagnetic engineering / S. Lai, B. Wang // Journal of electronic science and technology of China. – 2005. – Vol. 3, No. 4. – P. 328–333.

26. A method of automatic placement that reduces electromagnetic radiation noise from digital printed circuit boards / Y. Fukumoto, S. Miura, H. Ikeda, T. Nakayama, S. Tanimoto, H. Uemura // Proc. of IEEE International symposium on electromagnetic compatibility. – Washington, USA: IEEE publ., 2000. – P. 363–368.

27. Expert system algorithms for identifying radiated emission problems in printed circuit boards / H. Shim, T. Hubing, T. Van Doren, R. Dubroff, J. Drewniak, D. Pommerenke, R. Kires // Proc. of IEEE International symposium on electromagnetic compatibility. – Silicon Valley, USA: IEEE publ., 2004. – P. 1–6.

28. Fu Y. Analysis of radiated emissions from a printed circuit board using expert system algorithms / Y. Fu, T. Hubing // IEEE Transactions on electromagnetic compatibility. – 2007. – Vol. 49. – P. 68–75.

29. Research on remote EMC testing system / X. Lei, L. Shanghe, L. Guangqiang, J. Mingji // Proc. of 5th Asia-Pacific conference on environmental electromagnetics. – Xi'an, China: IEEE publ., 2009. – P. 281–284.

30. Van Doorn M. EMC expert system for architecture design // Proc. of Asia-Pacific EMC symposium. – Jeju Island, Korea, 2011. – P. 1–4.

31. Expert system FILTEX32 for computer-aided design of bandpass microstrip filters / B.A. Belyaev, S.V. Butakov, N.V. Laletin, A.A. Leksikov, V.V. Tyumev // Proc. of 15th International Crimean conference microwave & telecommunication technology. – Sevastopol, Ukraine: IEEE publ., 2005. – P. 504–505.

32. Kvasnikov A.A. Prototype of EMC Expert system for optimal design of radio-electronic equipment / A.A. Kvasnikov, S.P. Kuksenko, F.F. Idrisov // Journal of Physics: Conference Series. – 2021. – Vol. 1862, No. 012020. – P. 1–6.

33. Tayal M. Expert system using electromagnetic interference and electromagnetic compatibility based criteria for ship design, weapon selection and evaluation / M. Tayal, V. Waman Karve // Proc. of IEEE conference on electromagnetic interference and compatibility. – Hyderabad, India: IEEE publ., 1997. – P. 1–6.

34. Keyer C. EMC expert systems for our modern working environment / C. Keyer, F. Leferink // Proc. of International symposium on electromagnetic compatibility (EMC EUROPE). – Rome, Italy: IEEE publ., 2012. – P. 1–5.

35. Лемешко Н.В. Об использовании экспертных систем для решения задач электромагнитной совместимости // Теория и техника радиосвязи. – 2016. – № 4. – С. 48–52.

36. Li M. Applying risk assessment technique to electromagnetic compatibility analysis in Chinese high speed railway / M. Li, Y. Wen // Proc. of 6th IEEE International symposium on microwave, antenna, propagation, and EMC technologies (MAPE). – Shanghai, China: IEEE publ., 2015. – P. 441–445.

37. An expert system architecture to detect system-level automotive EMC problems / S. Ranganathan, D.G. Beetner, R. Wiese, T.H. Hubing // Proc. of IEEE International symposium on electromagnetic compatibility. – Minneapolis, USA: IEEE publ., 2002. – Vol. 2. – P. 976–981.

38. Validation of worst-case and statistical models for an automotive EMC expert system / D. Beetner, H. Weng, M. Wu, T. Hubing // Proc. of IEEE International symposium on electromagnetic compatibility. – Honolulu, USA: IEEE publ., 2007. – P. 1–5.

39. A system-level EMC technical support platform for network-based computers / Q. Wu, J.H. Fu, F.Y. Meng, H.L. Wang, B.S. Jin, F. Zhang // Proc. of Asia-Pacific symposium on electromagnetic compatibility and 19th International Zurich symposium on electromagnetic compatibility. – Singapore: IEEE publ., 2008. – P. 642–645.

40. Lo Vetri J. Evaluation of HardSys: a simple EMI expert system / J. Lo Vetri, A.S. Podgorski // Proc. of IEEE international symposium on electromagnetic compatibility. – Washington, USA: IEEE publ., 1990. – P. 228–232.

41. Demirkiran I. Knowledge-based approach to interference mitigation for EMC of transceivers on unmanned aircraft / I. Demirkiran, D.D. Weiner, A. Drozd, I. Kasperovich // Proc. of IEEE International symposium on electromagnetic compatibility. – Fort Lauderdale, USA: IEEE publ., 2010. – P. 425–430.

42. Application and demonstration of a knowledge-based approach to interference rejection for EMC / A. Drozd, A. Pesta, D. Weiner, P. Varshney, I. Demirkiran // Proc. of IEEE International symposium on electromagnetic compatibility. – Denver, USA: IEEE publ., 1998. – P. 537–542.

43. Mordachev V. Advanced options of expert system «EMC-Analyzer» / V. Mordachev, P. Litvinko // Proc. of International Symposium on EMC. EMC Europe. – Barcelona, Spain: Technical university of Catalonia publ., 2006. – P. 635–640.

44. Knowledge-based approach to interference rejection for EMC / I. Demirkiran, V.N.S. Samarasooriya, P.K. Varshney, D.D. Weiner, R. Mani, S. Hamid Nawab, S. Tyler // Proc. of IEEE International symposium on electromagnetic compatibility. – Denver, USA: IEEE publ., 1998. – P. 1150–1155.

45. A Knowledge-based approach to interference rejection for direct-sequence spread spectrum (DSSS) systems / U. Demirkiran, D.D. Weiner, P. Varshney, A. Drozd // Proc. of International waveform diversity & design conference. – Lihue, USA: IEEE publ., 2006. – P. 1–6.

Квасников Алексей Андреевич
Аспирант каф. телевидения и управления (ТУ)
Томского гос. ун-та систем управления
и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0001-7000-956X
Тел.: + 7 (382-2) 41-34-39
Эл. почта: aleksejkvasnikov@tu.tusur.ru

Куксенко Сергей Петрович
Д-р. техн. наук., профессор каф. ТУ ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0001-9713-458X
Тел.: +7 (382-2) 41-34-39
Эл. почта: ksergp@tu.tusur.ru

Kvasnikov A.A.., Kuksenko S.P.

Review of expert systems for electromagnetic compatibility of technical equipment

This paper presents a review of expert systems for electromagnetic compatibility of technical equipment. The history of development and classification of modern expert systems are described. The main elements and features of software architecture development are indicated, as well as examples of expert systems for electromagnetic compatibility of technical equipment for various purposes.

Keywords: electromagnetic compatibility, expert system, technical equipment, radio electronic equipment, printed circuit board, transmission line.
DOI: 10.21293/1818-0442-2021-24-4-7-18

References

1. Haider K.A., Rafiqul Z.K. Development of expert systems methodologies and applications. *International Journal of Information Technology & Management Information System*, 2015, vol. 6, pp. 49–59.

2. Liao S. Expert system methodologies and applications – a decade review from 1995 to 2004. *Expert Systems with Applications*, 2005, vol. 28, pp. 93–103.

3. Slater J., Mitiche I., Nesbitt A., Morison G., Boreham P. Automated identification of insulation faults using electro magnetic interference methods. *Proc. of IEEE Electrical Insulation Conference*. Calgary, Canada, IEEE Publ., 2019, pp. 473–476.

4. Jain M.B., Jain A., Srinivas M.B. A web based expert system shell for fault diagnosis and control of power system equipment. *Proceedings of International Conference on Condition Monitoring and Diagnosis*. Beijing, China, IEEE Publ., 2008, pp. 1310–1313.

5. Jain M.B., Srinivas M.B., Jain A. A novel web based expert system architecture for on-line and off-line fault diagnosis and control (FDC) of power system equipment. *Proceedings of Joint International Conference on Power System Technology and IEEE Power India Conference*. Hyderabad, India, IEEE Publ., 2008, pp. 1–5.

6. Ning Q., Quan Y., Wang D., Chen J., Gao W. The application of fuzzy mathematics to transformer diagnosis expert system. *Proceedings of 9th IEEE International Conference on the Properties and Applications of Dielectric Materials*. Harbin, China, IEEE Publ., 2009, pp. 161–164.

7. Tolun M.R., Sahin S., Oztoprak K. Expert systems. *Kirk-Othmer Encyclopedia of Chemical Technology*, 2016, pp. 1–12.

8. Marenko V.A. *Sposoby predstavleniya dannyh v ekspertnyh sistemah* [Methods for presenting data in expert systems]. *Mathematical Structures and Modeling*, 2001, no. 8, pp. 34–39 (in Russ.).

9. Kim. R, Moon A., Kang T., Kim H., Cho H. Learning apparatus and method of intelligent system. Patent US, no. 8356002, 2013.

10. Agrawal R., Srikant R. Fast algorithms for mining association rules in large databases. *Proceedings of 20th International Conference on Very Large Data Bases.* Santiago, Chile, Morgan Kaufmann Publ., 1994, pp. 487–499.

11. Agrawal R., Imieliński T., Swami A. Mining association rules between sets of items in large databases. *Proceedings of International Conference on Management of Data (ACM SIGMOD).* Washington, USA, Association for computing machinery Publ., 1993, pp. 207–216.

12. Demmin A.T., Zhang D.A. A web-based expert system for vehicle registration. *Proceedings of IEEE International Conference of Information Reuse and Integration.* Las Vegas, USA, IEEE Publ., 2003, pp. 420–427.

13. Campos A.M., Garcia D. A real-time expert system architecture based on a novel dynamic task scheduling technique. *Proceedings of IEEE International Conference on Industrial Electronics, Control and Instrumentation (IECON02).* Seville, Spain, IEEE Publ., 2002, pp. 1893–1898.

14. Sarker I.H., Khan A.I., Abushark Y.B., Alsolami F. Mobile expert system: exploring context-aware machine learning rules for personalized decision-making in mobile applications. *Symmetry*, 2021, vol. 13, no. 10, pp. 1–10.

15. Sarker I.H. Machine learning: algorithms, real-world applications and research directions. *SN Computer Science*, 2021, vol. 2, no. 160, pp. 1–20.

16. Ang J.K., Leong S.B., Lee C.F., Yusof U.K. Requirement engineering techniques in developing expert systems. *Proceedings of IEEE Symposium on Computers & Informatics.* Kuala Lumpur, Malaysia, IEEE Publ., 2011, pp. 640–645.

17. Agarwal M., Goel S. Expert system and it's requirement engineering process. *Proceedings of International Conference on Recent Advances and Innovations in Engineering.* Jaipur, India, IEEE Publ., 2014, pp. 1–4.

18. Paul C.R. *Transmission lines in digital systems for EMC practitioners*. Hoboken, New Jersey, John Wiley & Sons, 2012. 270 p.

19. Ganley M.D., Porter S.J., Dawson J.F., Marvin A.C., Robinson M.P. Computer-based design tools for EMC. *Proceedings of IEEE Colloquium on Circuit Design and Tools for EMC.* London, UK, IET Publ., 1995, pp. 1–7.

20. Hubing T. EMC Expert systems for evaluating automotive designs. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility.* Portland, USA, IEEE Publ., 2006, pp. 840–841.

21. Surekha M., Patki A.B., Radha G., Sudha A.V., Sekhar G.S., Shanthi P. Frame based knowledge systems for EMC analysis. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. Washington, USA, IEEE Publ., 1990, pp. 170–174.

22. Hubing T., Drewniak J., Van Doren T., Kashyap N. An expert system approach to EMC modeling. *Proceedings of Symposium on Electromagnetic Compatibility.* Santa Clara, USA, IEEE Publ., 1996, pp. 1–4.

23. Hubing T., Kashyap N., Drewniak J., Van Doren T. Expert system algorithms for EMC analysis. *Proceedings of 14th Annual Review of Progress in Applied Computational Electromagnetic*. Monterey, USA, ACES publ., 1998, pp. 905–910.

24. Nageswara Rao K., Venkata Ramana P., Krishnamurthy M.V., Srinivas K. EMC analysis in PCB designs using an expert system. *Proceedings of International Conference on*

Electromagnetic Interference and Compatibility (INCEMIC). Madras, India, IEEE Publ., 1995, pp. 59–62.

25. Lai S., Wang B. Progress of expert systems in electromagnetic engineering. *Journal of Electronic Science and Technology of China*, 2005, vol. 3, no. 4, pp. 328–333.

26. Fukumoto Y., Miura S., Ikeda H., Nakayama T., Tanimoto S., Uemura H. A method of automatic placement that reduces electromagnetic radiation noise from digital printed circuit boards. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. Washington, USA, IEEE Publ., 2000, pp. 363–368.

27. Shim H., Hubing T., Van Doren T., Dubroff R., Drewniak J., Pommerenke D., Kires R. Expert system algorithms for identifying radiated emission problems in printed circuit boards. *Proceedings of IEEE International Conference of Information Reuse and Integration*. Silicon Valley, USA, IEEE Publ., 2004, pp. 1–6.

28. Fu Y., Hubing T. Analysis of radiated emissions from a printed circuit board using expert system algorithms. *IEEE Transactions on Electromagnetic Compatibility*, 2007, vol. 49, pp. 68–75.

29. Lei X., Shanghe L., Guangqiang L., Mingji J. Research on remote EMC testing system. *Proceedings of 5th Asia-Pacific Conference on Environmental Electromagnetics*. Xi'an, China, IEEE Publ., 2009, pp. 281–284.

30. Van Doorn M. EMC Expert system for architecture design. *Proceedings of Asia-Pacific EMC Symposium*. Jeju Island, Korea, 2011, pp. 1–4.

31. Belyaev B.A., Butakov S.V., Laletin N.V., Leksikov A.A., Tyumev V.V. Expert system FILTEX32 for computer-aided design of bandpass microstrip filters. *Proceedings of 15th International Crimean Conference Microwave & Telecommunication Technology.* Sevastopol, Ukraine, IEEE Publ., 2005, pp. 504–505.

32. Kvasnikov A.A., Kuksenko S.P., Idrisov F.F. Prototype of EMC Expert system for optimal design of radioelectronic equipment. *Journal of Physics: conference series*, 2021, vol. 1862, no. 012020, pp. 1–6.

33. Tayal M., Waman Karve V. Expert system using electromagnetic interference and electromagnetic compatibility based criteria for ship design, weapon selection and evaluation. *Proceedings of IEEE on Electromagnetic Interference and Compatibility*. Hyderabad, India, IEEE Publ., 1997, pp. 1–6.

34. Keyer C., Leferink F. EMC Expert Systems for our modern working environment. *Proceedings of International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. Rome, Italy, IEEE Publ., 2012, pp. 1–5.

35. Lemeshko N.V. *Ob ispolzovanii ekspertnyh sistem dlya resheniya zadach elektromagnitnoi sovmestimosti* [On the use of expert systems for solving problems of electromagnetic compatibility]. *Theory and Technology of Radio Communication*, 2016, no. 4, pp. 48–52 (in Russ.).

36. Li M., Wen Y. Applying risk assessment technique to electromagnetic compatibility analysis in Chinese high speed railway. *Proceedings of 6th IEEE International Symposium on Microwave, Antenna, Propagation, and EMC Technologies (MAPE)*. Shanghai, China, IEEE Publ., 2015, pp. 441–445.

37. Ranganathan S., Beetner D.G., Wiese R., Hubing T. An expert system architecture to detect system-level automotive EMC problems. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility.* Minneapolis, USA, IEEE Publ., 2002, vol. 2, pp. 976–981.

38. Beetner D., Weng H., Wu M., Hubing T. Validation of worst-case and statistical models for an automotive EMC expert system. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. Honolulu, USA, IEEE Publ., 2007, pp. 1–5.

39. Wu Q., Fu J.H., Meng F.Y., Wang H.L., Jin B.S., Zhang F. A system-level EMC technical support platform for network-based computers. *Proceedings of Asia-Pacific Symposium on Electromagnetic Compatibility and 19th International Zurich Symposium on Electromagnetic Compatibility.* Singapore, IEEE Publ., 2008, pp. 642–645.

40. Lo Vetri J., Podgorski A.S. Evaluation of HardSys: a simple EMI expert system. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. Washington, USA, IEEE Publ., 1990, pp. 228–232.

41. Demirkiran I., Weiner D.D., Drozd A., Kasperovich I. Knowledge-based approach to interference mitigation for EMC of transceivers on unmanned aircraft. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. Fort Lauderdale, USA, IEEE Publ., 2010, pp. 425–430.

42. Drozd A., Pesta A., Weiner D., Varshney P., Demirkiran I. Application and demonstration of a knowledge-based approach to interference rejection for EMC. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. Denver, USA, IEEE Publ., 1998, pp. 537–542.

43. Mordachev V., Litvinko P. Advanced options of expert system «EMC-Analyzer». *Proceedings of International Symposium on EMC. EMC Europe.* Barcelona, Spain, Technical university of Catalonia Publ., 2006, pp. 635–640.

44. Demirkiran I., Samarasooriya V.N.S., Varshney P.K., Weiner D.D., Mani R., Hamid Nawab S., Tyler S. Knowledge-based approach to interference rejection for EMC. *Proceedings of IEEE International Symposium on Electromagnetic Compatibility*. Denver, USA, IEEE Publ., 1998, pp. 1150–1155.

45. Demirkiran U., Weiner D.D., Varshney P., Drozd A. A Knowledge-based approach to interference rejection for direct-sequence spread spectrum (DSSS) systems. *Proceedings of International Waveform Diversity & Design Conference*. Lihue, USA, IEEE Publ., 2006, pp. 1–6.

Aleksey A. Kvasnikov
Postgraduate student, Department of Television and Control,
Tomsk State University of Control Systems and
Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0001-7000-956X
Phone: +7 (382-2) 41-34-39
Email: aleksejkvasnikov@tu.tusur.ru

Sergei P. Kuksenko
Doctor of Science in Engineering, Professor,
Department of Television and Control, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0001-9713-458X
Phone: +7 (382-2) 41-34-39
Email: ksergp@tu.tusur.ru

УДК 621.382

И.А. Белова, М.В. Мартинович, Д.Ю. Федорова

Источник искусственного освещения, имитирующий солнечный спектр, для тестирования солнечных батарей

Разработан комбинированный источник искусственного освещения для исследования характеристик солнечных элементов. Произведен спектральный анализ различных источников излучения. На основе анализа были подобраны необходимые источники излучения, суммарный спектр которых после аппроксимации близок к спектру солнечного излучения. Выполнен расчет электрооптических характеристик. Рассчитано количество источников искусственного освещения для воспроизведения спектра солнечного излучения. Сделаны соответствующие выводы.

Ключевые слова: солнечный спектр, имитация солнечного излучения, солнечные батареи.
DOI: 10.21293/1818-0442-2021-24-4-19-24

Актуальность солнечной энергетики постоянно растет и является уже не просто перспективой, а переходит к масштабному практическому применению, которое расширяется с каждым годом. Солнечные батареи (СБ) находят применение в космической отрасли, промышленности, бытовых нуждах и т.д. По мере расширения области применения расширяются и требования к системам управления, которые должны работать на высоком уровне и отслеживать точку максимальной мощности солнечных батарей. Для этого современные системы управления оснащаются интеллектуальными устройствами, которые позволяют с высокой точностью отбирать от солнечной батареи максимальную энергию [1, 2]. При проектировании таких систем необходимо проводить предварительные испытания солнечных батарей и исследовать, как изменяются их вольт-амперные и вольт-ваттные характеристики при изменении условий окружающей среды, таких как мощность солнечного излучения (освещенность) и температура. Для построения модели солнечной батареи характеристики которой полностью совпадают с характеристиками реальной солнечной батареи необходимо провести соответствующие эксперименты. Так как проведение экспериментов проходит в лабораторных условиях, то спектр лабораторного источника освещения должен быть максимально приближен к спектру солнечного излучения [3–5].

Солнечное излучение определяется несколькими наиболее важными параметрами: солнечная постоянная и воздушная масса. Воздушная масса (Airmass или AM) – это показатель влияния атмосферы на интенсивность солнечного излучения, дошедшую до поверхности Земли. Спектральное распределение интенсивности солнечного излучения при разных значениях воздушных масс будет отличаться [6].

Средняя интенсивность излучения на Земле совпадает с интенсивностью излучения при AM =1,5 (солнце находится под углом 45° к горизонту) [7]. При исследовании работы солнечных батарей используют AM =1,5 т.е. максимальная мощность солнечного излучения равна 1000 Вт/м^2 и солнце находится под углом 45° к горизонту.

Спектр солнечного излучения на поверхности Земли определен международным стандартом ISO 9845-1, 1992 [8]. Этот стандарт характеризует стандартное распределение спектрального излучения, которое должно использоваться для определения относительной эффективности солнечных тепловых, фотовольтаических и других систем, в которых желателен компонент прямой и полусферической освещенности. Для адекватного исследования характеристик солнечных батарей в лабораторных условиях необходимо создать такой источник искусственного освещения, который максимально точно будет воспроизводить стандартный спектр, показанный на рис. 1.

Целью данного исследования является разработка модуля источника искусственного освещения, обеспечивающего воспроизведение солнечного спектра в диапазоне длин волн в зоне поглощения солнечной батареи, и создание методики расчета для различных спектров излучения и поглощения и для разного набора искусственных осветительных приборов.

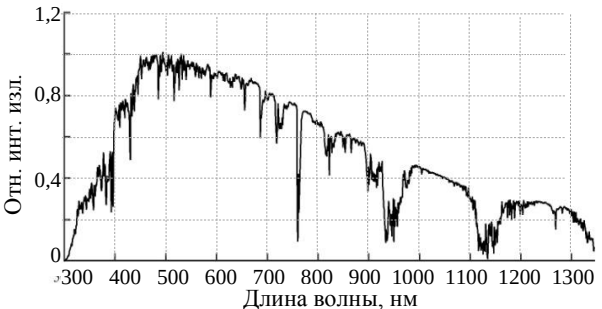

Рис. 1. Спектр солнечного излучения, установленный международным стандартом ISO 9845-1

Имитаторы солнечного излучения

Для исследования имитаторов солнечного излучения были сформированы основные требования, предъявляемые к излучателю:

• соответствие спектру естественного солнечного излучения;

• однородность падающего потока излучения;

• высокая временная стабильность параметров излучения;

• соответствие площади облучаемой поверхности размеру источника солнечного излучения.

Создать источник, который мог бы полностью удовлетворять вышеуказанным пунктам, на практике не предоставляется возможным. Именно поэтому практическое исследование имитаторов солнечного излучения обычно проходит по трем направлениям:

• использование коэффициентов коррекции, которые учитывают разницу между солнечным и суммарным спектрами излучения;

• применение фильтров, оптимизированных под используемый световой прибор;

• использование в имитаторе нескольких источников света, которые излучают только в относительно узком диапазоне длин волн с определенной интенсивностью.

Одним из примеров такого исследования является статья [9], в которой рассмотрено десять современных имитаторов солнечного излучения как отечественного, так и зарубежного производства. Из них восемь – серийного промышленного производства и два – единичных лабораторных образца, разработанных в научных центрах и исследовательских институтах. Целью исследования являлось комплексное представление о качестве имитации солнечного излучения рассматриваемых имитаторов, а также сравнительный анализ по некоторым параметрам. В процессе своего исследования авторы произвели анализ всех имитаторов по ключевым параметрам: источник излучения, спектральное соответствие солнечному излучению, неоднородность уровней плотностей падающего потока излучения, временная нестабильность, площадь облучаемой поверхности. Выявив плюсы и минусы каждого имитатора, определили оптимальные параметры и конструктивные особенности, которые представлялись наиболее эффективными.

Авторами были сделаны выводы о преимуществах и недостатках каждого из имитаторов. В восьми из десяти имитаторов в качестве источника использованы ксеноновые лампы, преимуществом которых является мощный световой поток с минимальным нагревом.

Еще одно практическое исследование, цель которого заключалась в воспроизведении спектра естественного солнечного излучения, проводилось в лаборатории Мордовского государственного университета им. Н.П. Огарева [10]. В качестве имитатора солнечного света использовали комбинации из пяти и семи типов светодиодов. Решая задачу, направленную на получение установленного спектра излучения на основе светодиодов, авторы построили математическую модель в программной среде MatLab, в которой за исходные данные были приняты спектры излучения всех компонентов люминесцентной смеси или спектры нескольких однотонных светодиодов. При моделировании процесса излучения проводилось исследование процедуры повышения цветопередачи для источника, спектральное распределение интенсивности которого соответствует спектру солнечного излучения. Выполнив расчеты среднеквадратичной ошибки аппроксимации спектра, В.В. Афонин и О.Ю. Коваленко произвели модельный эксперимент, в котором число светодиодов каждого типа задавалось от 0 до 400. Рабочий программный алгоритм напоминал метод покоординатного спуска, где в качестве значения каждой координаты использовалось число светодиодов определенного типа. На каждой итерации цикла производилось вычисление среднеквадратичной ошибки. Результатом моделирования являлось значение спектральной мощности излучения, мощность излучения светодиода, а также относительная погрешность. Анализируя спектр, который был получен в ходе исследования (рис. 2), можно отметить тот факт, что авторам не удалось добиться максимально приближенного спектра естественного солнечного излучения. У полученного спектра существуют провалы в области синего излучения и нехватка излучения в УФ- и ИК-зоне.

Оценка источников искусственного освещения и их спектрального распределения выявила основные преимущества и недостатки каждого источника. Можно сделать вывод, что галогенные лампы и светодиоды имеют хорошие оптические характеристики для использования при имитации солнечного излучения.

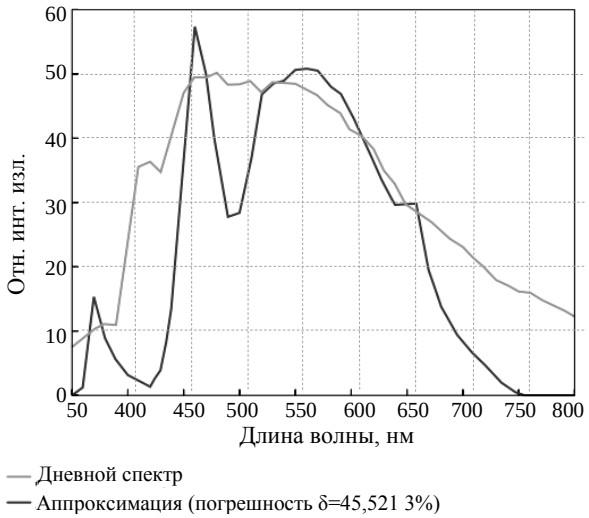

Рис. 2. Результат аппроксимации спектра солнечного излучения

Методика расчета

Исследований по воспроизведению спектра солнечного излучения и получению точных значений параметров и характеристик СБ, которые бы соответствовали ее реальной работе, проводилось довольно много, но практических результатов, которые можно воспроизвести в любой лаборатории, практически нет.

Авторами была сформулирована методика расчета стенда для исследования характеристик солнечных батарей, которая состоит из следующих пунктов:

1. Выбор источников искусственного освещения, отталкиваясь от их спектрального распределения интенсивности излучения.

2. Расчет основных электрооптических характеристик для каждого источника. Иными словами, на данном этапе необходимо определить силу света, телесный угол, световой поток и светоотдачу, зная которые, можно произвести расчет мощности излучения каждого источника.

3. Расчет количества источников излучения, используемых в качестве имитатора солнечного излучения.

4. Определение суммарной мощности излучения имитатора солнечного излучения, зная количество источников и их мощность излучения.

5. На основании полученной общей (полной) мощности излучения, производится расчет плотности мощности выделяемого излучения (Вт/дм^2).

6. Определение количества имитаторов, которые будут обеспечивать необходимую мощность излучения.

Реализация

1. *Выбор источников.*

В ходе выполнения работы были исследованы источники искусственного освещения и проанализированы их спектральные распределения.

Проанализированы спектры источников света: галогенной лампы, белого светодиода теплого свечения, голубого светодиода (λ~ 505 нм), ИК-светодиодов: λ~880; ~940; ~1050 нм.

Анализ спектральных распределений различных источников искусственного освещения помог определить их наиболее удачную комбинацию, аппроксимация которых дает спектр, близкий к спектру солнечного излучения, без значительных провалов, с небольшим набором источников. Данный спектр показан на рис. 3.

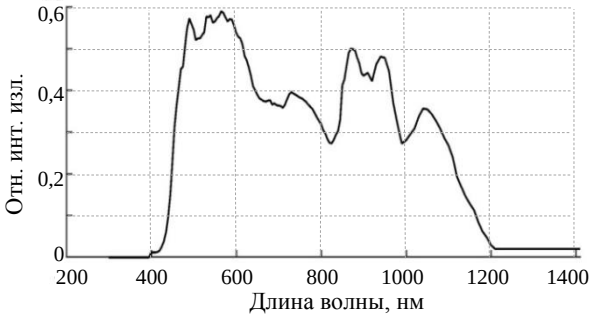

Рис. 3. Аппроксимация искусственных источников освещения без корректировки

Полученная комбинация источников искусственного освещения включает в себя 6 источников: галогенная лампа, голубой и белый (теплый) светодиоды, а также 3 инфракрасных светодиода с длинами волн λ_1~880, λ_2~940, λ_3~1050 нм.

Диапазон поглощения солнечных модулей всех типов расположен в длинах волн 300–1200 нм [11, 12]. В работе [13] И.М. Несмелова и Н.И. Астафьев подробно описывают оптические свойства монокристаллического кремния и особенности его спектрального поглощения. Спектр поглощения кремниевой солнечной батареи показан на рис. 4.

Следовательно, провалы в левой части спектра не требуют исключения в связи с тем, что спектр поглощения кремниевой солнечной батареи расположен в диапазоне λ ~380–1200 нм.

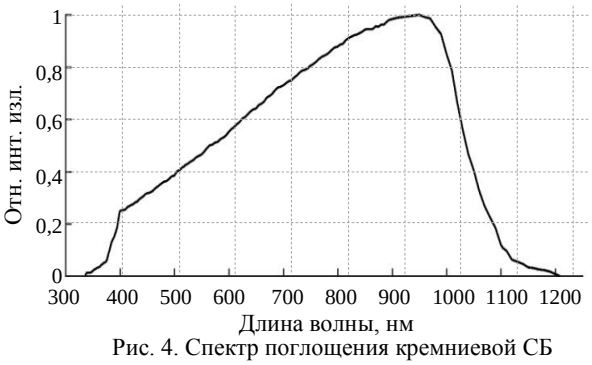

Рис. 4. Спектр поглощения кремниевой СБ

Учитывать спектральную чувствительность солнечных элементов нужно для того, чтобы получить эквивалентные мощности излучения.

2. *Расчет основных электрооптических характеристик.*

Для расчета мощности излучения необходимо знать световой поток Ф (лм) [14, 15]. Если в техническом паспорте источника он не указан, то его можно рассчитать, зная силу света I (кд) и телесный угол Ω(ср), по формуле

$$dK = I \cdot d\Omega. \qquad (1)$$

Чаще всего в документации на источники искусственного освещения указывается угол обзора Θ (градус), который по формуле легко можно перевести в телесный:

$$d\Phi = 2\pi\left(1-\cos\frac{\theta}{2}\right). \qquad (2)$$

Мощность излучения находится через определенный интеграл (от начального интервала длины волны к конечному), взятый от светового потока, умноженного на спектральную полосу пропускания Δλ:

$$P_{\text{изл}} = \int_{\lambda_1}^{\lambda_2} \Phi(\lambda)\cdot\Delta\lambda\cdot d\lambda. \qquad (3)$$

Световая отдача источников света определяется отношением полного светового потока к его потребляемой мощности

$$K_\lambda = \frac{\Phi(\lambda)}{P_{\text{потр}}}. \qquad (4)$$

КПД источников искусственного освещения рассчитывается по формуле

$$\eta = \frac{P_{\text{изл}}}{P_{\text{потр}}}\cdot 100\%. \qquad (5)$$

Результаты приведены в табл. 1. Обратим внимание, что выбранные источники освещения имеют высокий КПД.

Таблица 1

Мощности излучения различных источников

n	Источник искусственного излучения	Мощность излучения, Вт	КПД, %
1	Галогенная лампа	44,044	82
2	Голубой светодиод	0,095	79,2
3	Белый светодиод	0,084	70
4	ИК1-светодиод	0,05	65,2
5	ИК2-светодиод	0,072	90
6	ИК3-светодиод	0,05	71,4

3. *Расчет количества источников.*

Расчет количества источников искусственного излучения производится для того, чтобы оптимизировать спектр излучения разработанной комбинации из оптических элементов.

Для расчета количественного соотношения разных типов источников минимизируем выражение (6), характеризующее квадрат отклонения спектра имитатора от спектра солнечного излучения:

$$\sum_{m=0}^{M-1}\left[\left(\sum_{n=1}^{N}F_n(\lambda_m)P_{\text{изл}.n}B_n\right)-F_S(\lambda_m)\right]^2, \qquad (6)$$

где n – номер типа источника имитатора; N – количество типов источника имитатора (N = 6); m – номер точки на оси длин волн светового спектра; M – количество точек на оси длин волн светового спектра (M = 20); F_n – спектральная плотность n-го типа источника имитатора; F_S – спектральная плотность солнечного излучения; λ_m – точка на оси длин волн светового спектра, эти точки равномерно распределены на оси длин волн между $\lambda_{\min}$ и $\lambda_{\max}$, так что

$$\lambda_m=\lambda_{\min}+m(\lambda_{\max}-\lambda_{\min})/(M-1). \qquad (7)$$

$P_{\text{изл}.n}$ – мощность светового излучения одного n-го источника в направлении фотопанели; B_n – оптимизируемые относительные коэффициенты, характеризующие влияние количества однотипных источников.

Возьмём производные выражения (6) по B_n и приравняем их нулю:

$$2\sum_{m=0}^{M-1}\left[\left\{\left(\sum_{n=1}^{N}F_n(\lambda_m)P_{\text{изл}.n}B_n\right)-F_S(\lambda_m)\right\}\cdot F_n(\lambda_m)P_{\text{изл}.n}\right]=0. \qquad (8)$$

Приняв во внимание, что первый источник – галогеновая лампа – имеет подавляющую величину мощности излучения относительно других источников, рассчитаем количество этих источников (D), приходящихся на один галогеновый,

$$D_n=\frac{B_n}{B_1}, n=1...N \qquad (9)$$

и выберем ближайшие целые значения D_n.

Результаты приведены в табл. 2.

Для такого набора источников построен суммарный спектр. Этот спектр приведен на рис. 5.

Алгебраическая разница между превышением световой мощности солнечного и суммарного спектров должна компенсироваться недостачей на других участках спектра. На рис. 6 приведена разница между полученным спектром и солнечным, умноженная на спектр поглощения СБ. Максимальная ошибка составила 0,323.

Таблица 2

Количество источников

n	Источник искусственного излучения	Количество, шт
1	Галогенная лампа	1
2	Голубой светодиод	10
3	Белый светодиод	150
4	ИК1-светодиод	322
5	ИК2-светодиод	328
6	ИК3-светодиод	693

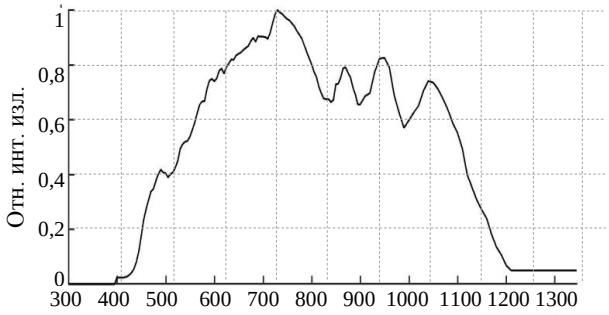

Рис. 5. Оптимизированный спектр

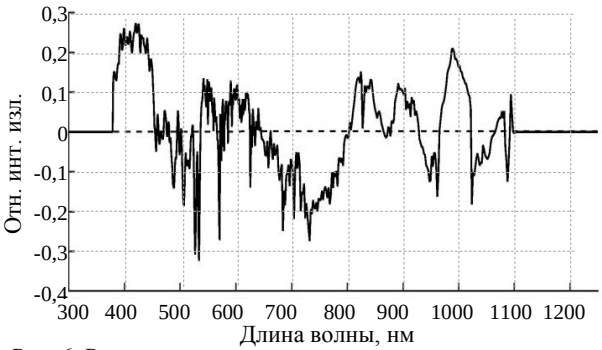

Рис. 6. Разница между полученным спектром и солнечным

4. *Определение суммарной мощности излучения.*

Общая мощность излучения разработанной концепции источников искусственного освещения, составила $P_{\text{изл.сум.}}$=132 Вт.

5. *Расчет плотности мощности выделяемого излучения.*

В ходе исследования основной упор был направлен не только на имитацию спектра солнечного излучения в лабораторных условиях, но и на получение мощности излучения, равной 10 Вт/дм^2. Представленная комбинация световых элементов может быть компактно размещена на площади 1,32 дм^2, таким образом обеспечивая требуемую плотность излучения с поверхности мощностью 13,2 Вт/дм^2, т.е. поставленная задача была выполнена.

Результаты оценки стоимости разработанного имитатора солнечного излучения приведены в табл. 3.

Таблица 3

Стоимость источников искусственного освещения

n	Источник	Количество, шт.	Цена за один элемент, руб.	Общая стоимость, руб.
1	Галогенная лампа	1	44	44
2	Голубой светодиод	10	6	60
3	Белый светодиод	150	49	7350
4	ИК1-светодиод	322	16	5152
5	ИК2-светодиод	328	11	3608
	ИК3-светодиод	693	95	65835
Итого:				82049

6. *Определение количества имитаторов.*

Так как $P_{\text{изл.сум}} = 132$ Вт, оценим количество модулей на требуемую площадь источника излучения.

$$N_{\text{мод}} = \frac{1000}{132} \cdot S, \qquad (10)$$

где S – площадь источника излучения в м^2.

Выводы и заключения

Создана и описана методика расчета источника искусственного освещения для различных спектров излучения и для разного набора искусственных осветительных приборов и (в общем случае) для произвольного спектра поглощения солнечной батареи, с высокой точностью воспроизводящего спектр солнечного излучения, установленный международным стандартом ISO 9845-1, в диапазоне длин волн в зоне поглощения солнечной батареи. Проведен расчет по этой методике и разработан модуль источника искусственного освещения (имитатор), обеспечивающий воспроизведение солнечного спектра.

Полученный спектр излучения значительно лучше приближен к спектру естественного солнечного излучения по сравнению с имитатором, рассмотренным в статье [10], но имеет в своем составе 1 504 источника, что более чем в два раза больше, чем в [10], где использовано 655 источников.

В отличие от имитаторов, исследуемых в статье [9], разработанный имитатор не требует дополнительных конструктивных элементов, таких как зеркала и отражатели.

Предложенная методика может быть использована в том числе для перспективных солнечных панелей, отличающихся от современных устройств по спектру поглощения (например, в ультрафиолетовой зоне), а также при появлении новых, более эффективных (по КПД, излучаемой мощности, форме спектра излучения, по конструктивным особенностям) источников света.

Литература

1. Maximum power point tracking methods for the solar batter / I.A. Belova, M.V. Martinovich, V.A. Skolota, I.V. Zaev // International Conference of Young Specialists on Micro / Nanotechnologies and Electron Devices. – 2018. – P. 445–451.

2. Application of photovoltaic cells with an intelligent control system for railway transport / I.A. Belova, M.V. Martinovich, V.A. Skolota // 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). – 2016. – Vol. 03. – P. 64–68.

3. Гришанов В.Н. Классификация и рациональное проектирование солнечных имитаторов // Компьютерная оптика. – М.: МЦНТИ, 1995. – Вып. 14-15, ч. 2. – С. 46–52.

4. Имитаторы солнечного излучения для термовакуумных испытаний космического аппарата / Р.О. Асланян, Д.И. Анисимов, И.А. Марченко, В.И. Пантелеев // Сибирский журнал науки и технологии. – 2017. – Т. 18, № 2. – С. 323–327.

5. Ларионов В.Р. Измерительные комплексы для исследований солнечных фотоэлектрических преобразователей каскадного типа и концентраторных модулей на их основе // Журнал технической физики. Физико-техн. ин-т им. А.Ф. Иоффе. – 2015. – Т. 85, № 6. – С. 104–110.

6. Мейтин М. Фотовольтаика: материалы, технологии, перспективы. Пусть всегда будет Солнце // Электроника-НТБ. – 2000. – № 6. – С. 40–47.

7. Солнечная энергетика: учеб. пособие для вузов / В.И. Виссарионов, Н.К. Малинин, Г.В. Дерюгина, В.А. Кузнецова. – М.: Изд. дом МЭИ, 2008. – 317 с.

8. ISO 9845-1:1992, ISO [Электронный ресурс]. – Режим доступа: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/01/77/17723.html, свободный (дата обращения: 12.12.2019).

9. Колинчук А.В. Имитаторы солнечного излучения для испытаний фотоэлектрических батарей космического назначения // Авиационно-космическая техника и технология. – 2015. – № 3. – С. 73–79.

10. Моделирование спектра солнечного излучения с помощью светодиодов / В.А. Афонин, О.Ю. Коваленко, Е.Д. Гусева, Ю.А. Пильщикова // Фотоника. – 2016. – Вып. 2. – С. 72–77.

11. Поглощательная способность полупроводников, используемых в производстве солнечных панелей / Л.А. Косяченко, Е.В. Грушко // Физика и техника полупроводников. – 2012. – Вып. 4. – С. 482–486.

12. Зависимость коэффициента поглощения кристаллического германия в ИК области спектра от удельного сопротивления / И.М. Несмелова, Н.И. Астафьев, Е.А. Несмелов // Оптический журнал. – 2007. – Т. 74, № 1. – С. 88–92.

13. Оптические свойства монокристаллического кремния в области спектра 3–5 мкм / И.М. Несмелова, Н.И. Астафьев, Н.А. Кулакова // Оптический журнал. – 2012. – Т. 79, № 3. – С. 87–90.

14. Гончаров А.Д. Универсальный метод расчета коэффициента использования светового потока осветительных приборов / А.Д. Гончаров, В.И. Туев // Доклады ТУСУР. – 2017. – Т. 20, № 2. – С. 55–60.

15. Якушенков Ю.Г. Теория и расчёт оптико-электронных приборов. – М.: Логос, 2014. – 568 с.

Белова Ирина Анатольевна
Ассистент каф. электроники и электротехники (ЭЭ)
Новосибирского гос. технического университета (НГТУ)
Карла Маркса пр-т, 20, г. Новосибирск, Россия, 630073
Тел.: +7-923-258-44-93
Эл. почта: ira.belowa@gmail.com

Мартинович Мирослав Владимирович
Канд. техн. наук, доцент каф. ЭЭ НГТУ
Карла Маркса пр-т, 20, г. Новосибирск, Россия, 630073
Тел.: +7-913-892-98-48
Эл. почта: martinovich_m@mail.ru

Федорова Дарья Юрьевна
Магистр каф. ЭЭ НГТУ
Карла Маркса пр-т, 20, г. Новосибирск, Россия, 630073
Тел.: +7-913-208-24-89
Эл. почта: careglazaia@mail.ru

Belova I.A, Martinovich M.V., Fedorova D.Y.
Artificial light source simulating the solar spectrum for testing solar panels

This work is devoted to the development of a combined source of artificial lighting to study the characteristics of solar cells. Spectral analysis of various radiation sources is performed. Based on the analysis, the necessary radiation sources are selected, which total spectrum, after approximation, is close to the spectrum of solar radiation. The calculation of electro-optical characteristics is carried out. The number of artificial lighting sources needed to reproduce the spectrum of solar radiation is calculated. The corresponding conclusions are made.
Keywords: solar spectrum, imitation of solar radiation, solar panels.
DOI: 10.21293/1818-0442-2021-24-4-19-24

References

1. Belova I.A., Martinovich M.V., Skolota V.A., Zaev I.V. Maximum power point tracking methods for the solar battery. *International Conference of Young Specialists on Micro / Nanotechnologies and Electron Devices*, 2018, pp. 445–451.

2. Belova I.A., Martinovich M.V., Skolota V.A. Application of photovoltaic cells with an intelligent control system for railway transport. *13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering*, 2016, vol. 03, pp. 64–68.

3. Grishanov V.N. [Classification and rational design of solar simulators]. *Computer optics*, 1995, pp. 46–52 (in Russ.).

4. Aslanyan R.O., Anisimov D.I., Marchenko I.A., Panteleev V.I. [Simulators of solar radiation for thermal vacuum tests of a spacecraft]. *Siberian Journal of Science and Technology*, 2017, vol. 18, no. 2, pp. 323–327 (in Russ.).

5. Larionov V.R. [Measuring complexes for research of cascade-type solar photovoltaic converters and concentrator modules based on them]. *Journal of Technical Physics, Physico-Technical Institute named after A.F. Ioffe*, 2015, vol. 85, no.6, pp. 104–110 (in Russ.).

6. Meitin M. [Photovoltaics: materials, technologies, prospects. May there always be sun]. *Electronics-NTB*, 2000, no. 6, pp. 40–47 (in Russ.).

7. Vissarionov V.I., Malinin N.K., Deryugina G.V., Kuznetsova V.A. [Solar energy]. Textbook for universities. Moscow: Publishing House MEI, 2008, 317 c. (in Russ.).

8. ISO 9845-1:1992, ISO. [Online]. Available at: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/01/77/17723.html, free (Accessed: December 12, 2019).

9. Kolinchuk A.V. [Solar simulators for testing space photovoltaic batteries]. *Aerospace Engineering and Technology*, 2015, no. 3, pp. 73–79 (in Russ.).

10. Afonin V.A., Kovalenko O.Yu., Guseva E.D., Pil'shchikova Yu.A. [Modeling the solar spectrum using LEDs]. *Photonics*, 2016, no. 2, pp. 72–77 (in Russ.).

11. Kosyachenko L.A., Grushko E.V. [Absorption capacity of semiconductors used in the manufacture of solar panels]. *Semiconductor Physics and Technology*, 2012, vol. 4, pp. 482–486 (in Russ.).

12. Nesmelova I.M., Astafiev N.I., Nesmelov E.A. [The dependence of the absorption coefficient of crystalline germanium in the IR spectral region of the resistivity]. *Optical Magazine*, 2007, vol. 74, no. 1, pp. 88–92 (in Russ.).

13. Nesmelova I.M., Astafiev N.I., Kulakova N.A. [Optical properties of monocrystalline silicon in the spectral range 3–5 μm]. *Optical Magazine*, 2012, vol. 79, no. 3, pp. 87–90. (in Russ.).

14. Goncharov A.D. [A universal method for calculating the coefficient of using the light flux of lighting devices]. *TUSUR reports*, 2017, vol. 20, no. 2, pp. 55–60 (in Russ.).

15. Yakushenkov Yu.G. [Theory and calculation of optoelectronic devices]. M.: Logos, 2014, 568 p. (in Russ.).

Irina A. Belova
Assistant to the Department Electronics and Electrical Engineering (EE) Novosibirsk State Technical University (NSTU)
20, Karl Marx pr., Novosibirsk, Russia, 630073
Phone: +7-923-258-44-93
Email: ira.belowa@gmail.com

Miroslav V. Martinovich
Candidate of Science in Engineering,
Associate Professor EE NSTU
20, Karl Marx pr., Novosibirsk, Russia, 630073
Phone: +7-913-892-98-48
Email: martinovich_m@mail.ru

Daria Y. Fedorova
Master student, Department of EE NSTU
20, Karl Marx pr., Novosibirsk, Russia, 630073
Phone: +7-913-208-24-89
Email: careglazaia@mail.ru

УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

УДК 681.322.067

А.В. Павлычев, К.С. Солдатов, В.А. Сказин

Выявление сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения

Разработан алгоритм поиска и выявления сетевых аномалий в системных журналах операционной системы Microsoft Windows с применением методов машинного обучения. Проведены предобработка, кластеризация и визуализация исследуемых данных. Предложенный алгоритм подтвердил свою эффективность, выявив в исследуемом наборе данных события, являющиеся признаками работы вредоносного программного обеспечения.
Ключевые слова: аудит безопасности, системные журналы Windows, машинное обучение, кластеризация, сетевые аномалии.
DOI: 10.21293/1818-0442-2021-24-4-27-32

В современном цифровом мире на передний план выходят задачи обеспечения целостности, доступности и конфиденциальности информации, обрабатываемой в государственных и иных информационных системах.

Согласно отчетам крупнейших аналитических центров, одной из наиболее заметных в 2020 и 2021 гг. угроз в области кибербезопасности является использование так называемых вирусов-шифровальщиков (Ransomware) [1, 2]. Деятельность различных хакерских группировок направлена на получение несанкционированного сетевого доступа в целевую информационную инфраструктуру с целью похищения информации ограниченного распространения с дальнейшим шифрованием пользовательских данных и требованием финансового выкупа как за расшифровку данных, так и за нераспространение конфиденциальной информации [3].

Ввиду изменения ландшафта киберугроз изменяются и подходы к обеспечению информационной безопасности. Сегодня основная цель организации состоит в правильной оценке киберрисков, а также разработке системы адекватных мер реагирования [4, 5].

Выявление сетевых аномалий представляет собой важную задачу в рамках построения превентивной системы обеспечения информационной безопасности и эффективного противодействия несанкционированному доступу. Особенно данная задача актуальна для объектов критической информационной инфраструктуры [6].

Одним из способов выявления сетевых аномалий является исследование файлов журналов различных информационных систем, в том числе системных журналов операционной системы [7].

В настоящий момент Windows – самая популярная операционная система в мире. По данным аналитического агентства StatCounter по состоянию на сентябрь 2021 г., данная операционная система установлена на 76,13% всех компьютеров, в России данный показатель составляет 78,34%. Если рассматривать конкретные версии операционной системы Windows, по состоянию на август 2021 г. самой популярной в мире версией является Windows 10 (78,34%), за ней следуют Windows 7 (15,98%), Windows 8.1 (3,62%), Windows 8 (1,15%). В России места распределены следующим образом: Windows 10 (75,79%), Windows 7 (16,74%), Windows 8.1 (3,79%), Windows 8 (2,29%) [8].

В операционной системе Windows ведутся журналы, которые регистрируют пользовательские события и работу системных и прикладных программ на компьютере.

Журналы событий Windows содержат ряд дескрипторов, позволяющих объединять события в такие категории, как «информационные» и «критические». Отдельные идентификаторы указывают на конкретные типы событий, а последние версии Windows имеют отдельные файлы журналов событий для различных приложений и служб [9].

Несмотря на имеющиеся во встроенном приложении для работы с журналами варианты фильтрации, специалисту по информационной безопасности зачастую сложно найти интересующее его событие среди большого объема хранимых данных. Особенно задача усложняется при необходимости расследования компьютерного инцидента, в ходе которого требуется изучить большое количество взаимосвязанных событий, которые могут находиться в разных журналах [10].

Журнал событий представляет собой бинарный файл специального формата (с расширением EVTX), схожий с файлом базы данных. Журнал включает в себя следующие данные:

1. Уровень. Указывает, к какому типу относится событие:

1.1. Предупреждение – некритичное событие, которое указывает на возможность возникновения более серьезных ошибок в будущем. Предупреждением считается восстановление приложения без утраты данных или потери функциональности.

1.2. Ошибка – событие, которое указывает на значительную проблему, например на потерю функциональности или утрату данных.

1.3. Сведения – события, которые описывают успешную работу службы, драйвера или приложения. Например, целесообразно создать информационное событие в случае успешной загрузки сетевого драйвера.

1.4. Аудит успеха – событие, которое фиксирует проверенную успешную попытку доступа к функционалу безопасности. К таким событиям можно отнести успешную попытку пользователя войти в систему.

1.5. Аудит отказа – событие, которое фиксирует проверенную неудачную попытку доступа к функционалу безопасности. Например, событие будет создано, если пользователь попытается получить доступ к диску, который не будет предоставлен.

2. Дата и время регистрации события.

3. Источник события – это имя программного обеспечения, которое регистрирует событие. Часто это имя приложения или имя подкомпонента приложения, если оно большое.

4. Категории. Помогают объединять события, чтобы программа просмотра событий могла их фильтровать. Каждый источник событий может определять свои собственные пронумерованные категории и текстовые строки, в которые они отображаются. Категории должны быть пронумерованы последовательно, начиная с номера 1. Могут храниться в отдельном файле сообщений или в файле, который содержит сообщения других типов.

5. Идентификаторы событий. Однозначно идентифицируют конкретное событие. Каждый источник событий может определять свои собственные пронумерованные события и строки описания, с которыми они отображаются в своем файле сообщений.

6. Пользователь. Содержит имя пользователя, от которого выполнялись процессы. Многие события связаны с конкретными пользователями, имена которых указаны в данном поле.

7. Компьютер. Указывает имя компьютера, на котором произошла регистрация события.

Аудит безопасности является инструментом, который необходимо использовать для поддержания целостности системы. Базовая политика аудита определяет категории связанных с безопасностью событий, указанные для проверки. Когда Windows впервые устанавливается, все категории аудита отключены. Включая различные категории событий аудита, появляется возможность реализовать политику аудита, которая соответствует установленным требованиям безопасности.

Журнал безопасности записывает каждое событие в соответствии с политиками аудита, которые устанавливаются для каждого объекта. В аудит могут быть добавлены следующие категории событий:

1) аудит событий входа;
2) аудит доступа к объектам;
3) аудит отслеживания процессов;
4) аудит доступа к службе каталогов;
5) аудит событий входа в аккаунт;
6) аудит управления учетными записями;
7) изменение политики аудита;
8) использование привилегий аудита;
9) аудит системных событий.

Методология поиска аномалий в системных журналах

Алгоритм выявления аномалий состоит из пяти основных этапов: сбор файлов системных журналов, предварительная обработка данных, снижение размерности и визуализация, кластеризация данных и поиск аномалий.

Сбор файлов системных журналов: стандартное приложение «Просмотр событий» позволяет выгружать события в формате *.csv. На первом этапе производится выгрузка содержимого системного журнала Security (журнал безопасности) в csv-файл. Данный журнал содержит события, относящиеся к безопасности компьютера, например, вход/выход пользователя, доступ к объектам, изменение политик и т.д.

Предварительная обработка данных: выгружаемый csv-файл зачастую содержит данные в плохо структурированной форме и представленные в некорректном формате. Цель предварительной обработки – удаление событий или признаков, в дальнейшем не используемых в алгоритме. Также на этом этапе производится приведение данных к однообразному виду для лучшей кластеризации.

Снижение размерности и визуализация: алгоритмы снижения размерности широко применяются в визуализации данных в пространстве большой размерности. Визуализация данных критически важна для понимания и интерпретации структуры больших наборов данных [11]. Наиболее популярным алгоритмом на сегодняшний день является алгоритм t-SNE.

t-SNE представляет собой итерационный алгоритм визуализации многомерных данных путем сопоставления точек данных в двух- или трехмерном пространстве. Он создает единую карту, которая показывает внутренние структуры в многомерном наборе данных, включая тенденции, закономерности и выбросы, с помощью метода нелинейного уменьшения размеров [12]. Рассмотрим математическую модель алгоритма.

Если дан набор из N объектов высокой размерности x_i, …, x_j, то для набора объектов вычисляются вероятности $P(i|j)$, которые пропорциональны похожести объектов x_i и x_j:

$$P_{i|j} = \frac{\exp\left(\frac{-\left|x_i - x_j\right|^2}{2\sigma_i^2}\right)}{\sum_{k \neq j}^{n} \exp\left(\frac{-\left|x_i - x_k\right|^2}{2\sigma_i^2}\right)}, \quad (1)$$

σ_i – дисперсия в точке данных x_i, x_j в качестве соседа выбирает x_j, основываясь на пропорции его гауссовой плотности вероятности с центром в точке x_i:

$$P_{ij} = \frac{P_{j|i} + P_{i|j}}{2n}. \quad (2)$$

Для близлежащих точек $P(i|j)$ плотность будет высокой, а для точек, расположенных далеко друг от друга, $P(i|j)$ будет незначительной. Плотность распределения вероятности двух точек прямо пропорциональна сходству этих точек.

На следующем шаге работы алгоритм стремится получить отображение $y_1, \ldots, y_n$ в d-мерное пространство, которое отражает, насколько это возможно, похожести $P(i|j)$. Для этого алгоритм измеряет похожесть $q(i|j)$ между двумя точками y_i и y_j:

$$q_{ij} = \frac{\left(1+\left\|y_i - y_j\right\|^2\right)^{-1}}{\sum_{k\neq 1}\left(1+\left\|y_k - y_i\right\|^2\right)^{-1}}. \quad (3)$$

Затем для того, чтобы непохожие объекты расположить далеко друг от друга, происходит измерение похожести между точками в пространстве низкой размерности.

Расположение точек y_i в пространстве малой размерности определяется минимизацией расстояния Кульбака–Лейблера распределения Q от распределения P, т.е.

$$KL\left(P\|Q\right) = \sum_{(i\neq j)} P_{ij} \log \frac{p_{ij}}{q_{ij}}. \quad (4)$$

Минимизация расстояния Кульбака–Лейблера к точкам y_i осуществляется с помощью градиентного спуска. Результатом оптимизации является отображение, которое отражает похожесть между объектами пространства высокой размерности.

Также необходимо использовать кластеризацию, т.е. решить задачу разделения всех данных на группы (кластеры) таким образом, чтобы объекты с разных групп отличались друг от друга, а объекты в одной группе были «похожи» друг на друга [13, 14]. В данной работе рассматривается метод DBSCAN. Данный алгоритм имеет ряд преимуществ:

- не требует спецификации числа кластеров;
- умеет находить кластеры произвольной формы;
- имеет понятия шума и устойчивости к выбросам;
- требует всего два параметра и нечувствителен к порядку точек в базе данных.

Рассмотрим математическую модель данного алгоритма.

Для множества объектов X задана метрическая функция расстояния ρ, minOb_j – минимальное количество соседних объектов, необходимых для образования одного кластера, а ε – максимальное расстояние между соседними объектами.

Объект $p \in X$ будет являться кластерным, если в ε-окрестности точки p находятся minOb_j объектов (включая сам объект p). Такие объекты называются прямо достижимыми из p. Объект $q \in X$ называется достижимым из p, если существует такой путь $p_1, \ldots, p_n$, где $p_1 = p$ и $p_n = q$, а каждый объект $p_i + 1$ достижим из p_i. Отсюда следует, что все объекты в пути, кроме объекта q, должны быть кластерными. Все объекты, которые не достижимы ни из одного другого объекта, считаются выбросами (шумом). Соответственно, кластером является множество кластерных объектов, достижимых друг из друга, а также граничные объекты, которые достижимы из любой другой точки кластера [15].

Расстояние ρ между двумя объектами кластеризуемого множества вычисляется с использованием метрики Евклида:

$$Q(p,q) = \sqrt{(p_1-q_1)^2 + (p_2-q_2)^2 + \ldots (p_n-q_n)^2} = \\ = \sqrt{\sum_{k=1}^{n}(p_k-q_k)^2}. \quad (5)$$

В данной работе в качестве аномалий считаются данные, находящиеся в кластере «–1». В данный кластер заносятся данные, которые алгоритм считает выбросами (шумом).

Результаты

На первом этапе с тестового компьютера осуществлена выгрузка файла журнала «Security.evtx». Содержимое журнала импортировано в csv-файл для дальнейшей обработки. Выбор компьютера обусловлен зафиксированной на нем вредоносной активностью в течение продолжительного периода времени.

На втором этапе в ходе предобработки в итоговый набор данных выбраны следующие поля:

«TimeWritten» – время создания события;

«EventID» – идентификатор события;

«EventType» – идентификатор типа события;

«EventCategory» – идентификатор категории события.

На третьем этапе применяем алгоритм визуализации и снижения размерности итогового набора данных t-SNE (рис. 1).

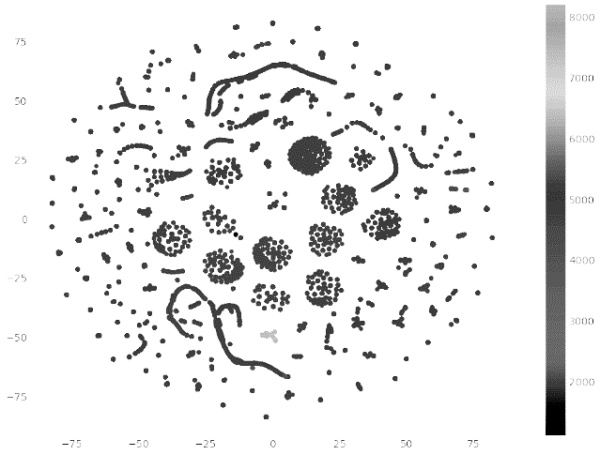

Рис. 1. Результат применения алгоритма t-SNE

На четвертом этапе итоговый набор данных кластеризован с помощью алгоритма DBSCAN. Коэффициент максимального расстояния между соседними объектами и коэффициент минимального количества соседних объектов, необходимых для образования кластера, определялись путем перебора.

На рис. 2 звездочками выделены аномальные выбросы нашего набора данных.

Последним этапом с помощью ранее описанного метода кластеризации выявляются выбросы (шумы). Результатом работы кластеризации является

csv-файл, содержащий информацию об аномальном событии: идентификатор события и время его возникновения. Для выявления вредоносной активности необходимо в исходном файле журнала событий найти выявленное «аномальное» событие и проверить соседние события, предшествующие или наступившие после возникновения «аномального» события.

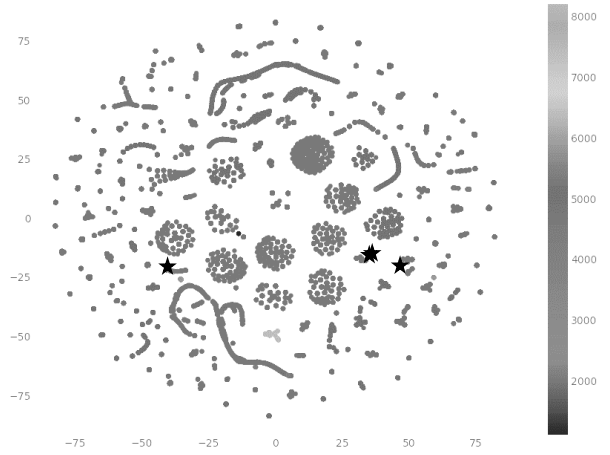

Рис. 2. Результат кластеризации DBSCAN

В результате работы алгоритм выделил в качестве аномалий следующие события (EventID):

4624: пользователь успешно вошел в систему. Может быть признаком несанкционированных действий при выполнении дополнительных условий, например вход в систему во внерабочее время;

4672: особые привилегии, назначенные новому входу в систему. Событие генерируется для входа в новую учетную запись, если для нового сеанса входа в систему назначены какие-либо особые привилегии;

4657: изменено значение реестра. Является одним из ключевых событий в системе, поскольку целью большинства вредоносных программ – является модификация пользовательских или системных данных;

4663: попытка доступа к объекту. Может иметь важное значение при копировании «тела» вируса или создании скрипта для последующего исполнения.

При проверке исходных файлов журналов выявлено, что события 4624 и 4672 следуют друг за другом. Событие 4624 (пользователь успешно вошел в систему) зафиксировало использование NTLM пакета аутентификации и тип входа – 3 (пользователь или компьютер вошел на этот компьютер из сети). Отличие легитимного соединения NTLM – использование пароля. Следовательно, в случае, если данный вход осуществлялся пользователем, события в журнале должны быть следующие:

4768: запрошен билет проверки подлинности Kerberos (TGT);

4769: запрошен билет службы Kerberos (TGS);

4648: попытка входа в систему с использованием явных учетных данных;

4624: учетная запись была успешно авторизована.

В исходном файле журнала после события 4624 зафиксировано событие 4672 (особые привилегии, назначенные новому входу в систему), что может свидетельствовать об успешно проведенной атаке типа pass-the-hash. Данная атака направлена на обход механизма авторизации по протоколу NTLM.

События 4663 и 4657 фиксируются через короткий промежуток времени и также следуют друг за другом. Событие 4663 (попытка доступа к объекту) фиксирует создание файла «mmkt.exe» в директории «%System Root%\Users\All Users», а событие 4657 (изменено значение реестра) – добавление ранее созданного исполняемого файла в ключе автозапуска системного реестра ([HKCU\Software\Microsoft\Windows\CurrentVersion\Run]).

Использование техники pass-the-hash с дальнейшим закреплением на атакуемой машине может являться индикацией заражения устройства.

Дальнейшая проверка данного устройства антивирусом выявила ВПО, классифицируемое как «Trojan.Win32.MIMIKATZ.AEG».

В результате описанной процедуры было обработано 4 000 событий (N). Каждое из событий было отдельно изучено и промаркировано. При применении рассмотренного алгоритма неправильно были отнесены к аномальным 22 события (FP), неправильно были распознаны в качестве неаномальных 4 события (FN).

Проведем расчет точности (6), уровня ошибок первого рода (7) и уровня ошибок второго рода (8):

$$Acc = \left(1 - \frac{FN + FP}{N}\right) \times 100\%, \quad (6)$$

$$P_1 = \frac{FP}{N}, \quad (7)$$

$$P_2 = \frac{FN}{N}. \quad (8)$$

В результате расчетов получим следующие значения: точность – 99,35%, уровень ошибок первого рода – $5{,}5 \cdot 10^{-3}$, уровень ошибок второго рода – 10^{-3}.

Заключение

В ходе исследования был разработан способ выявления сетевых аномалий в системных журналах операционной системы Microsoft Windows с использованием методов машинного обучения. Предложенный алгоритм подтвердил свою эффективность, выявив в исследуемом наборе данных события, являющиеся признаками работы вредоносного программного обеспечения.

Литература

1. Solar JSOC Security Report. Итоги 2020 года [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/ upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf, свободный (дата обращения: 02.12.2021).

2. Kaspersky Security Bulletin. Обзор активности APT-групп в 2020 году [Электронный ресурс]. – Режим доступа: https://securelist.ru/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99480, свободный (дата обращения: 02.12.2021).

3. Xin L. Awareness Education as the Key to Ransomware Prevention / L. Xin, Q. Liao // Information Systems Security. – 2012. – Vol. 16, No. 4. – P. 195–202.

4. Signature-less ransomware detection and mitigation / Y.S. Joshi, H. Mahajan, S.N. Joshi et al. // J. Comput Virol Hack Tech. – 2021. – No. 17. – P. 299–306.

5. Zavarsky P. Experimental analysis of ransomware on windows and android platforms: evolution and characterization / P. Zavarsky, D. Lindskog // Procedia Comput. Sci. – 2016. – Vol. 94. – P. 465–472.

6. Кибербезопасность 2020–2021. Тренды и прогнозы [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2020-2021/, свободный (дата обращения: 02.12.2021).

7. Berlin K., Slater D., Saxe J. Malicious Behavior Detection using Windows Audit Logs // In Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. Association for Computing Machinery, New York, NY, USA, 2015. – https://arxiv.org/pdf/1506.04200.pdf

8. Развитие информационных угроз во втором квартале 2021 года. Статистика по ПК [Электронный ресурс]. – Режим доступа: https://securelist.ru/it-threat-evolution-in-q2-2021-pc-statistics/103374/, свободный (дата обращения: 02.12.2021).

9. CIS Microsoft Windows Desktop Benchmarks: Securing Microsoft Windows Desktop an objective, consensus-driven security guideline for the Microsoft Windows Desktop Operating Systems [Электронный ресурс]. – Режим доступа: https://www.cisecurity.org/benchmark/microsoft_windows_desktop/, свободный (дата обращения: 02.12.2021).

10. Ring M., Schlör D., Wunderlich S., Landes D., Hotho A. Malware detection on windows audit logs using LSTMs // Computers&Security. – 2021. – Vol. 109. – P. 1–12.

11. Thomas T. Machine learning approaches in cyber security analytics / T. Thomas, A.P. Vijayaraghavan, S. Emmanuel. – Singapore: Springer, 2020. – 217 p.

12. Aldahoul N. Model fusion of deep neural networks for anomaly detection / N. Aldahoul, H.A. Karim, A. Wazir // J. of Big Data. – 2021. – No. 8. – P. 106.

13. Patcha A. An overview of anomaly detection techniques: Existing solutions and latest technological trends / A. Patcha, Jung-Min Park // Computer Networks. – 2007. – Vol. 51, Iss. – 12. – P. 3448–3470.

14. Kwon D., Kim H., Kim J. et al. A survey of deep learning-based network anomaly detection // Cluster Comput. – 2019. – No. 22. – P. 949–961.

15. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning / Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS-17). – 2017. – DOI 10.1145/3133956.3134015

Павлычев Алексей Викторович
Директор Центра информационной безопасности
Дальневосточного федерального ун-та (ДВФУ)
Аякс п., 10, о. Русский, г. Владивосток, Россия, 690922
Тел.: +7-994-000-04-40
Эл. почта: pavlychev.av@dvfu.ru

Солдатов Константин Сергеевич
Канд. физ.-мат. наук, доцент
Департамента информационной безопасности ДВФУ
Аякс п., 10, о. Русский, г. Владивосток, Россия, 690922
Тел.: +7-914-686-53-11
Эл. почта: soldatov_ks@dvfu.ru

Сказин Виктор Андреевич
Вед. специалист Центра информационной безопасности ДВФУ
Аякс п., 10, о. Русский, г. Владивосток, Россия, 690922
Тел.: +7-968-142-59-50
Эл. почта: skazin_va@dvfu.ru

Pavlychev A.V., Soldatov K.S., Skazin V.A.

Network anomaly detection in the Microsoft Windows system logs using machine learning methods

An algorithm for network anomaly detection in the system security logs of the Microsoft Windows operating system with using machine learning methods was developed. Preprocessing, clustering, and visualization of the studied data were carried out. The proposed algorithm has confirmed its efficiency by identifying events in the studied dataset that indicate the operation of a malicious software.

Keywords: cybersecurity audit, Windows system journals, machine learning, clusterization, network anomaly.
DOI: 10.21293/1818-0442-2021-24-4-27-32

References

1. Solar JSOC Security Report. Results of 2020. Available at: https://rt-solar.ru/upload/iblock/7d1/Solar-JSOC-Security-Report_2020_rgb.pdf, free (Accessed: December 02, 2021).

2. Kaspersky Security Bulletin [Overview of APT Group Activity in 2020]. Available at: https://securelist.ru/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99480, free (Accessed: December 02, 2021) (in Russ.).

3. Xin Luo, Qinyu Liao. Awareness Education as the Key to Ransomware Prevention. *Information Systems Security*, 2012, vol. 16, no. 4, pp. 195–202.

4. Joshi Y.S., Mahajan H., Joshi S.N. et al. Signature-less ransomware detection and mitigation. *Journal of Computer Virology and Hacking Techniques*, 2021, no. 17, pp. 299–306.

5. Zavarsky P., Lindskog D. et al. Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, 2016, vol. 94, pp. 465–472.

6. [Cybersecurity 2020-2021. Trends and Forecasts]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2020-2021, free (Accessed: December 02, 2021) (in Russ.).

7. Berlin K., Slater D., Saxe J. Malicious Behavior Detection using Windows Audit Logs. *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. Association for Computing Machinery*, New York, NY, USA (2015). https://arxiv.org/pdf/1506.04200.pdf

8. [Development of information threats in the second quarter of 2021. PC statistics]. Available at: https://securelist.ru/it-threat-evolution-in-q2-2021-pc-statistics/103374/, free (Accessed: December 02, 2021) (in Russ.).

9. CIS Microsoft Windows Desktop Benchmarks: Securing Microsoft Windows Desktop An objective, consensus-driven security guideline for the Microsoft Windows Desktop Operating Systems. Available at: https://www.cisecurity.org/benchmark/microsoft_windows_desktop/, free (Accessed: December 02, 2021).

10. Ring M., Schlör D., Wunderlich S., Landes D., Hotho A. Malware detection on windows audit logs using LSTMs. *Computers & Security*, 2021, vol. 109, pp. 1–12.

11. Thomas T., Vijayaraghavan A.P., Emmanuel S. *Machine Learning Approaches in Cyber Security Analytics*. Singapore: Springer, 2020, 217 p.

12. Aldahoul N., Karim H.A., Wazir A. Model fusion of deep neural networks for anomaly detection. *Journal of Big Data*, 2021, no. 8, pp. 106.

13. Animesh P., Jung-Min P. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 2007, vol. 51, iss. 12. P. 3448–3470.

14. Kwon D., Kim H., Kim J., Suh S.C., Kim I., Kim K.J. A survey of deep learning-based network anomaly detection. *Cluster Computing*, 2019, 22(1), P. 949–961.

15. Du Min, Li Feifei, Zheng Guineng, Srikumar Vivek. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (*CCS-17*), 2017. DOI 10.1145/3133956.3134015

Aleksey V. Pavlychev
Director, Cybersecurity Center,
Far Eastern Federal University (FEFU)
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
Phone: +7-994-000-04-40
Email: pavlychev.av@dvfu.ru

Konstantin S. Soldatov
Candidate of Science in Physics and Mathematics,
Department of Information Security FEFU
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
Phone: +7-914-686-53-11
Email: soldatov_ks@dvfu.ru

Viktor A. Skazin
Leading expert, Cybersecurity Center FEFU
10, Ajax Bay, Russky Island, Vladivostok, Russia, 690922
Phone: +7-968-142-59-50
Email: skazin_va@dvfu.ru

УДК 004.056.5

А.Е. Жиляев

Классификация схем выработки и распределения ключей в сетях квантового распределения ключей произвольной топологии

Квантовые ключи, создаваемые в результате выполнения протокола квантового распределения ключей, обладают абсолютной стойкостью в силу физических законов и не подвержены взлому даже при неограниченных вычислительных мощностях атакующего. Однако системы квантового распределения ключей имеют ограниченную дальность. Для преодоления проблемы максимальной дальности возможно построение сетей квантового распределения ключей на основе доверенных промежуточных узлов. В работе рассматривается связь магистральных сетей с сетями произвольной топологии, вводятся критерии классификации схем выработки и распределения ключей и проводится классификация некоторых схем по введенным критериям.

Ключевые слова: квантовое распределение ключей, сети КРК, классификация, квантовый ключ, квантовый маршрут.

DOI: 10.21293/1818-0442-2021-24-4-33-39

Развитие новых и совершенствование опробованных методов защиты информации связаны в первую очередь с ростом киберпреступлений в информационной сфере и расширением спектра угроз и рисков при атаках на информационные ресурсы. Это предопределят создание новых подходов к обеспечению информационной безопасности [1–5]. Перспективным подходом повышения уровня защищенности информации является применение и развитие систем квантового распределения ключей (КРК), которые позволяют создавать идентичные секретные ключи у двух географически разнесенных абонентов. Причем скорость создания таких ключей пусть и уступает скорости известных асимметричных алгоритмов, например схемы Диффи–Хелмана, но остается достаточно высокой для частой смены секретных ключей в средствах криптографической защиты информации (СКЗИ). Системы КРК могут использоваться в качестве замены доверенной доставки большого объема ключей курьером, т.е. исключается человеческий фактор из процесса распределения ключей [6].

Однако известны практические ограничения систем КРК, а именно предельная удаленность двух абонентов друг от друга, т.е. длина квантового канала, соединяющего абонентов [7]. Важно учитывать, что квантовый канал не может содержать активных оптических и электрооптических компонентов, в том числе усилителей сигнала, так как подобные элементы необратимо разрушают передаваемые квантовые состояния [8].

Известным и реализуемым с учетом настоящего уровня развития техники решением проблемы максимальной дальности в системах КРК является создание сетей КРК на основе доверенных промежуточных узлов (ДПУ). Концепция передачи квантового ключа по цепочке узлов, соединенных квантовыми каналами, была предложена в работах [9, 10]. Существенным недостатком такого подхода является требование доверия к промежуточным узлам, так как передаваемый ключ в открытом виде появляется на каждом ДПУ.

В настоящей работе покажем свойства возможных схем выработки и распределения ключей и предложим подход к классификации схем в зависимости от их параметров. Также покажем место известных схем выработки ключей согласно приведенной классификации и связь некоторых критериев классификации со свойствами безопасности, присущими этим схемам.

Связь сети произвольной топологии и магистральной сети

Задача создания общего ключа между двумя произвольными узлами сети КРК произвольной топологии в общем случае достаточно сложная [11]. Передача и/или создание ключа требует вычисления цепочки узлов, соединенных квантовыми каналами, через которые будет передаваться ключ или его составные части. Такую цепочку узлов будем называть квантовым маршрутом. Способ вычисления квантового маршрута не является предметом данной работы.

Для магистральной сети КРК, в которой два узла, формирующие общий ключ, соединены только одной цепочкой ДПУ, квантовый маршрут определяется однозначно. Для городских сетей распространенной является топология сети КРК «звезда» [12, 13], что позволяет оптимизировать число узлов в сети и уменьшить количество необходимых квантовых каналов. Такая сеть КРК состоит из выделенного узла в центре звезды и периферийных узлов. Каждый периферийный узел соединен квантовым каналом с центральным узлом. Общий ключ формируется для пар периферийных узлов. Для каждой пары периферийных узлов квантовый маршрут также определяется однозначно и состоит ровно из трех узлов: начинается на одном периферийном узле, проходит через центральный узел и заканчивается на втором периферийном узле из пары. То есть в сети топологии «звезда» можно однозначно выделить магистральную подсеть для любой пары периферийных улов.

В сетях произвольной топологии вычисление квантового маршрута также сводится к выделению некоторой магистральной подсети, соединяющей

два узла, формирующих общий ключ. Таким образом, задача создания общего ключа в произвольной сети КРК для некоторой фиксированной пары узлов сводится к задаче создания общего ключа в магистральной сети КРК. Далее будем рассматривать только способы создания общего ключа в магистральной сети КРК и их свойства.

Критерии классификации схем

Для формирования классификации схем выработки ключей предлагается рассматривать критерии двух категорий: критерии, связанные с конструкциями схем, и критерии, связанные с характеристиками полученной схемы.

Во-первых, схемы по своей конструкции существенно различаются по источнику ключа. Так, в сетях КРК, описываемых в документах ETSI [14] и ITU-T [15], предлагается использовать квантовый ключ, созданный на некотором сегменте сети. Однако каждый узел сети КРК, содержащий элементы аппаратуры КРК, обязательно содержит физический датчик случайных чисел, способный формировать ключевой материал для создания квантового ключа [16]. Этот датчик случайных чисел может использоваться и для создания общего ключа пары удаленных узлов. Соответственно, источником ключа может являться любой из узлов квантового маршрута. Выделим схемы, в которых источником ключа является оконечный узел, который формирует общий ключ, и схемы, в которых источник ключа расположен не на оконечных узлах квантового маршрута.

Следующим критерием для классификации схем является способ передачи созданной ключевой информации. Ожидаемый способ – последовательная передача по узлам, входящим в квантовый маршрут. Однако возможны схемы, создающие служебные, вспомогательные ключи защиты между узлами, не соединенными квантовым каналом, и использующие такие ключи для передачи ключевой информации, составляющей создаваемый общий ключ. То есть передача ключа может осуществляться по квантовому маршруту; по маршруту, полученному путем усечения квантового маршрута за счет создания вспомогательных ключей. Граничный случай – передача ключа напрямую между двумя оконечными узлами. Для единообразия дальнейшего описания будем считать прямой маршрут тривиальным вариантом усечения квантового маршрута.

Следующий критерий классификации относится к типу используемых методов защиты при передаче ключа по маршруту. Системы КРК создают квантовые ключи, стойкие в теоретико-информационном смысле [17, 18]. Потенциальный нарушитель при корректной реализации протокола КРК не способен узнать создаваемый квантовый ключ даже при наличии неограниченных вычислительных мощностей. Желательно, чтобы подобным свойством обладала схема создания ключа и для магистральной сети КРК, т.е. при передаче и формировании общего ключа использовались примитивы, обеспечивающие стойкость в теоретико-информационном смысле. Тогда результирующий общий ключ будет близок по своим свойствам к квантовому ключу, создаваемому на одном сегменте. Существенные объемы ключевого материала, которые потребуются для теоретико-информационно стойких примитивов, дают почву для создания схем, стойких в вычислительном смысле. То есть общий ключ формируется с применением вычислительно стойких примитивов [19].

Важным критерием является способ обработки ключевой информации на промежуточных узлах маршрута, который будет определять требования доверия к этим узлам. В идеальной модели доступ к ДПУ имеют только легитимные пользователи, и потенциальный нарушитель не может никаким образом узнать передаваемую ключевую информацию. Тогда специальная обработка передаваемой ключевой информации не требуется. Также возможны схемы, использующие дополнительные методы защиты, что предотвращает раскрытие ключевой информации на ДПУ при ее передаче по квантовому маршруту в различных моделях нарушителя: имеющего доступ в контролируемую зону, имеющего прямой доступ к памяти узла или узлов и др.

Отдельным блоком целесообразно рассматривать эксплуатационные критерии классификации, такие как скорость создания общего ключа (в некоторых элементарных операциях), величины дополнительных данных (оверхеда), передаваемых помимо самой ключевой информации.

Анализ некоторых известных схем

Далее приводятся некоторые известные схемы выработки и распределения общего ключа с последующей их классификацией согласно предложенным критериям.

Схема 1

Наиболее часто встречающаяся схема выработки общего ключа представлена на рис. 1.

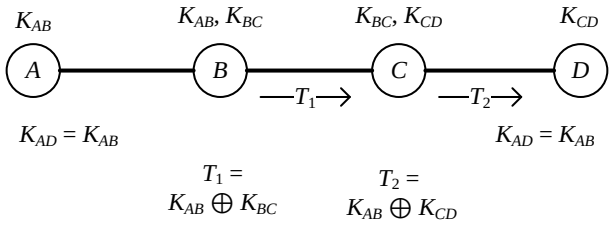

Рис. 1. Базовая схема выработки и распределения общего ключа

Ключ первого сегмента K_{AB} полагается общим ключом, который надо передать до второго оконечного узла. Защита при передаче от второго до последнего узлов осуществляется путем последовательного кодирования и декодирования одноразовым шифроблокнотом на квантовых ключах следующих сегментов K_{BC}, K_{CD} соответственно. В канале передаются закодированные сообщения T_1, T_2.

Схема 2

Модификация данной схемы, в которой в качестве общего ключа назначается квантовый ключ некоторого сегмента на квантовом маршруте, представлена на рис. 2. Оптимально с точки зрения скорости доставки общего ключа на оконечные узлы

выбирать квантовый ключ с сегмента, находящегося в середине квантового маршрута.

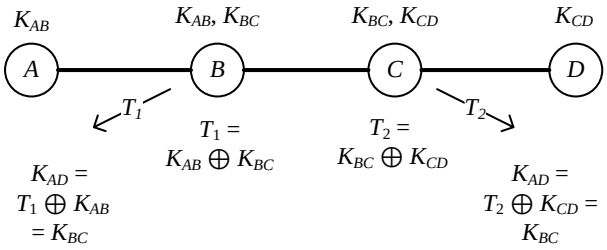

Рис. 2. Модифицированная схема выработки и распределения общего ключа

Схема 3

Представленные выше схемы не решают проблему раскрытия передаваемого ключа на промежуточных узлах. Рассмотрим некоторые подходы, позволяющие решить данную проблему. Следующая схема основана на соображениях, что одноразовый шифроблокнот (операция, исключающая ИЛИ) является линейным. Легко получить ключ совместного преобразования, а именно для некоторого ДПУ *i*-квантового маршрута ключ совместного преобразования получается по (1):

$$K_{(i-1,\, i+1)} = K_{(i-1,i)} \oplus K_{(i,i+1)}, \qquad (1)$$

где $K_{(i,j)}$ – ключ между узлами *i* и *j*.

За одно преобразование производится декодирование сообщения предыдущего сегмента с одновременным кодированием на ключе следующего сегмента. Общим ключом полагается некоторая случайная последовательность *X*, полученная с датчика случайных чисел ДПУ *A*. Схема изображена на рис. 3.

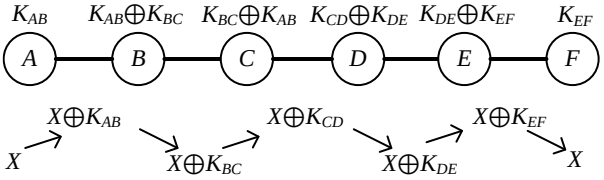

Рис. 3. Схема выработки ключа с созданием ключей совместного преобразования

ДПУ должны хранить только ключи совместного преобразования, безвозвратно удалив исходные квантовые ключи, из которых были получены эти ключи совместного преобразования. Эксплуатационные характеристики такой схемы оказываются существенно хуже, так как для каждого маршрута необходимо заранее подготовить и рассчитать ключи совместного преобразования. Если некоторый узел в сети соединен с *n* соседними узлами, то необходимо хранить C_n^2 ключей совместного преобразования вместо *n* квантовых ключей.

Схема 4

Реализация последовательного кодирования передаваемой ключевой информации совместно с использованными ключами порождает схему, описанную в патенте [20]. Схема представлена на рис. 4.

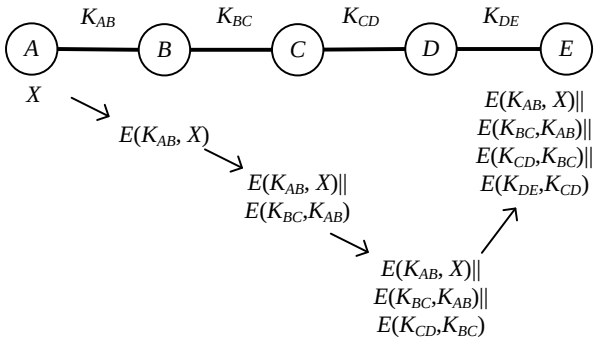

Рис. 4. Схема распределения общего ключа по принципу «матрешки»

Защита при передаче случайного числа, выступающего в качестве создаваемого общего ключа, осуществляется по принципу «матрешки». На первом узле случайное число кодируется функцией *E*() на первом квантовом ключе и полученное сообщение передается на второй узел. На втором узле ключ, использованный для кодирования на первом узле, кодируется функцией *E*() на квантовом ключе следующего сегмента и т.д. На последний узел квантового маршрута, состоящего из *r* узлов, поступает сообщение из *r*–2 сообщений, представляющих собой квантовый ключ некоторого сегмента, закодированный на квантовом ключе следующего сегмента, и одного сообщения, соответствующего закодированному случайному числу, из которого формируется общий ключ. Последний узел квантового маршрута последовательно декодирует части полученного сообщения, получая все необходимые ключи для декодирования случайного числа.

Несмотря на отсутствие требований к функции кодирования в описании [20], необходимо применять независимый набор квантовых ключей для каждого квантового маршрута даже при пересечении нескольких маршрутов на некоторых сегментах. При применении примитивов с теоретико-информационной стойкостью не возникает проблем повышенного расходования ключей, но с увеличением длины квантового маршрута необходимо передавать сообщения все большей длины.

Если достаточно обеспечивать вычислительную стойкость при передаче ключевой информации для формирования общего ключа, то для фиксированного квантового маршрута возможно однократно передать квантовые ключи всех сегментов на оконечный узел маршрута и в дальнейшем пересылать случайное число, закодированное квантовым ключом первого сегмента, напрямую на оконечный узел, минуя узлы квантового маршрута. С точки зрения стойкости схемы в целом это означает, что потенциальному нарушителю необходимо либо атаковать ключ кодирования первого сегмента (как единственное сообщение, появляющееся в открытом канале), либо реализовывать атаку на ДПУ для компрометации ключей защиты во время их передачи по квантовому маршруту. Причем в предложенной схеме на каждом следующем ДПУ маршрута раскрываются ключи со всех предыдущих сегментов маршрута.

Схема 5

Добавление ограничений на способ обработки ключевой информации на промежуточных узлах или на их структуру позволяет защититься от чтения передаваемой информации на промежуточных узлах потенциальным нарушителем. Так, способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей [21] накладывает специальное требование на используемые алгоритмы кодирования при передаче случайного числа. Используемые алгоритмы должны быть коммутативными. Для них должно выполняться свойство (2):

$$X = D_{K1}\left(E_{K1}\left(X\right)\right) = D_{K2}\left(E_{K2}\left(X\right)\right) = \\ = D_{K1}\left(D_{K2}\left(E_{K1}\left(E_{K2}\left(X\right)\right)\right)\right), \qquad (2)$$

где $D_{Ki}()$ – функция декодирования на ключе Ki; $E_{Ki}()$ – функция кодирования на ключе Ki; Ki – используемый ключ кодирования; X – передаваемое сообщение.

Тогда специальное устройство ДПУ и сохранение порядка преобразований позволяет добиться сокрытия передаваемых ключей на промежуточных узлах квантового маршрута. При этом не происходит увеличение расхода ключей защиты, отсутствует необходимость хранить большое количество различных ключей для различных вариантов маршрутов, а объем передаваемой закодированной информации по сегментам маршрута не увеличивается.

Для реализации способа требуется, чтобы каждый узел квантового маршрута помимо блоков квантовой аппаратуры (КА) имел независимые блоки СКЗИ, обозначены левый (Л) и правый (П) на рис. 5. Тогда последовательное кодирование полученного от предыдущего узла закодированного ключа C_i ключом следующего сегмента K_j в блоке П, передача промежуточного сообщения $C'_{i,j}$ в блок Л, декодирование на ключе предыдущего сегмента K_i в блоке Л и последующая передача закодированного передаваемого ключа C_j в блок П следующего узла квантового маршрута позволяет добиться защиты передаваемых данных на промежуточных узлах даже в случае, если потенциальный нарушитель обладает доступом к памяти одного из блоков узла.

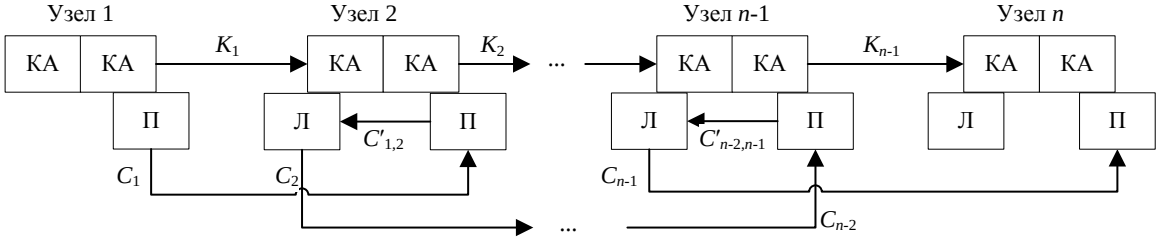

Рис. 5. Схема распределения общего ключа с фиксированным порядком преобразований

Схема 6

При наличии предварительно распределенного общего ключа между двумя оконечными узлами возможна реализация схемы со сквозной и транзитной защитой. Случайное число кодируется на предварительно распределенном ключе, получая таким образом некоторое защищенное представление случайного числа. Далее защищенное представление передается последовательно по узлам квантового маршрута с последовательной защитой на квантовых ключах каждого сегмента. В результате на промежуточных узлах маршрута возникает не само случайное число, формирующее общий ключ двух оконечных узлов, а только его защищенное представление. Даже имея прямой доступ к памяти промежуточного узла, становится невозможно получить непосредственно передаваемое случайное число.

Однако такая сквозная защита может быть реализуема и оправдана только для вычислительно стойких примитивов. Теоретико-информационно стойкие примитивы требуют однократного использования ключа защиты, следовательно, на оконечные узлы необходимо разместить достаточно большой запас предварительно распределенных ключей. В этом случае целесообразней не передавать никакой ключевой информации по сети, а использовать предварительно распределенные ключи в качестве общих ключей оконечных узлов. В то же время использование вычислительно стойких примитивов позволяет из малого объема предварительно распределенных ключей создавать значительно больший объем требуемых общих ключей.

В таблице приведена классификация описанных схем согласно предложенным критериям. Заметим, что для длинных квантовых маршрутов источник ключевой информации, расположенный на маршруте, практически не отличается от источника ключа, реализуемого протоколом КРК.

В настоящей работе рассматриваются только критерии, относящиеся к конструкции схем, так как для анализа эксплуатационных схем требуется дальнейшая конкретизация используемых алгоритмов. Указываются только некоторые важные эксплуатационные особенности.

Из таблицы видно, что схемы, предъявляющие меньше требований к используемым примитивам, не предоставляют защиты передаваемой ключевой информации на ДПУ и требуют повышенного доверия к ДПУ, что на практике приводит к реализации дополнительных организационно-технических мер защиты и особых правил размещения и/или эксплуатации ДПУ. Если схема обеспечивает защиту передаваемой ключевой информации, в том числе и при обработке на ДПУ, то появляются дополнительные ограничения к допустимым примитивам и ухудшаются эксплуатационные характеристики схемы.

Классификация схем по критериям, связанным с конструктивными особенностями

Критерий	Схема 1	Схема 2	Схема 3	Схема 4	Схема 5	Схема 6
Источник ключевой информации	Первый узел (квантовый ключ)	Произвольный узел (квантовый ключ)	Произвольный узел (случайное число)	Первый узел	Первый узел	Первый узел
Способ передачи	Последовательный от первого к последнему	Параллельный от источника до обоих оконечных	Последовательный от первого к последнему	Последовательная передача закодированных ключей совместно с закодированными ключами защиты по маршруту	Последовательно по маршруту. Специальный порядок обработки на ДПУ	Последовательно по маршруту
Класс используемых примитивов	Одноразовый шифроблокнот. Возможно применение произвольных алгоритмов	Одноразовый шифроблокнот. Возможно применение произвольных алгоритмов	Одноразовый шифроблокнот	Произвольные	Коммутативные	Вычислительно стойкие
Требование доверия к ДПУ	Максимальное	Максимальное	Среднее	Среднее	Минимальное	Минимальное
Эксплуатационные особенности	–	–	Предварительное вычисление всех ключей перекодирования. Повышенный объем хранимых ключей	Существенное повышение объема передаваемых данных при увеличении длины маршрута	Требуется контроль порядка обработки на ДПУ	Обязательны предварительно распределенные ключи на оконечных узлах

О влиянии источника ключевой информации

Отдельно отметим возможность навязывать общий ключ оконечных узлов узлом, на котором формируется исходная ключевая информация для дальнейшей передачи. Если такой узел-источник не совпадает ни с одним оконечным узлом, то допустимость такого навязывания определяется ожиданиями от конкретной сети КРК. Процессы, происходящие в сетях с централизованным управлением, более предсказуемы, но такой центральный узел требует максимальных усилий по его защите, и ему должны доверять все участники информационного взаимодействия. При этом любая схема, требующая передачи ключа строго от начала квантового маршрута в последний узел маршрута, адаптируется для централизованной сети КРК путем построения двух квантовых маршрутов и передачи одинаковых ключей до оконечных узлов от центрального узла.

В случае децентрализованных систем, где затруднительно выделить специальный узел и обеспечить для него высокую степень защиты, целесообразнее формировать ключевую информацию для создания общего ключа непосредственно на оконечном узле. Однако в этом случае оконечный узел может навязывать конкретные значения общего ключа, что может создать вектор атаки для потенциального нарушителя, если он сможет некоторым образом влиять на данный оконечный узел.

Решением проблемы является построение симметричных схем, в которых каждый из двух оконечных узлов вносит равный вклад в создание общего ключа. Фактически необходимо расширить схему создания ключа таким образом, чтобы каждый оконечный узел формировал свою часть ключевой информации, передавал ее второму оконечному узлу, после чего они независимо друг от друга объединяли две части ключевой информации для получения требуемого общего ключа. Правильный выбор способа объединения позволит исключить возможность навязывания и/или предсказывания итогового общего ключа любым из оконечных узлов до непосредственного формирования этого ключа.

Выводы

В работе предложены критерии для классификации схем выработки и распределения общих ключей для оконечных узлов магистральной сети КРК. Показана взаимосвязь процессов создания общих ключей в сетях КРК произвольной топологии с аналогичными процессами в магистральных сетях КРК. Проведена классификация некоторых схем выработки и распределения ключей в соответствии с предложенными критериями. Результаты анализа проведенной классификации показывают, что схемы с дополнительными ограничениями снижают требуемый уровень доверия к промежуточным узлам, но повышают эксплуатационные затраты или требуют специфичных реализаций системы КРК. Показаны возможные направления модификаций схем выработки и распределения ключей для улучшения их эксплуатационных свойств и свойств безопасности.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУРа на 2020–2022 гг. (проект № FEWM-2020-0037).

Литература

1. Миронова В.Г. Реализация модели TAKE-GRANT как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Н.Т. Югов // Доклады ТУСУР. – 2011. – № 2(24), ч. 3. – С. 206–210.

2. Text marking approach for data leakage prevention / A.V. Kozachok, S.A. Kopylov, A.A. Shelupanov, O.O. Evsutin // Journal of computer virology and hacking techniques. – 2019. – Vol. 15, No. 3. – P. 219–232.

3. Shelupanov A. Threat model for IoT systems on the example of openUNB protocol / A. Shelupanov, A. Konev, T. Kosachenko, D. Dudkin // International Journal of Emerging Trends in Engineering Research. – 2019. – Vol. 7, No. 9. – P. 283–290.

4. Novokhrestov A.K. Model of threats to computer network software / A.K. Novokhrestov, A.A. Konev, A.A. Shelupanov // Symmetry. – 2019. – Vol. 11, No. 12. – P. 1506.

5. Актуальные направления развития методов и средств защиты информации / А.А. Шелупанов, О.О. Евсютин, А.А. Конев, Е.Ю. Костюченко, Д.В. Кручинин, Д.С. Никифоров // Доклады ТУСУР. – 2017. – Т. 20. – С. 11–24.

6. White Paper No. 27 Implementation Security of Quantum Cryptography. Introduction, challenges, solutions [Электронный ресурс]. – Режим доступа: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf, свободный (дата обращения: 11.12.2021).

7. Испытание комплекса квантовой криптографической аппаратуры защиты информации на городских волоконно-оптических линиях связи / А.В. Борисова, А.Е. Жиляев, С.В. Алферов, В.Л. Елисеев, Ю.В. Кармазиков, А.Н. Климов, К.А. Балыгин // Вестник Российского нового университета. – Сер.: Сложные системы: модели, анализ и управление. – 2019. – № 4. – С. 100–110.

8. Молотков С.Н. О стойкости волоконной квантовой криптографии при произвольных потерях в канале связи: запрет измерений с определенным исходом // Письма в ЖЭТФ. – 2014. – Т. 100, вып. 6. – С. 457–464.

9. Elliot C. Building the quantum network // New Journal of Physics. – 2002. – Vol. 4. – P. 46.1–46.12.

10. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters / M. Lucamarini, Z.L. Yuan, J.F. Dynes, A.J. Shields // Nature. – 2018. – № 557. – P. 400–403.

11. Quantum Key Distribution: A Networking Perspective / M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, M. Voznak // ACM Comput. Surv. – 2021. – Vol. 53, No. 5. – P. 1–41.

12. Field and long-term demonstration of a wide area quantum key distribution network / S. Wang, W. Chen, Z.Q. Yin, H.W. Li, D.Y. He, Y.H. Li, Z. Zhou, X.T. Song, F.Y. Li, D. Wang // Optics Express. – 2014. – Vol. 22, No. 18. – P. 21739–21756.

13. Quantum key distribution network for multiple applications / A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami // Quantum Science and Technology. – 2017. – Vol. 2, No. 3. – P. 034003.

14. ETSI GS QKD 004 v.2.1.1 Quantum Key Distribution (QKD); Application Interface [Электронный ресурс]. – Режим доступа: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf, свободный (дата обращения: 11.12.2021).

15. ITU-T Recommendation Y.3800: Overview on networks supporting quantum key distribution [Электронный ресурс]. – Режим доступа: https://www.itu.int/rec/T-REC-Y.3800-202004-I!Cor1/en, свободный (дата обращения: 11.12.2021).

16. Реализация квантового генератора случайных чисел, основанного на оптимальной группировке фотоотсчетов / К.А. Балыгин, В.И. Зайцев, А.Н. Климов, С.П. Кулик, С.Н. Молотков // Письма в ЖЭТФ. – 2017. – Т. 106, вып. 7. – С. 451–458.

17. Bennet C.H. Quantum Cryptography: Public Key Distribution and Coin Tossing / C.H. Bennet, G. Brassard. // Theoretical Computer Science – 2014. –Vol. 560, Pt. 1. – P. 175–179.

18. Renner R. Security of Quantum Key Distribution [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/quant-ph/0512258.pdf, свободный (дата обращения: 11.12.2021).

19. Borodin M. Key generation schemes for channel authentication in quantum key distribution protocol / M. Borodin, A. Zhilyaev, A. Urivskiy // IET Quantum Communication. – 2021. – Vol. 2, No. 3. – P. 90–97.

20. Пат. 2 697 696 РФ, МПК H 04 L 9/08. Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей / А.М. Поздняков (РФ). – № 2 019 101 393; заявл. 18.01.19; опубл. 16.08.19, Бюл. № 23. – 3 с.

21. Пат. 2 708 511 РФ, МПК H 04 L 9/08, G 06 F 21/72. Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей / А.Е. Жиляев (РФ). – № 2 019 102 923; заявл. 04.02.2019; опубл. 09.12.19, Бюл. № 34. – 2 с.

Жиляев Андрей Евгеньевич
Исследователь Центра научных исследований
и перспективных разработок АО «ИнфоТеКС»
Отрадная ул., 2Б, стр. 1, г. Москва, Россия, 127273
ORCID: 0000-0001-6717-1785
Тел.: +7-903-960-05-27
Эл. почта: Andrey.zhilyaev@infotecs.ru

Zhilyaev A.E.

Key generation and distribution schemes classification for quantum key distribution networks of arbitrary topology

Quantum keys created during the quantum key distribution protocol have absolute secrecy due to physical laws and are not susceptible to breaking even with the unlimited computing power of the attacker. However, quantum key distribution systems have a range limit. Quantum key distribution networks based on trusted intermediate nodes are built to overcome the problem of the maximum range. This paper examines the connection of backbone networks with networks of arbitrary topology, introduces criteria for the classification of key generation and distribution schemes, and classifies some schemes according to the criteria introduced.

Keywords: quantum key distribution, QKD network, classification, quantum key, quantum path.
DOI: 10.21293/1818-0442-2021-24-4-33-39

References

1. Mironova V.G., Shelupanov A.A., Yugov N.T. [Implementation of the TAKE-GRANT model as a representation of systems for differentiating access rights in an organization]. *Proceedings of TUSUR University*, 2011, no. 2(24), part 3, pp. 206–210 (in Russ.).

2. Kozachok A.V., Kopylov S.A., Shelupanov A.A., Evsutin O.O. Text marking approach for data leakage prevention. *Journal of Computer Mirology and Hacking Techniques*, 2019, vol. 15, no. 3, pp. 219–232. DOI: 10.1007/s11416-019-00336-9.

3. Shelupanov A., Konev A., Kosachenko T., Dudkin D. Threat model for IoT systems on the example of openUNB protocol. International *Journal of Emerging Trends in Engineering Research*, 2019, vol. 7, no. 9, pp. 283–290. DOI: 10.30534/ijeter/2019/11792019.

4. Novokhrestov A.K.,Konev A.A., Shelupanov A.A. Model of threats to computer network software. *Symmetry*, 2019, vol. 11, no. 12, p. 1506. DOI: 10.3390/sym11121506.

5. Shelupanov A.A., Evsyutin O.O., Konev A.A., Kostyuchenko E.Yu., Kruchinin D.V., Nikiforov D.S. [Current trends in the development of methods and means of information protection]. *Proceedings of TUSUR University*, 2017, vol. 20, pp. 11–24 (in Russ.).

6. ETSI White Paper No. 27 Implementation Security of Quantum Cryptography. Introduction, challenges, solutions. *ETSI*, 2018. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf, free (Accessed: December 11, 2021).

7. Borisova A.V., Zhilyaev A.E., Alferov S.V., Eliseev V.L., Karmazikov U.V., Klimov A.N., Balygin K.A. [Testing of Quantum Key Distribution System in Urban Fiber-Optic Communication Lines]. *Vestnik ROSNOU: Complex systems: models, analysis, management*, 2019, no 4, pp. 100–110. DOI: 10.25586/RNU.V9187.19.04.P.100. (in Russ.).

8. Molotkov S.N. [On the stability of fiber-optic quantum cryptography at arbitrary losses in a communication channel: Exclusion of unambiguous measurements] *Jetp Letters*, 2014, vol. 100, no. 6, pp. 457–464 (in Russ).

9. Elliot C. Building the quantum network. *New Journal of Physics*, 2002, vol. 4, pp. 46.1–46.12.

10. Lucamarini M., Yuan Z.L., Dynes J.F., Shields A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 2018. no. 557, pp. 400–403. DOI: 10.1038/s41586-018-0066-6.

11. Mehic M., Niemiec M., Rass S., Ma J., Peev M., Aguado A., Martin V., Schauer S., Poppe A., Pacher C., Voznak M. Quantum Key Distribution: A Networking Perspective. *ACM Computing Surveys*, 2021, vol. 53, no 5, pp. 1–41. DOI: 10.1145/3402192.

12. Wang S., Chen W., Yin Z.Q., Li H.W., He D.Y., Li Y.H. , Zhou Z., Song X.T., Li F.Y., Wang D. Field and long-term demonstration of a wide area quantum key distribution network. *Optics Express*, 2014, vol. 22, no 18, pp. 21739-21756. doi: 10.1364/OE.22.021739.

13. Tajima A., Kondoh T., Ochi T., Fujiwara M., Yoshino K., Iizuka H., Sakamoto T., Tomita A., Shimamura E., Asami S. Quantum key distribution network for multiple applications. *Quantum Science and Technology*, 2017, vol. 2, no. 3, p. 034003.

14. ETSI GS QKD 004 v.2.1.1 Quantum Key Distribution (QKD); Application Interface. *ETSI*, 2020. Available at: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf, free (Accessed: December 11, 2021).

15. ITU-T Recommendation Y.3800: Overview on networks supporting quantum key distribution. Available at: https://www.itu.int/rec/T-REC-Y.3800-202004-I!Cor1/en, free (Accessed: December 11, 2021).

16. Balygin K.A., Zaitsev V.I., Klimov A.N., Kulik S.P., Molotkov S.N. [Implementation of a quantum random number generator based on the optimal clustering of photocounts]. *Jetp Letters*, 2017, vol. 106, no 7, pp. 451–458. DOI: 10.7868/S0370274X17190109 (in Russ).

17. Bennet C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theoretical Computer Science*, 2014, vol. 560, part 1, pp. 175–179. DOI: 10.1016/j.tcs.2014.05.025.

18. Renner R. Security of Quantum Key Distribution, 2006. Available at: https://arxiv.org/pdf/quant-ph/0512258.pdf, free (Accessed: December 11, 2021).

19. Borodin M., Zhilyaev A., Urivskiy A. Key generation schemes for channel authentication in quantum key distribution protocol. *IET Quantum Communication*, 2021, vol. 2, no. 3, pp. 90–97. DOI: 10.1049/qtc2.12020.

20. Pozdnyakov A.M. Sposob peredachi soobshcheniya cherez vychislitel'nuyu set' s primeneniem apparatury kvantovogo raspredeleniya klyuchei [The way to transmit a message through the computational network using the quantum key distribution devices]. Patent RF, no. 2697696, 2019.

21. Zhilyaev A.E. Sposob formirovaniya klyucha mezhdu uzlami vychislitel'noi seti s ispol'zovaniem sistemy kvantovogo raspredeleniya klyuchei [The way to compute a key between nodes of the computational network using quantum key distribution systems]. Patent RF, no. 2708511, 2019.

Andrey E. Zhilyaev
Researcher, Research and Development Center,
JSC «InfoTeCS»
2B, Otradnaya st., bld.1, Moscow, Russia, 127273
ORCID: 0000-0001-6717-1785
Phone: +7-903-960-05-27
Email: Andrey.zhilyaev@infotecs.ru

УДК 004.056

В.И. Васильев, В.Е. Гвоздев, Р.Р. Шамсутдинов

Обнаружение аномалий в системах промышленного Интернета вещей на основе искусственной иммунной системы

Проведен анализ актуальности обеспечения безопасности беспроводных сенсорных сетей. Для обнаружения аномалий в таких сетях предложено использование механизмов искусственной иммунной системы (ИИС). С целью обучения и оценки эффективности системы использован тестовый набор данных о сетевых соединениях WSN-DS. Проведены вычислительные эксперименты, осуществлено сравнение полученных результатов при использовании в ИИС в качестве меры близости косинусного расстояния, Евклидовой меры и расстояния Хэмминга. Показано, что разработанная система демонстрирует высокую эффективность при использовании расстояния Хэмминга.

Ключевые слова: искусственная иммунная система, информационная безопасность, обнаружение аномалий, WSN-DS, беспроводные сенсорные сети.
DOI: 10.21293/1818-0442-2021-24-4-40-45

Стремительное развитие и широкое применение систем промышленного Интернета вещей (Industrial Internet of Things, IIoT) приводит к увеличению рисков нарушения кибербезопасности промышленных объектов. Так, 20% респондентов, опрошенных Лабораторией Касперского [1], в качестве одной из главных киберугроз определяют атаки на IIoT, а утечки данных и атаки на цепочки поставок считают наиболее опасными по 15% респондентов. 55% опрошенных выделили использование IIoT в качестве одного из главных факторов, влияющих на кибербезопасность АСУ ТП, но только 14% компаний внедрили инструменты детектирования сетевых аномалий и 19% – средства мониторинга сети и трафика. По данным CheckPoint [2], 67% предприятий уже столкнулись с инцидентами безопасности, связанными с IoT-устройствами. IIoT-сети становятся всё более сложными, а решения для обеспечения их безопасности остаются далеко позади.

Нарушение безопасности IIoT может привести к несанкционированному распространению защищаемой информации, возникновению угроз жизни и здоровью людей в результате аварий на промышленных предприятиях или деструктивного воздействия на IIoT-устройства в медицинских учреждениях.

Одной из ключевых уязвимостей систем IIoT является широкое применение беспроводных сетевых технологий, в частности, в беспроводных сенсорных сетях (Wireless Sensor Network, WSN), нередко используемых в IIoT. WSN характеризуются высокой степенью уязвимости, обусловленной их распределённостью, открытостью и ограниченностью ресурсов сенсорных узлов [3].

С целью обнаружения сетевых атак в информационных системах в последнее время все чаще предлагается применение механизмов искусственных иммунных систем (ИИС). ИИС способны обнаруживать неизвестные атаки, демонстрируют высокую производительность и низкое число ошибок 1-го и 2-го рода [4, 5]. В данной работе рассматривается применение ИИС для обнаружения аномалий в WSN. Под аномалиями при этом понимаются отклонения от нормального поведения, вызванные попытками несанкционированного доступа к данным, изменения протоколов обмена и передачи данных и т.п.

Анализ современного состояния исследований

В [6] проанализированы протоколы маршрутизации, применяемые в WSN, основные атаки, такие как Sinkhole, Blackhole, Byzantine Attack и др., а также основные проблемы исследований в области беспроводных сенсорных сетей.

В [7] проанализированы функциональные особенности WSN и наиболее распространенные типы атак. В качестве защиты от вредоносных или скомпрометированных узлов предлагается использовать адаптивное взаимодействие элементов системы, основанное на анализе поведения соседних узлов.

В [8] подчеркивается высокая уязвимость сенсорных узлов WSN, возможность злоумышленников нанести большой ущерб при успешной компрометации узла; определены уязвимости алгоритмов обмена аутентификационной информацией. Во избежание компрометации узла авторы предлагают дополнить существующий алгоритм новой схемой обмена аутентификационной информацией. Оценка BAN-логикой, а также проведённые оценки производительности и защищённости показывают эффективность предложенной схемы.

В [9] предлагается адаптивный иммуноинспирированный энергоэффективный кроссслойный протокол маршрутизации (Adaptive Immune-inspired Energy-Efficient Cross-layer Routing protocol (AIEECR)). Данный протокол используется для выбора наиболее эффективного маршрута передачи данных на базовую станцию от каждого центра кластера (Cluster Head). Производительность предложенного подхода сравнивается с другими методами, результаты экспериментов демонстрируют эффективность предлагаемого авторами метода.

В [10] предложено использование алгоритма муравьиной колонии для повышения уровня защищенности сенсорной сети. Вопросы обеспечения безопасности WSN подробно рассматриваются в [11–13].

С целью обучения систем обнаружения аномалий и оценки их эффективности используются различные наборы данных. В [14] подробно описан WSN-DS – один из таких наборов, преимуществом которого является то, что он основан на протоколе LEACH – одном из наиболее широко используемых иерархичных протоколов маршрутизации в беспроводных сенсорных сетях. Этот набор содержит около 370 тыс. строк, включает 4 вида атак: Blackhole, Grayhole, Scheduling, Flooding. Каждая запись WSN-DS содержит 18 параметров. Этот набор данных служит основой для построения различных систем обнаружения атак и использован в данной работе.

В [15] для обнаружения вторжений в WSN используется модель, основанная на применении генетических алгоритмов и градиентного бустинга. Оценка эффективности системы проводилась с применением набора данных WSN-DS. Предложенный подход позволил выявить 97,8% атак.

В [16] для анализа WSN-DS использовался случайный лес (СЛ) в сравнении с искусственной нейронной сетью (ИНС), где точность обнаружения атак с помощью СЛ составила 97,2%, ИНС – 95,8%.

В [17] авторы также анализируют вышеуказанный набор данных с применением таких классификаторов, как машина опорных векторов, J48, СЛ, наивный Байесовский классификатор (НБК), ИНС. Наилучшую точность обнаружения атак продемонстрировал случайный лес – 99,7% верно выявленных атак.

В [18] используется алгоритм бэггинга (Bagging algorithm) для построения ансамбля деревьев решений C4.5. Система обучена распознаванию атак, представленных в WSN-DS, выявлено 98,4% атак.

Проанализированные выше работы демонстрируют высокую точность обнаружения известных атак на примере рассматриваемого набора данных, однако постоянное возникновение новых атак обусловливает актуальность разработки системы, способной выявлять в том числе неизвестные атаки. Кроме того, с целью повышения производительности систем актуальным остается вопрос уменьшения пространства параметров.

Искусственные иммунные системы (ИИС) демонстрируют высокий уровень обнаружения неизвестных атак при низком уровне ошибок, способны постоянно самообучаться в процессе анализа. ИИС также применяются для решения задачи обнаружения атак в беспроводных сенсорных сетях. В рассматриваемых ниже работах для оценки эффективности используются другие наборы данных, отличные от WSN-DS, однако это не является критичным для сравнения методологий.

В [19] предлагается многоуровневая система обнаружения вторжений для WSN на основе иммунной теории. Система включает блоки: B-клеток, T-клеток, дентритных клеток и базофилов. Здесь B-клетки проводят первичный анализ данных, они формируются только на этапе обучения системы. Система не способна постоянно обучаться. Для измерения расстояния между векторами используется алгоритм битового сопоставления. Сравнения с другими метриками не произведено. Дальнейший анализ данных производится дентритными клетками, в случае выявления аномалии передается сигнал блоку T-клеток, который осуществляет реакцию, изолирует аномальный узел, не участвует в анализе. Блок базофилов в работе пока не реализован.

В [20] предложен алгоритм глубокого обучения и дентритных клеток (Deep Learning and Dendritic Cell Algorithm, DeepDCA). Для оценки эффективности применяется набор данных BoT-IoT. В работе реализовано сжатие пространства параметров, применяется самоорганизующаяся ИНС, осуществляющая первичную обработку данных и категорирование входного сигнала на сигналы об опасности и о безопасном состоянии. Дальнейший анализ осуществляется дендритными клетками. Представлены результаты сравнения с такими классификаторами, как k-ближайших соседей, машина опорных векторов, многослойный перспетрон, НБК. DeepDCA продемонстрировал наилучшую точность обнаружения. Однако в данной работе речь идет об обнаружении только известных атак с опорой на первичные сигналы опасности от ИНС.

В [21], как и в предлагаемом подходе, используются алгоритмы негативной селекции для обеспечения толерантности системы к нормальному состоянию, клональной селекции, обеспечивающей адаптивность системы, возможность ее постоянного самообучения. В моделировании использован протокол LEACH, проанализированы следующие виды атак: Resource depletion, Sinkhole, Wormhole, Sybil, Selective forwarding attack. Обнаружение строится с использованием теории опасности.

В первую очередь члены и центры кластера в WSN обнаруживают изменения своих собственных свойств, извлекают ключевые данные и получают информацию о сигналах среды, оценивают риск. В случае опасности член кластера передает соответствующий сигнал опасности центру кластера, объединяющего несколько сигналов опасности, переводящих их узлу-приемнику. Узел-приемник вычисляет степень риска, область риска запрашивает представления антигенов. Узлы датчиков опасной зоны собирают информацию о сетевом трафике для формирования антигенов. После этого узел-приемник проводит анализ на предмет вторжения. Подобный алгоритм создает дополнительную нагрузку на членов и центры кластера.

Искусственная иммунная система

ИИС имитирует работу естественной иммунной системы человека, способной обнаруживать неизвестные организму чужеродные патогены. Адаптивная составляющая иммунитета основывается на функционировании так называемых лимфоцитов – иммунных клеток, отвечающих за приобретенный иммунитет.

В ИИС нет необходимости подробного моделирования каждого вида лимфоцитов по отдельности, достаточно выделить основные функции. Для обучения ИИС достаточно данных о нормальном пове-

дении анализируемой системы. Первичное обучение заключается в генерации формальных лимфоцитов – точек-детекторов, обнаруживающих аномалии в пределах заданного от них расстояния. С целью исключения ошибочного определения нормального состояния системы как аномального проводится процедура отрицательного отбора или негативной селекции, которая заключается в удалении из числа детекторов всех тех, что «реагируют» на данные о нормальном состоянии системы.

Адаптивность ИИС обеспечивается реализацией алгоритма клональной селекции, а также периодическим обновлением набора детекторов. Клональная селекция заключается в многократном клонировании с некоторой случайной мутацией (искажением) детектора, выявившего угрозу. Данный механизм позволяет более эффективно обнаруживать аномалии, подобные уже выявленным ранее, обеспечивая постоянное самообучение системы. Необходимо отметить, что каждый такой клон также подвергается процедуре отрицательного отбора для обеспечения толерантности к нормальному состоянию системы. Клоны заменяют собой «худшие» детекторы, т.е. выявившие наименьшее число аномалий.

С целью периодического обновления детекторов каждому из них устанавливается некоторое время жизни, по истечении которого, если детектор не обнаружил аномалий, он уничтожается, вместо него генерируется новый случайный детектор, также подвергаемый негативной селекции. Если детектор обнаружил аномалию, время его жизни значительно увеличивается.

Процедура анализа данных заключается в вычислении расстояния между анализируемым вектором и каждым вектором-детектором: если хотя бы одно значение меньше порогового, считается, что соответствующий детектор выявил аномалию.

Результаты вычислительных экспериментов

Предлагаемая система предполагает формирование отдельных узлов-снифферов, что не требует дополнительных ресурсов членов кластера. Она, в отличие от проанализированных выше [19–21], не основывается на теории опасности. Анализ проводится постоянно обновляемым набором детекторов с реализацией алгоритмов негативной селекции, клональной селекции на основе различных метрик, что позволяет системе автоматически дообучаться на основе выявленных в процессе анализа аномалий, оставаясь толерантной к нормальному состоянию.

Система, помимо выявления известных атак, позволяет обнаруживать также ранее неизвестные атаки. Реализовано сжатие пространства параметров WSN-DS, сравнение мер близости векторов, используемых в процессе анализа.

В рамках предыдущего исследования [3] авторами настоящей статьи была проведена оценка эффективности применения искусственной иммунной системы для выявления аномалий в беспроводных сенсорных сетях на основе WSN-DS с использованием расстояния Хэмминга в качестве меры близости между векторами, однако не были рассмотрены другие критерии.

Рассмотрим косинусную меру, описываемую формулой

$$\cos\phi = \frac{\sum_{i=1}^{n} x_i y_i}{\sqrt{\sum_{i=1}^{n} x_i^2}\sqrt{\sum_{i=1}^{n} y_i^2}}. \quad (1)$$

В этой формуле x_i и y_i – компоненты векторов параметров сравниваемых шаблонов детекторов, n – размерность этих векторов. Соответственно, чем более похожи векторы, тем ближе значение косинуса к единице, если они менее похожи – к нулю.

Также было рассмотрено Евклидово расстояние, вычисляемое как

$$d(x,y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}. \quad (2)$$

Набор данных был предварительно обработан таким образом, чтобы значения всех параметров лежали в диапазоне [0; 1] с точностью до сотых. Флаговые значения были оставлены без изменений; значения, кодирующие номера узлов, были переведены в вышеуказанный диапазон. Все остальные значения были также равномерно распределены в вышеуказанном диапазоне, их нормализованные значения были вычислены следующим образом:

$$c = \frac{p}{\max(p_i)}, \quad (3)$$

где p – значение параметра до нормализации; $\max(p_i)$ – максимальное среди всех возможных значений данного параметра до нормализации.

Были проведены вычислительные эксперименты, которые показали, что эффективность ИИС при использовании меры расстояния на основе (1) оказалась крайне низкой. Поэтому был проведен следующий анализ. Нормализованный набор данных был разделен на подмножество данных о нормальном состоянии системы и подмножество данных об аномалиях. Затем для каждого вектора данных о нормальном состоянии был найден максимально похожий вектор данных об аномалиях с использованием косинусной меры. Оказалось, что более чем для 65% таких пар векторов значение косинуса превышает 0,98, для более чем 80% – 0,95, хотя число идентичных строк между двумя подмножествами менее 0,01%. Таким образом, подмножества трудноразделимы косинусной мерой.

Эффективность ИИС при измерении расстояния по критерию (2) оказалась более высокой. Анализ вначале проводился по всем 18 нормализованным параметрам. С целью улучшения производительности было принято решение уменьшить число анализируемых параметров.

Для каждого вектора данных о нормальной активности был найден ближайший вектор множества данных об аномалиях, вычислен и записан модуль разности по каждому параметру (координате). Затем была найдена сумма этих модулей отдельно по каждому параметру, после чего они были ранжированы

по наибольшему значению полученной суммы, как представлено в таблице.

Ранжированные параметры

Номер параметра	Наименование параметра	Сумма модулей разности
1	ID	10 706 270
4	Who_CH	9 286 618
2	Time	5 407 324
12	Rank	2 720 009
5	Dist_To_CH	1 762 264
13	DATA_S	1 733 408
16	dist_CH_To_BS	1 014 887
7	ADV_R	733 664
14	DATA_R	556 365
18	Consumed Energy	442 674
17	send_code	259 555
15	Data_Sent_ To_BS	199 383
9	JOIN_R	18 551
6	ADV_S	16 398
10	SCH_S	4 316
11	SCH_R	2 529
3	Is_CH	544
8	JOIN_S	147

При проведении анализа сначала учитывались все параметры, затем их число постепенно уменьшалось. Как показали результаты, при использовании первых 9 ранжированных параметров сохраняется высокая эффективность обнаружения, как это представлено на рис. 1. При дальнейшем уменьшении их количества эффективность обнаружения аномалий заметно снижается.

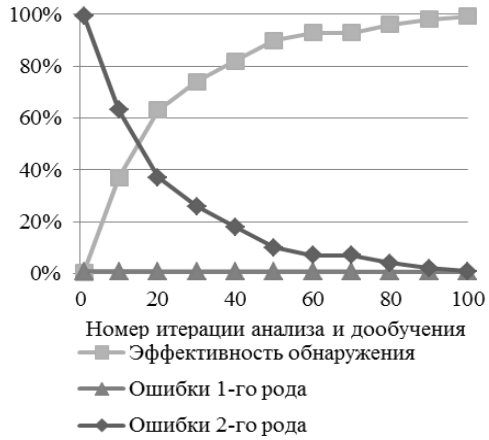

Рис. 1. Эффективность ИИС с использованием Евклидова расстояния

Отметим, что динамика обучения ИИС при использовании Евклидовой меры схожа с динамикой, наблюдаемой при использовании расстояния Хэмминга, представленной рис. 2.

Таким образом, использование и расстояния Хэмминга, и Евклидова расстояния позволяет обнаруживать как известные, так и неизвестные аномалии с высокой точностью и низким количеством ошибок, однако скорость вычисления расстояния Хэмминга, как показывает практика, более чем в 5 раз превышает скорость вычисления Евклидова расстояния.

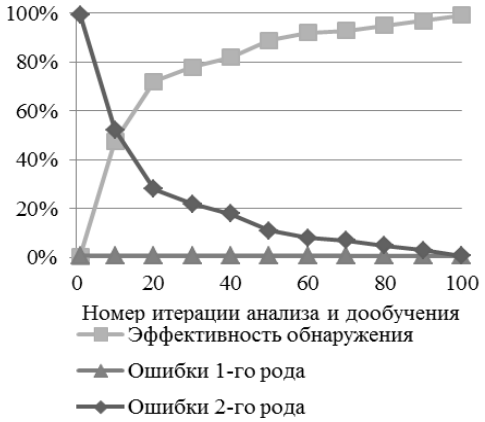

Рис. 2. Эффективность ИИС с использованием расстояния Хэмминга [3]

Достигнутый показатель точности распознавания при этом составляет 99,2%, что превышает аналогичные показатели, приведенные в работах [15, 16, 18–21]. В качестве примечания следует отметить, что алгоритм СЛ, использованный в [17], обеспечивает сходные показатели точности, однако не позволяет обнаруживать неизвестные атаки.

Заключение

Применение систем промышленного Интернета вещей значительно увеличивает риски нарушения кибербезопасности. По данным CheckPoint [2], 67% предприятий уже столкнулись с инцидентами безопасности, связанными с IoT-устройствами. Широкое использование беспроводных соединений, в том числе беспроводных сенсорных сетей, делает системы IIoT более уязвимыми.

Для выявления аномалий в информационных системах целесообразно применение искусственных иммунных систем, имитирующих работу естественной иммунной системы человека. Ключевые алгоритмы ИИС:

– отрицательный отбор – обеспечивает толерантность ИИС к нормальному состоянию системы;

– клональная селекция – осуществляет дообучение системы в процессе её функционирования;

– обновление детекторов – обеспечивает адаптивность системы и повышает вероятность обнаружения неизвестных атак.

Оценка эффективности разработанной системы в ходе экспериментов осуществлялась с использованием набора данных WSN-DS [14], содержащего около 370 тыс. строк, 4 вида атак на WSN. Было проведено сравнение работы ИИС на основе трёх мер расстояния между векторами: косинусного, Евклидова расстояния и расстояния Хэмминга. Результаты вычислительных экспериментов показали невысокую эффективность применения косинусной меры для анализируемого набора данных и высокую точность обнаружения при использовании Евклидовой меры и расстояния Хэмминга. Наибольшее быстродействие при этом демонстрирует ИИС, основанная на вычислении расстояния Хэмминга.

В целом применение ИИС демонстрирует высокую эффективность обнаружения аномалий в беспроводных сенсорных сетях.

Работа выполнена при поддержке гранта РФФИ № 20-37-90024.

Литература

1. Лаборатория Касперского: распространение умных устройств в промышленности повлечёт за собой смену подхода к киберзащите [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-rasprostranenie-umnih-ustroistv-v-promishlennosti-povlechyot-za-soboi-smenu-podhoda-k-kiberzaschite, свободный (дата обращения: 13.03.2021).

2. Check Point IoT Protect [Электронный ресурс]. – Режим доступа: https://www.checkpoint.com/downloads/products/cp-iot-security-solution-brief.pdf, свободный (дата обращения: 13.03.2021).

3. Vasilyev V. Providing Information Security on the Base of Artificial Immune System for Industrial Internet of Thing / V. Vasilyev, R. Shamsutdinov // Advances in Intelligent Systems Research. – 2020. – Vol. 174. – P. 212–217.

4. Tarakanov A.O. A Comparison of Immune and Genetic Algorithms for Two Real-Life Tasks of Pattern Recognition / A.O. Tarakanov, Y.A. Tarakanov // Int. J. of Unconventional Computing. – 2004. – Vol. 1.4. – P. 357–374.

5. Tarakanov A.O. A Comparison of Immune and Neural Computing for Two Real-Life Tasks of Pattern Recognition / A.O. Tarakanov, Y.A. Tarakanov // Lecture Notes in Computer Science. – 2004. – Vol. 3239. – P. 236–249.

6. Saini V. WSN Protocols, Research challenges in WSN, Integrated areas of sensor networks, security attacks in WSN / V. Saini, J. Gupta, K.D. Garg // European Journal of Molecular & Clinical Medicine. – 2020. – Vol. 7, Iss. 3. – P. 5145–5153.

7. Ovasapyan T. Security Provision in WSN on the Basis of the Adaptive Behavior of Nodes [Электронный ресурс] / T. Ovasapyan, D. Moskvin // Proceedings of the 4th World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). – Режим доступа: https://ieeexplore.ieee.org/document/9210421, свободный (дата обращения: 05.03.2021).

8. An Authentication Information Exchange Scheme in WSN for IoT Applications / S. Yang, Y. Shiue, Z. Su, I. Liu, C. Liu // IEEE Access. – 2020. – Vol. 8. – P. 9728–9738.

9. Yarde P. Adaptive immune-inspired energy-efficient and high coverage cross-layer routing protocol for wireless sensor networks / P. Yarde, S. Srivastava, K. Garg // IET Communications. – 2020. – Vol. 14, Iss. 15. – P. 2592–2600.

10. Iwendi C. ACO based key management routing mechanism for WSN security and data collection [Электронный ресурс] / C. Iwendi, Z. Zhang, X. Du // 2018 IEEE International Conference on Industrial Technology (ICIT). – 2018. – P. 1935–1939. – Режим доступа: https://ieeexplore.ieee.org/document/8352482, свободный (дата обращения: 05.03.2021)

11. Kavitha T. Security Vulnerabilities in Wireless Sensor Networks: a survey / T. Kavitha, D. Sridharan // Journal of Information Assurance and Security. – 2010. – Vol. 5. – P. 31–44.

12. Dimitrievski1 A. Security Issues and Approaches in WSN [Электронный ресурс] / A. Dimitrievski, V. Pejovska, D. Davcev. – Режим доступа: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.6190&rep=rep1&type=pdf, свободный (дата обращения: 06.06.2021).

13. Furtak J. Security techniques for the WSN link layer within military IoT [Электронный ресурс] / J. Furtak, Z. Zieliński, J. Chudzikiewicz // 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). – 2016. – P. 233–238. – Режим доступа: https://ieeexplore.ieee.org/document/7845508, свободный (дата обращения: 02.03.2021)

14. Almomani I. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks [Электронный ресурс] / I. Almomani, B. Al-Kasasbeh, M. AL-Akhras // Journal of Sensors. – 2016. – Vol. 2016. – Режим доступа: https://www.hindawi.com/journals/js/2016/4731953, свободный (дата обращения: 01.03.2020).

15. A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks / M. Alqahtani, A. Gumaei, H. Mathkour, M. Maher Ben Ismail // Sensors (Basel). – 2019. – Vol. 19. – P. 1–20.

16. An Effective Classification for DoS Attacks in Wireless Sensor Networks [Электронный ресурс] / T.-T.-H. Le, T. Park, D. Cho, H. Kim // 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). – 2018. – P. 689–692. – Режим доступа: https://www.researchgate.net/publication/327065277_An_Effective_Classification_for_DoS_Attacks_in_Wireless_Sensor_Networks, свободный (дата обращения: 06.09.2021).

17. Alsulaimanand L. Performance evaluation of machine learning techniques for DOS detection in wireless sensor network / L. Alsulaimanand, S. Al-Ahmadi // International Journal of Network Security & Its Applications (IJNSA). – 2021. – Vol. 13, No. 2. – P. 21–29.

18. Dong R.-H. An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm / R.-H. Dong, H.-H. Yan, Q.-Y. Zhang // International Journal of Network Security. – 2020. – Vol. 22, No. 2. – P. 218–230.

19. Alaparthy V. A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory / V. Alaparthy, S. Morgera // IEEE Access. – 2018. – Vol. 6. – P. 47364–47373.

20. DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System / S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani, A. Al-Barakat // Applied Sciences. – 2020. – Vol. 10. – P. 1909–1932.

21. Xiao X. A Danger Theory Inspired Protection Approach for Hierarchical Wireless Sensor Networks / X. Xiao, R. Zhang // KSII Transactions on Internet and Information Systems. – 2019. – Vol. 13, No. 5. – P. 2732–2753.

Васильев Владимир Иванович
Д-р техн. наук, проф. каф. вычислительной техники и защиты информации (ВТиЗИ) Уфимского государственного авиационного технического университета (УГАТУ)
Карла Маркса ул., 12, г. Уфа, Россия, 450008
Тел.: +7-917-350-11-39
Эл. почта: vasilyev@ugatu.ac.ru

Гвоздев Владимир Ефимович
Д-р техн. наук, профессор каф. технической кибернетики (ТК) УГАТУ
Карла Маркса ул., 12, г. Уфа, Россия, 450008
Тел.: +7-917-369-27-73
Эл. почта: wega55@mail.ru

Шамсутдинов Ринат Рустемович
Аспирант каф. ВТиЗИ УГАТУ
Карла Маркса ул., 12, г. Уфа, Россия, 450008
Тел.: +7-927-950-84-13
Эл. почта: shrr2019@yandex.ru

Vasilyev V.I., Gvozdev V.E., Shamsutdinov R.R.

Network Anomaly Detection Based on Artificial Immune System for Industrial Internet of Things

The paper analyzes the relevance of ensuring the security of wireless sensor networks (WSN), proposes the use of an artifi-

cial immune system (AIS) to detect anomalies in such networks. A dataset on WSN connections called WSN-DS was used to train and evaluate the efficiency of proposed system. Computational experiments were conducted with the use of the cosine distance, Euclidean measure and Hamming distance in the AIS. The system demonstrated the highest efficiency when using Hamming distance measure.

Keywords: Artificial Immune System, Information Security, Anomaly Detection, WSN-DS, Wireless Sensor Networks.
DOI: 10.21293/1818-0442-2021-24-4-40-45

References

1. *Laboratoriya Kasperskogo: rasprostranenie umnyh ustrojstv v promyshlennosti povlechyot za soboj smenu podhoda k kiberzashchite* [Kaspersky Lab: the proliferation of smart devices in the industry will lead to a change in the approach to cyber defense]. Available at: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-rasprostranenie-umnih-ustroistv-v-promishlennosti-povlechyot-za-soboi-smenu-podhoda-k-kiberzaschite, free (Accessed: March 13, 2021) (in Russ.).

2. Check Point IoT Protect, CheckPoint Software Technologies LTD. Available at: https://www.checkpoint.com/downloads/products/cp-iot-security-solution-brief.pdf, free (Accessed: March 13, 2021).

3. Vasilyev V., Shamsutdinov R. Providing Information Security on the Base of Artificial Immune System for Industrial Internet of Thing, *Advances in Intelligent Systems Research*, 2020, vol. 174, pp. 212–217.

4. Tarakanov A.O., Tarakanov Y.A. A Comparison of Immune and Genetic Algorithms for Two Real-Life Tasks of Pattern Recognition, *International Journal of Unconventional Computing*, 2004, vol. 1.4, pp. 357–374.

5. Tarakanov A.O., Tarakanov Y.A. A Comparison of Immune and Neural Computing for Two Real-Life Tasks of Pattern Recognition, *Lecture Notes in Computer Science*, 2004, vol. 3239, pp. 236–249.

6. Saini V., Gupta J., Garg K.D. WSN Protocols, Research challenges in WSN, Integrated areas of sensor networks, security attacks in WSN, *European Journal of Molecular & Clinical Medicine*, 2020, vol. 7, iss. 3, pp. 5145–5153.

7. Ovasapyan T., Moskvin D. Security Provision in WSN on the Basis of the Adaptive Behavior of Nodes, *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, UK, 2020, pp. 81–85. Available at: https://ieeexplore.ieee.org/document/9210421, free (Accessed: March 05, 2021).

8. Yang S., Shiue Y., Su Z., Liu I., Liu C. An Authentication Information Exchange Scheme in WSN for IoT Applications, *IEEE Access*, 2020, vol. 8, pp. 9728–9738.

9. Yarde P., Srivastava S., Garg K. Adaptive immune-inspired energy-efficient and high coverage cross-layer routing protocol for wireless sensor networks, *IET Communications*, 2020, vol. 14, iss. 15, pp. 2592–2600.

10. Iwendi C., Zhang Z., Du X. ACO Based Key Management Routing Mechanism for WSN Security and Data Collection, *2018 IEEE International Conference on Industrial Technology (ICIT)*, 2018, pp. 1935–1939. Available at: https://ieeexplore.ieee.org/document/8352482, free (Accessed: March 05, 2021).

11. Kavitha T., Sridharan D. Security Vulnerabilities In Wireless Sensor Networks: A Survey, *Journal of Information Assurance and Security*, 2010, vol. 5, pp. 31–44.

12. Dimitrievski A., Pejovska V., Davcev D. Security Issues and Approaches in WSN. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.6190&rep=rep1&type=pdf, free (Accessed: June 06, 2021).

13. Furtak J., Zieliński Z., Chudzikiewicz J. Security techniques for the WSN link layer within military IoT, *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp. 233–238. Available at: https://ieeexplore.ieee.org/document/7845508, free (Accessed: March 02, 2021).

14. Almomani I., Al-Kasasbeh B., AL-Akhras M. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks, *Journal of Sensors*, 2016, vol. 2016. Available at: https://www.hindawi.com/journals/js/2016/4731 953, free (Accessed: March 01, 2021).

15. Alqahtani M., Gumaei A., Mathkour H., Maher Ben Ismail M. A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks, *Sensors (Basel)*, 2019, vol. 19, pp. 1–20.

16. Le T.-T.-H., Park T., Cho D., Kim H. An Effective Classification for DoS Attacks in Wireless Sensor Networks, *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2018, pp. 689–692. Available at: https://www.researchgate.net/publication/327065277_An_Effective_Classification_for_DoS_Attacks_in_Wireless_Sensor_Networks, free (Accessed: September 06, 2021).

17. Alsulaimanand L., Al-Ahmadi S. Performance Evaluation of Machine Learning Techniques for DOS Detection in Wireless Sensor Network, *International Journal of Network Security & Its Applications (IJNSA)*, 2021, vol.13, no. 2, pp. 21–29.

18. Dong R.-H., Yan H.-H., Zhang Q.-Y. An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm, *International Journal of Network Security*, 2020, vol. 22, no. 2, pp. 218–230.

19. Alaparthy V., Morgera S. A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory, *IEEE Access*, 2018, vol. 6, pp. 47364–47373.

20. Aldhaheri S., Alghazzawi D., Cheng L., Alzahrani B., Al-Barakat A. DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System, *Applied Sciences*, 2020, vol. 10, pp. 1909–1932.

21. Xiao X., Zhang R. A Danger Theory Inspired Protection Approach for Hierarchical Wireless Sensor Networks, *KSII Transactions on Internet and Information Systems*, 2019, vol. 13, no. 5, pp. 2732–2753.

Vladimir I. Vasilyev
Doctor of Science in Engineering, Professor,
Department of Computing and Information Security
Ufa State Aviation Technical University
12, Karl Marx st., Ufa, Russia, 450008
Phone: +7-917-350-11-39
Email: vasilyev@ugatu.ac.ru

Vladimir E. Gvozdev
Doctor of Science in Engineering, Professor,
Department of Technical Cybernetics,
Ufa State Aviation Technical University
12, Karl Marx st., Ufa, Russia, 450008
Phone: +7-917-369-27-73
Email: wega55@mail.ru

Rinat R. Shamsutdinov
Postgraduate student,
Department of Computing and Information Security,
Ufa State Aviation Technical University
12, Karl Marx st., Ufa, Russia, 450008
Phone: +7-927-950-84-13
Email: shrr2019@yandex.ru

УДК 004.056

И.А. Лубкин

Метрики защищенности приложений при использовании средств противодействия уязвимостям, основанных на возвратно-ориентированном программировании

Уязвимости, использующие возвратно-ориентированное программирование, создают угрозу функционирования информационных систем. Для противодействия им создано множество средств защиты, основанных на различных принципах функционирования. При этом отсутствуют общепризнанные подходы к оценке защищенности применяемых решений. В работе предложены метрики защищенности, позволяющие получить объективные данные об эффективности средств защиты от RoP-уязвимостей. Формируемые показатели защищенности отражают возможность проведения атаки при получении атакующим контроля над графом потока управления.
Ключевые слова: уязвимость, удаленное исполнение кода, RoP, защита кода, метрики.
DOI: 10.21293/1818-0442-2021-24-4-46-51

Потребность защиты от атак, основанных на возвратно-ориентированном программировании (RoP-атак), привела к созданию множества подходов, применяемых для решения проблемы. Атаки данного типа позволяют реализовать класс уязвимостей удаленного исполнения кода. Актуальность защиты связана с тем, что злоумышленник может получить как минимум возможность исполнения произвольного алгоритма на атакуемой системе. Это в дальнейшем может привести к повышению привилегий, получению удаленного доступа и иным негативным последствиям.

С началом выпуска процессоров, поддерживающих технологию теневого стека (например, реализация CET [1], предложенная Intel), наметился прогресс в решении проблемы RoP-атак. При этом информационные системы, аппаратное обеспечение которых не поддерживает указанную технологию и экономически неприемлема его замена, остаются уязвимы. Уязвимыми также остаются приложения, для которых нет возможности проведения перекомпиляции. Технология теневого стека требует модификации машинного кода программы.

Для повышения защищенности в системах, не поддерживающих аппаратные средства защиты, для противодействия RoP-атакам применяются программные меры защиты. Нужно оценивать эффективность таких мер защиты, потому что не удаётся в общем случае доказать её теоретически. Это обусловлено невозможностью создания программного обеспечения с доказанно корректным алгоритмом. Также проблема оценки эффективности зачастую связана с тем, что средства защиты основаны на неизвестности для атакующего сведений об образе исполняемой программы или о месте его размещения в памяти.

Автором была предложена система защиты от RoP-атак. Принцип ее работы заключается в защите эпилогов подпрограмм и снижении числа пригодных для использования в рамках атаки участков (далее – гаджетов) вне эпилогов. Описание приведено в [2]. Особенностью подхода является отсутствие необходимости в исходных текстах и перекомпиляции, так как выполняется вставка кода непосредственно в бинарный образ. Средство вставки описано в [3].

Общепринятые подходы к оценке подобных систем защиты отсутствуют. Для такой оценки нужны метрики, по которым можно сравнить предлагаемое решение и аналогичные ему. Сравнивать подобные решения тяжело, потому что их авторы редко приводят детали программной реализации и результатов работы. Более того, решения могут не иметь общих характеристик для сравнения.

Рассматриваются операционные системы семейства GNU/Linux, функционирующие на аппаратной платформе с архитектурой AMD64 и Intel64.

Обзор существующих подходов

Рассмотрим принципы работы аналогов предлагаемого решения. По ним можно определить, пригодны существующие подходы к оценке эффективности или нет. Показатели качества средства защиты зависят от этих принципов. Анализ систем защиты от RoP-уязвимостей показал следующие основные направления защиты:

1. Рандомизация размещения (периодически [4], при старте [5], в родительских процессах [6]). Для данного подхода безопасность основана на неизвестности атакующему сведений о содержимом исполнимой памяти атакуемой программы. При наличии примитива чтения у атакующего программа становится уязвима перед атаками от момента получения достаточной информации и до следующего переразмещения, если таковое предусмотрено системой защиты. Метрики защищенности могут быть выражены как оценка вероятности наличия у атакующего примитива чтения и определение статистических показателей временно́го «окна», когда возможна атака. Такие метрики неприменимы для предлагаемой системы защиты, так как она построена на предположении известности атакующему информации о содержимом исполнимой памяти.

2. Снижение числа пригодных для атаки гаджетов (на этапе компиляции [7, 8], в процессе работы за счет оверлеев [9]). Предлагаемая система защиты

включает меры, соответствующие данному направлению. Анализ подходов, применяемых для оценки защищенности, рассмотрен подробнее далее.

3. Затруднение получения контроля над ГПУ (путем контроля целостности адреса возврата [10], сигнатуры в стеке [11], косвенного указания адресов переходов [12]). Предлагаемая система защиты включает меры, соответствующие данному направлению, поэтому анализ подходов, применяемых для оценки защищенности, рассмотрен подробнее далее.

Проанализируем подходы, используемые во втором и третьем направлениях оценки защищенности для определения возможности применения в данной работе:

– качественный анализ подверженности атакам. Основан на экспертной оценке путем соотнесения предлагаемых мер и модели атаки. Его недостатком является возможная неполнота рассмотрения, что может приводить к последующему выявлению недостатков защиты, пропущенных при авторском анализе [13] (возможным улучшением ситуации могло бы стать проведение аудита безопасности, но такая практика не встречается в проанализированном материале);

– подсчет числа гаджетов. Арифметический подсчет является корректным, когда целью ставится устранение всех инструкций возврата. При синонимическом преобразовании опасных участков с целью сделать их непригодными для атаки такой подход не может показать корректного результата без доработки с целью учета не только количества, но и качества гаджетов;

– применение существующих эксплойтов (с адаптацией или без). Не является показательным в общем случае при изменении конфигурации фреймов стека (как, например, в предлагаемом принципе защиты), так как применимость зависит от их структуры. При этом потенциально возможно создание иного эксплойта, применимого к защищенной программе.

Для объективной оценки защищенности программ при применении предлагаемого и подобных ему решений необходимо определить количество реально пригодных для атак гаджетов. Такой подход позволит обойтись без субъективных экспертных оценок и экстраполяции существующих уязвимостей на защищаемую программу. Качественная оценка является неполноценной, так как оперирует предположениями о действиях атакующего, а не объективными данными, показывающими возможность атаки.

Постановка задачи

Ставится задача формирования набора метрик, показывающих возможность проведения RoP-атак.

Исходные посылки, определяющие состояние системы на начало атаки: невыполнение любого из перечисленных условий делает атаку невозможной. Атакующий:

– преодолел ASLR за счет примитива чтения (наличие которого предполагается);

– разместил в стеке или куче произвольные данные, которые могут быть использованы как управляющие данные и аргументы гаджетов;

– имеет возможность передачи управления на произвольный адрес (т.е. рассматривается ситуация, когда существует возможность запустить исполнение RoP-цепочки при наличии набора подходящих гаджетов);

– обладает полной информацией о принципе работы системы защиты и образе атакуемой программы.

Рассмотрим детальнее гаджеты, используемые для реализации уязвимостей. Структурно они состоят из двух частей: алгоритмической и управляющей. Первая содержит последовательность обрабатывающих данные инструкций, вторая – управляющую инструкцию, которой он оканчивается. В зависимости от вида управляющей инструкции гаджеты могут быть разделены на:

– RoP – оканчивается инструкциями «RETN», «RETN imm16», «RETF» и «RETF imm16». Для их использования в составе гаджета в стеке (со смещением или без) должен быть размещен адрес следующего гаджета или он же, но с указанием сегментного регистра соответственно. Их классификация приведена в [14];

– JoP – оканчивается инструкцией вида «JMP reg». Для её использования в составе гаджета в регистр-аргумент атакующий должен поместить адрес следующего гаджета;

– CoP – оканчивается инструкцией вида «CALL reg». Для её использования в составе гаджета в регистр-аргумент атакующий должен поместить адрес следующего гаджета, а в рамках его исполнения извлечь адрес возврата, записанный в стек ранее.

Применимость гаджетов в рамках атак определяется целью злоумышленника. Например, если атакующему необходимо вызвать функцию, принимающую аргументы через регистры *xmm*, то при отсутствии инструкций работы с ними в составе гаджетов конечная цель не может быть достигнута. Были проанализированы существующие эксплойты для определения конечных состояний, достижение которых является критерием успешности атаки. В качестве них были определены критерии:

– вызов подпрограммы из системной библиотеки, спроецированной на адресное пространство атакуемой программы. В стек атакующим помещаются данные, в регистрах передаются аргументы, в финале управление передается на целевую системную функцию (например, установки атрибута исполнимости на необходимую атакующему страницу памяти). Порядок передачи аргументов определяется БИП [15];

– для уязвимостей кода в привилегированном режиме – отключение аппаратных систем защиты процессора путем изменения режима работы процессора вследствие записи в управляющие регистры;

– простой передачи управления недостаточно для атаки, так как это соответствовало бы ситуации,

когда в программе содержится участок кода, выполняющий все необходимые для злоумышленника операции (а это означает наличие программной закладки или НДВ).

Из анализа целей следует, что атакующему необходимо конкретное состояние системы для успешности атаки. Рассмотрим в качестве примера ситуацию, когда ему необходимо передать один аргумент в подпрограмму с указанием некоторого числа. Если атакующий может влиять на ГПУ, но не может записать в регистр rdi, используемый для передачи первого аргумента, необходимое значение, то атака не может быть проведена успешно. Соответственно, разрабатываемые метрики должны учитывать это.

Выбранные метрики оценки должны учитывать, что аргументы работы с памятью имеют различную разрядность. Вследствие этого атакующий может располагать, например, средствами взаимодействия в ОЗУ или передачи управления в диапазоне адресов от 0 до 2^{32}–1. Данный диапазон штатно не используется ОС, вследствие чего все такие средства становятся бесполезными. Отсутствие учета таких аспектов ведет к неверной оценке результатов применения защиты.

Предлагаемые метрики защищенности

В качестве исходных данных для метрик целесообразно использовать перечни гаджетов, формируемые существующими средствами их поиска. Это позволяет работать с тем же списком, что и атакующий. Корректность инструментария для поиска обеспечивается распространенностью использования, вследствие чего их ошибки устраняются.

При этом использовать напрямую результаты работы средств поиска гаджетов некорректно, так как не все выявляемые ими гаджеты применимы и полезны. Необходимо учитывать только те гаджеты, которые приближают атакующего к состоянию, соответствующему критерию успешной атаки. Найденные гаджеты подлежат фильтрации, а лишь затем анализу.

Для учета специфики предлагаемой методики защиты гаджеты должны быть проанализированы на наличие штатных инструкций, модифицирующих вершину стека, которая используется как адрес возврата, и известность атакующему аргумента этих инструкций. Это отражает принцип рассматриваемой методики защиты, когда перед инструкцией возврата производится вставка инструкции, выполняющей над адресом возврата операцию XOR. При этом аргумент операции генерируется случайно в прологе каждой подпрограммы. Если в рамках гаджета выполняется неизвестная операция, то вместо следующего гаджета управление будет передано на неопределенный адрес, что с близкой к 100% вероятностью вызовет нештатное прекращение работы защищенного приложения. В результате уязвимость удаленного кода не будет реализована.

При выборе метрик должен быть учтен вопрос возможности транслировать численные показатели в возможность проведения атаки. Например, если атакующий имеет в распоряжении набор гаджетов, который не позволяет модифицировать память или регистры, но позволяет передавать управление, то такой набор не обеспечивает достижения цели атакующего. Таким образом, гаджеты, которые не позволяют менять состояние регистров или памяти, исключаются из рассмотрения и не должны влиять на метрики.

Изложенные в предыдущем разделе требования позволяют сформировать следующие метрики:

– число уникальных гаджетов после исключения из рассмотрения неприменимых гаджетов (критерии описаны далее, так как они зависят от программного средства выявления гаджетов). Данная метрика показывает общее количество потенциальных гаджетов. Её расчет важен для определения относительного снижения числа гаджетов при сравнении оригинальной и защищенной программ, а также исключения ложноположительного вывода о повышении защищенности для приложений, сформированных средствами защиты, интегрированными в компилятор (такими, как G-free);

– перечень регистров, значение которых может задавать атакующий напрямую (например, в результате извлечения данных из стека). Может быть определен как аргумент-назначение таких команд, как «MOV», «POP» и т.п. Для краткости аргументы группируются по принципу вложенности (например, если атакующий может определять значение части регистра *ch* и регистра *ecx*, то достаточно указать значение *ecx*). Данная метрика показывает возможности атакующего задавать произвольные значения в регистрах программы. Без её расчета невозможно определение способности атакующего задавать значения регистров и параметры алгоритма, исполняемого в ходе атаки;

– перечень регистров, значение которых может задавать атакующий косвенно, – определяются регистры, на значение которых атакующий может влиять через выполнение операций или транзитных передач (из этого множества исключаются регистры, значение которых атакующий может задавать напрямую). Необходимость введения данной метрики обусловлена тем, что предыдущая метрика не отражает полного множества регистров, доступных атакующему;

– показатель доступных подпрограмм – при наличии возможности задать значение первого аргумента показатель равен единице, первого и второго – он равен двойке и т.д. Первые шесть аргументов передаются через регистры (указаны в порядке возрастания номера аргумента): *rdi*, *rsi*, *rdx*, *rcx*, *r*8, *r*9. Данный показатель отражает разнообразие возможных конечных подпрограмм, которые может вызывать атакующий (указывается для полноценно вызываемых подпрограмм и для частично определяемых аргументов, когда атакующий не может полностью определять значение регистра). При этом вследствие последнего критерия успешной атаки конечным состоянием не может быть вызов подпрограммы без

аргументов. Так как атакующий имеет возможность управлять ГПУ (и, следовательно, вызывать любую подпрограмму), то возможность атаки сводится к возможности указания аргументов необходимой подпрограммы.

Указанные метрики позволяют определить принципиальную невозможность проведения атаки. То есть если атакующий не имеет средств для достижения конечного состояния атаки, то атака удаленного исполнения кода не может быть проведена. Иначе атака потенциально может быть реализована.

Программная реализация

Средство реализации вычисления метрик представляет собой программу на языке python, выполняющую первичное определение состава гаджетов, их фильтрацию и определение метрик. Анализируемая программа обрабатывается как «черный ящик». Для получения первичных данных используется программное средство ROPgadget [16]. Его результаты работы записываются в файл. Для сформированных данных проводится фильтрация, в ходе которой устраняются ложно обнаруженные гаджеты. Удаляются из перечня при фильтрации гаджеты:

– содержащие инструкцию «RETF», если перед ней отсутствует REX-префикс «0×48», который задает 64-разрядный режим обработки. Это связано с тем, что при отсутствии префикса может быть задан только адрес в пределах 32 бит с расширением нулями старших 32 бит, но ОС не использует данный диапазон, что делает их ложно пригодными;

– состоящие только из инструкций передачи управления, так как без модификации содержимого регистров и/или памяти атакующий не может достигнуть цели атаки. Возможна ситуация, когда без некоторой специфичной инструкции передачи управления построение RoP-цепочки станет невозможным. Определение таких ситуаций требует анализа конкретного сценария проведения атаки. Вследствие того, что он не может быть определен без рассмотрения конкретной уязвимости, то для отсутствия сужения применимости метрик будем считать, что у атакующего присутствуют в составе гаджетов все необходимые инструкции для передачи управления, а гаджеты, состоящие только из таких инструкций, исключаются из рассмотрения;

– содержащие операции с неканоническими адресами (старшие два байта адреса должны быть равны 0 или 0xFFFF) или неиспользуемыми диапазонами адресов (первые 2^{32} байт);

– выполняющие операции с неизвестным для атакующего и не модифицируемым им аргументом над адресом возврата. Например, в рамках предлагаемой системы защиты над адресом возврата проводится операция XOR с регистром *r*11, содержащим неизвестное атакующему значение. Если у злоумышленника нет возможности определить содержимое регистра, то исполнение такой инструкции в составе гаджета приведет к аварийному завершению программы.

Для отфильтрованных данных проводится обработка, в ходе которой вычисляются значения метрик, характеризующих защищенность от RoP-атак, и делается вывод о возможности или невозможности атаки.

Результаты экспериментальной проверки

Для проверки корректности оценки защищенности была сформирована выборка программ. Для каждой программы из выборки применяется методика защиты. Для оригинальной и защищенной программы проводится получение метрик защиты. Полученные результаты анализируются.

В состав выборки программ включены: синтетические тесты (содержащие намеренно внесенные дефекты, позволяющие проводить RoP-атаки), заведомо уязвимые приложения (используемые в различных соревнованиях по информационной безопасности) и приложения из состава ОС для оценки защищенности до и после применения системы противодействия RoP-атакам.

Примеры результатов определения метрик представлены в таблице. Из приведенных данных следует, что состав регистров, на которые может влиять атакующий, радикально уменьшается после применения предлагаемой системы защиты. Это приводит к тому, что атакующий хотя и может передать управление на целевую подпрограмму, но не имеет возможности указать ни один её аргумент. Из этого можно сделать вывод о том, что RoP-атака для удаленного исполнения кода нереализуема, а защита обеспечена. Для выборки в целом состав гаджетов после применения системы защиты соответствует приведенным примерам и не позволяет злоумышленнику проводить атаки.

Метрики защищенности, полученные для приложений до и после защиты

Приложение	Уникальные гаджеты		Регистры, определяемые атакующим		Оперируемые регистры		Дост. арг. (полностью / частично)		Защита обеспечена
	Ориг.	Защ.	Ориг.	Защ.	Ориг.	Защ.	Ориг.	Защ.	
Синтетический тест, нет оптимиз.	389	3	*rax, ch, rbx, edx, rsi, rdi, rbp, rsp, r8d, r12, r13, r14, r15*	Нет	*rcx, rdx, fr7*	*al*	4/5	0	Да
Синтетический тест, ур. оптимиз. 2	122	3	*eax, rbx, rsi, rdi, rbp, rsp, r12, r13, r14, r15*	Нет	*rax, ecx, edx*	*al*	2/4	0	Да
Учебное уязвимое приложение [17]	85	3	*eax, rbx, rsi, rdi, rbp, rsp*	Нет	*rax, edx*	*al*	2/3	0	Да
coremark	232	4	*rax, rbx, rsi, rdi, rbp, rsp, r8b, r12, r13, r14, r15, xmm0*	*bh*	*ecx, edx, r9d*	*eax*	2/6	0	Да
sshd	4713	23	*eax, rbx, rsi, rdi, rbp, rsp, r8, r11, r12, r13, r14, r15*	*eax, edx*	*r9, r10*	*rax*	6/6	0	Да

Для синтетических тестовых и для заведомо уязвимых приложений было осуществлено формирование эксплойтов для оригинального и защищенного варианта. Целью являлся вызов подпрограммы «system», принимающей один аргумент – имя и аргументы приложения, запускаемого в командной оболочке. Для оригинальных приложений эксплойты корректно сработали и позволили выполнить запуск целевой подпрограммы. Для защищенного варианта реализация эксплойта оказалась невозможна вследствие отсутствия гаджетов, помещающих в регистр *rdi* первый аргумент вызывающей целевой подпрограммы. Эксплойт, выполняющий только передачу управления на целевую подпрограмму, приводит к аварийному завершению работы атакуемого приложения. Данный результат свидетельствует о корректности выбранных метрик.

Данный подход, в отличие от аналогов, основанных на экспертных оценках, оперирует объективными данными. Это устраняет человеческий фактор при анализе защищенности.

Заключение

Предлагаемые метрики позволяют получить объективные данные об изменении подверженности RoP-атакам в результате применения системы защиты. При изменении модели атак предложенные метрики могут быть адаптированы для новых условий. Фильтрация неприменимых в атаках гаджетов позволяет исключить ложноотрицательные результаты. Анализ применимости гаджетов для достижения атакующим его цели обеспечивает определение возможности проведения RoP-атак в принципе.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ). Проект № 21/2020.

Литература

1. Shanbhogue V. Security Analysis of Processor Instruction Set Architecture for Enforcing Control-Flow Integrity / V. Shanbhogue, D. Gupta, R. Sahita // Proceedings of the 8th International Workshop on Hardware and Architectural Support for Security and Privacy. – New York: Association for Computing Machinery, 2019. – P. 1–11.

2. Лубкин И.А. Комплексная система защиты от уязвимостей, основанных на возвратно-ориентированном программировании / И.А. Лубкин, В.В. Золотарев // Труды СПИИРАН. – 2022. – № 21 (1) – в печати.

3. Lubkin I.A. Automatic equivalency restoration after software patching / I.A. Lubkin, V.V. Zolotarev // Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies». – Yaroslavl: Saint Petersburg Electrotechnical University «LETI», 2021. – P. 217–222.

4. Shuffler: Fast and deployable continuous code re-randomization / D. Williams-King, G. Gobieski, K. Williams-King, J.P. Blake // Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation. – Savannah, GA, USA: USENIX Association, 2016. – P. 367–382.

5. Selfrando: Securing the Tor Browser against De-anonymization Exploits/ M. Conti, S. Crane, T. Frassetto, A. Homescu // Proceedings on Privacy Enhancing Technologies. – 2016. – № 4. – P. 454–469.

6. How to Make ASLR Win the Clone Wars: Runtime Re-Randomization. K. Lu, S. Nürnberger, M. Backes, W. Lee [Электронный ресурс]. – Режим доступа: http://dx.doi.org/10.14722/ndss.2016.23173, свободный (дата обращения: 01.09.2021).

7. G-Free: Defeating return-oriented programming through gadget-less binaries / K. Onarlioglu, L. Bilge, A. Lanzi, D. Balzarotti // Proceedings of ACSAC. – Austin, Texas, USA: ACM Press, 2010. – P. 49–58.

8. Defeating return-oriented rootkits with «return-less» kernels / J. Li, Z. Wang, X. Jiang, M. Grace // Proceedings of EuroSys. – Paris, France: ACM Press, 2010. – P. 195–208.

9. Execution Integrity with In-Place Encryption / D. Sullivan, O. Arias, D. Gens, L. Davi, A. Sadeghi, Y. Jin [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/1703.02698.pdf, свободный (дата обращения: 01.09.2021).

10. RAP:RIP ROP 2015 [Электронный ресурс]. – Режим доступа: https://pax.grsecurity.net/docs/PaXTeam-H2HC15-RAP-RIP-ROP.pdf, свободный (дата обращения: 01.09.2021).

11. Perry Wagle, Crispin Cowan, StackGuard: Simple Stack Smash Protection for GCC, GCC Developers Summit, 2003 [Электронный ресурс]. – Режим доступа: https://gcc.gnu.org/pub/gcc/summit/2003/Stackguard.pdf, свободный (дата обращения: 01.09.2021).

12. Применение компиляторных преобразований для противодействия эксплуатации уязвимостей программного обеспечения / А.Р. Нурмухаметов, Ш.Ф. Курмангалеев, В.В.Каушан, С.С. Гайсарян // Труды ИСП РАН. – М.: ИСП РАН, 2014. – Т. 26, вып. 3. – С. 113–126.

13. Koo Z.Z. Analysis of ROP attack on grsecurity. PaX linux kernel security variables / Z.Z. Koo, Z. Ayop, Z.Z. Abidin // International Journal of Applied Engineering Research. – 2017. – Vol. 12, Iss. 23. – C. 13179–13185.

14. Вишняков А.В. Классификация ROP гаджетов // Труды ИСП РАН. – М.: ИСП РАН, 2016. – Т. 28, № 6. – С. 27–36.

15. AMD64 Architecture Processor Supplement Draft Version 0.99.7 [Электронный ресурс]. – Режим доступа: https://www.uclibc.org/docs/psABI-x86_64.pdf, свободный (дата обращения: 01.09.2021).

16. Инструмент ROPgadget. Репозиторий с исходным кодом [Электронный ресурс]. – Режим доступа: https://github.com/JonathanSalwan/ROPgadget, свободный (дата обращения: 01.09.2021).

17. Return oriented programming. Собираем exploit по кусочкам [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/255519/, свободный (дата обращения: 01.09.2021).

Лубкин Иван Александрович
Ст. преп. каф. безопасности информационных технологий (БИТ) Сибирского государственного ун-та науки и технологий (СибГУ) им. акад. М.Ф. Решетнева
Имени газеты «Красноярский рабочий» пр-т, 48б,
г. Красноярск, Россия, 660037
ORCID: 0000-0002-9657-0440
Тел.: +7 (391-2) 22-76-39
Эл. почта: lubkin@rambler.ru

Lubkin I.A.

Application security metrics when using defense system against vulnerabilities based on return-oriented programming

The vulnerabilities using return-oriented programming pose threats to the functioning of information systems. There are many protection systems to counteract them. They are based on various principles of functioning. At the same time, there are no generally accepted approaches to assess the security of applied solutions. The paper proposes security metrics that allow obtaining objective data on the efficiency of protection against RoP vulnerabilities. Proposed security metrics show ability to perform attack by gain control over control flow graph.

Keywords: vulnerability, remote code execution, RoP, code protection, metrics.
DOI: 10.21293/1818-0442-2021-24-4-46-51

References

1. Shanbhogue V., Gupta D., Sahita R. Security Analysis of Processor Instruction Set Architecture for Enforcing Control-Flow Integrity. *Proceedings of the 8th International Workshop on Hardware and Architectural Support for Security and Privacy*. New York, Association for Computing Machinery, 2019, pp. 1–11.

2. Lubkin I.A., Zolotarev V.V. Comprehensive defense system against vulnerabilities based on return-oriented programming. *SPIIRAS Proceedings*, 2022, no. 21 (1) (in Russ.). In press.

3. Lubkin I.A. Automatic equivalency restoration after software patching. *Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies»*, Yaroslavl, Saint Petersburg Electrotechnical University «LETI», 2021, pp. 217–222.

4. Williams-King D., Gobieski G., Williams-King K., Blake J. P. Shuffler: Fast and deployable continuous code re-randomization. *Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation*, Savannah, GA, USA, USENIX Association, 2016, pp. 367–382.

5. Conti M., Crane S., Frassetto T., Homescu A. Selfrando: Securing the tor browser against de-anonymization exploits. *Proceedings on Privacy Enhancing Technologies*, 2016, no. 4, pp. 454–469.

6. How to Make ASLR Win the Clone Wars: Runtime Re-Randomization. Lu K., Nürnberger S., Backes M., Lee W. Available at: http://dx.doi.org/10.14722/ndss.2016.23173, free (Accessed: September 1, 2021).

7. Onarlioglu K., Bilge L., Lanzi A., Balzarotti D., Kidra E. G-Free: Defeating return-oriented programming through gadget-less binaries. *Proceedings of ACSAC*. Austin, Texas, USA, ACM Press, 2010, pp. 49–58.

8. Li J., Wang Z., Jiang X., Grace M., Bahram S. Defeating return-oriented rootkits with «return-less» kernels. *Proceedings of EuroSys*, Paris, France, ACM Press, 2010, pp. 195–208.

9. Execution Integrity with In-Place Encryption. Sullivan D., Arias O., Gens D., Davi L., Sadeghi A., Jin Y. Available at: https://arxiv.org/pdf/1703.02698.pdf, free (Accessed: September 1, 2021).

10. RAP:RIP ROP 2015. Available at: https://pax.grsecurity.net/docs/PaXTeam-H2HC15-RAP-RIP-ROP.pdf, free (Accessed: September 1, 2021).

11. StackGuard: Simple Stack Smash Protection for GCC. Wagle P., Cowan C. Available at: https://gcc.gnu.org/pub/gcc/summit/2003/Stackguard.pdf, free (Accessed: September 1, 2021).

12. Nurmukhametov A.R., Kurmangaleev S.F., Kaushan V.V., Gaissaryan S.S. Compiler protection techniques against software vulnerabilities exploitation. *Proceedings of the Institute for System Programming of the RAS*, 2014, no. 26(3), pp. 113–126 (in Russ.).

13. Koo Z.Z., Ayop, Z., Abidin Z.Z. Analysis of ROP attack on grsecurity. PaX linux kernel security variables. *International Journal of Applied Engineering Research*, 2017, no. 12, pp. 13179–13185.

14. Vishnjakov A.V. Classification of ROP-gadgets. *Proceedings of the ISP RAS*, 2016, vol. 28, issue 6, pp. 27–36 (in Russ.).

15. AMD64 Architecture Processor Supplement Draft Version 0.99.7 Available at: https://www.uclibc.org/docs/psABI-x86_64.pdf, free (Accessed: September 1, 2021).

16. ROPgadget tool. Source code repository. Available at: https://github.com/JonathanSalwan/ROPgadget, free. (Accessed: September 1, 2021).

17. *Return oriented programming. Sobiraem exploit po kusochkam* [Return oriented programming. Exploit construction by pieces]. Available at: https://habr.com/ru/post/255519/, free (Accessed: September 1, 2021) (in Russ.).

Ivan A. Lubkin
Senior Lecturer, Department of Information Technologies Security, Reshetnev Siberian State University of Science and Technology
48b, Imeni gazety «Krasnoyarskiy rabochiy» pr., Krasnoyarsk, Russia, 660037
ORCID: 0000-0002-9657-0440
Phone: +7 (391-2) 22-76-39
Email: lubkin@rambler.ru

УДК 331.108.2, 004.056

А.А. Шелупанов, С.В. Глухарева, М.М. Немирович-Данченко

Оценка благонадежности сотрудника в системе кадровой безопасности предприятия

Предлагается методика оценки надежности сотрудника в системе кадровой безопасности предприятия. Проведен анализ существующих решений в различных отраслях. В рамках апробации разработанной рекомендательной системы показаны этапы оценки и уровни надежности. Проведена численная оценка компетенции сотрудников, показана согласованность результатов с оценкой компетенций, проводимой по фактическим результатам деятельности сотрудников.

Ключевые слова: кадровая безопасность, оценка благонадёжности, принятие решений, объекты КИИ.
DOI: 10.21293/1818-0442-2021-24-4-52-57

За последние пять лет число и масштаб экономических преступлений внутри компаний существенно выросли. Хищение ресурсов, промышленный шпионаж, разглашение коммерческой тайны наносят колоссальный вред экономике предприятий [1, 2]. Наряду с внешними дестабилизирующими факторами любое предприятие несет внутренние риски, связанные с действиями сотрудников.

В обзорной работе [3] подчеркивается роль преднамеренных и непреднамеренных действий сотрудников в повышении числа инцидентов, связанных с экономической безопасностью. Для снижения данных рисков на этапе отбора кандидатов и мониторинга состояния сотрудников применяются различные методы оценки, позволяющие оценить наличие или отсутствие у персонала необходимых для работы компетенций, наиболее подходящих для конкретной должности индивидуальных черт и социально-психологических качеств личности или, напротив, опасных психологических свойств и фактов деятельности [4–8].

Закономерно, что именно эффективное обеспечение кадровой безопасности эксперты относят к одному из самых приоритетных направлений, обеспечивающих стабильность развития и конкурентное преимущество для предприятий, а в масштабах экономической системы государства в целом – базу для развития экономики [1].

Требования к данным

Для большинства российских компаний проблема внедрения системы оценки и обеспечения кадровой безопасности является первоочередной. Система кадровой безопасности предприятия невозможна без системы оценки благонадежности сотрудников и имеет большое значение для предприятия, поскольку делает их поведение вполне предсказуемым и безопасным. Но при этом не следует забывать, что благонадежность является динамичным процессом, подверженным влиянию внутренних и внешних факторов.

При количественном изучении вопросов экономической безопасности используют различные методики. Успешно применяются обобщенные коэффициенты [9], используется SWOT-анализ [10].

Однако на сегодняшний день отсутствуют методики для оценки персонала. В различных отраслях используются разные методы для оценки персонала, но основные среди них – психологическое тестирование и собеседование. Классифицируются методы в группы по отраслям (табл. 1).

Таблица 1

Критерии, применяемые для оценки кандидатов в методиках оценки персонала

№	Критерии	Методы, применяемые			
		в банковской системе и на биржах	в космической отрасли	на производственных предприятиях	в атомной промышленности
1	Интеллектуальный потенциал	+	+	+	+
2	Профессионализм	+	+	+	+
3	Честность	+	+	+	+
4	Творческий потенциал (креативность)	+	+	+	+
5	Межличностные отношения	+	+	+	+
6	Уровень образования	+	+	+	+
7	Благонадежность сотрудника	+	–	–	–

1. Методики, применяемые в банковской системе и на биржах [11]. Цель данных методик – выбор самого честного кандидата. Основу методики составляет психологическое тестирование, направленное на оценку потенциала и профессиональной пригодности будущего сотрудника (интеллектуальные тесты,

личностные тесты, профессиональные (специальные) тесты).

2. Вторая группа методик была разработана для должностей, связанных с освоением космоса [12]. Первоначальной целью данных методик является выбор самых умных и способных кандидатов, а затем исключение внутренних и внешних угроз по отношению к безопасности предприятия (абсолютной безопасности). Используются интеллектуальные и личностные тесты.

3. Третья группа методик была разработана для оценки персонала производственных предприятий [13]. Первоначальная цель данных методик – определение самого талантливого кандидата. Сфера применения – производство электронных приборов и развития рынка. Используются профессиональные (специальные) тесты, личностные тесты, тесты на межличностные отношения.

4. Четвертая группа методик направлена на оценку персонала в атомной промышленности [14]. Особенностью данных методик являются высокий уровень секретности и обеспечения информационной безопасности.

Анализ данных методик показывает, что они используют, как правило, только психологические тесты и не позволяют дать полную оценку кандидата. Оценка благонадежности не проводится, лишь в банковской системе имеются скоринговые методы для ее оценки.

Сегодня государство отводит большую роль предприятиям, имеющим объекты критической информационной инфраструктуры (КИИ). Такие объекты есть во всех вышеназванных отраслях. Следовательно, необходима новая методика, которая дополнит уже существующие, но будет и отличаться от них. Кроме этого, необходимо обратить внимание, что методика должна отражать не только особенности и специфику компании, но и особенности функционала каждой конкретной должности в организации.

Основы методики

Под кадровой безопасностью будем понимать систему предприятия, связанную с эффективной работой персонала и функционированием организации (предприятия) в условиях безопасности и направленную на развитие самой организации в целом и каждого сотрудника в отдельности [15, 16].

Процедура оценки сотрудников, имеющих отношение к КИИ, включает соответствие необходимой квалификации занимаемой должности и соответствующему профессиональному стандарту. В рамках кадровой безопасности предприятия большая роль отводится не только профессиональным компетенциям, но и личным, компетенциям безопасности, социально-психологическим и компетенциям будущего. Особую важность в данном процессе представляет качественная оценка сотрудников. В данном случае речь идет не только о выявлении фактического уровня профессиональных компетенций, но и получении представлений о психологических характеристиках сотрудника, его «soft skills» или «self skills». Также важными для обеспечения кадровой и экономической безопасности являются оценка поведенческих компетенций, исключение негативных форм проявления в процессе трудовой деятельности.

Разработанная в рамках рекомендательной системы кадровой безопасности предприятия методика основана на составлении профиля компетенций для каждой конкретной должности [15, 16]. Структура компетенций включает в себя следующие основные блоки компетенций: личные, профессиональные, корпоративные, безопасности, специальности, будущего, поведенческие, социально-психологические, успешности.

В методике используются различные методы: метод анкетирования, оценки компетенций, автоматизированные методы оценки, метод тестирования, кейс-метод, собеседование, интервью. Метод оценки по компетенциям представляет собой процесс, направленный на сравнение компетенций отдельного сотрудника с разработанной эталонной моделью. Данный метод позволяет на всех этапах работы осуществлять системную оценку сотрудника в соответствии с выбранными ключевыми компетенциями, в наибольшей степени сказывающимися на качестве трудового процесса.

Анкетирование позволяет получить от кандидата ряд сведений, имеющих значение для определения его профессиональной пригодности к данной должности. Интервью, собеседование являются самыми распространенными методами оценки персонала с целью выявления компетенций, необходимых для успешной работы на конкретной должности.

Автоматизированные методы оценки набирают все большую популярность. Данный факт объясняется существенным снижением издержек проведения процедуры оценки, благодаря исключению из процесса сотрудников, занятых управлением персоналом. Еще одним существенным плюсом является возможность проходить оценку дистанционно, что особенно актуально в современных условиях пандемии и удаленной работы.

Система кадровой безопасности предприятия представляет собой программный комплекс [16], состоящий из трех модулей: анкетирование, тестирование и кейсы. По итогам прохождения каждого модуля определяется уровень благонадежности.

Градация оценки делится на «высокий», «средний» и «низкий» уровень благонадежности. Коэффициент «высокого» уровня находится в диапазоне от 0,75 до 1, «среднего» от 0,45 до 0,74, и «низкого» – соответственно от 0 до 0,44. Для прохождения на следующий этап необходимо обладать уровнем благонадежности выше 0,44. В рамках рекомендательной системы для дальнейшей работы рассматривается сотрудник с уровнем благонадежности не ниже 0,45. Сотрудник с «низким» уровнем благонадежности для прохождения дальнейших этапов не допускается. Сотрудник со «средним» уровнем благонадежности может быть принят на работу при условии дальнейшей работы над его «слабыми» сторонами с целью повы-

шения уровня его благонадежности. Сотрудник с «высоким» уровнем благонадежности однозначно проходит на следующий этап. Для обеспечения кадровой безопасности сотрудникам необходим средний и высокий уровень благонадежности.

Таблица 2

Оценки компетенций

Компетенция	Оценка по модели компетенций	Оценка предприятия	Оценка, полученная при использовании системы кадровой безопасности предприятия
Командная работа	4	2	0,6
Ответственность	3	1	0,6
Коммуникативные компетенции	4	3	0,67
Дисциплина	4	2	0,67
Лояльность	4	2	0,67
Клиентоориентированность	3	2	0,67
Стрессоустойчивость	3	3	0,7
Лидерские компетенции	4	3	0,7
Организаторские способности	3	1	0,7
Внимательность	4	3	0,7
Эмоциональный интеллект	4	2	0,73
Способность принимать решения	4	2	0,75
Аналитическое мышление	5	3	0,75
Способность к обучению	4	3	0,8
Критическое мышление	5	3	0,8
Гибкость	5	2	0,83
Мобильность	5	3	0,83
Высокий уровень памяти	5	3	0,83
Способность абстрагироваться	5	3	0,83
Мотивация успеха	5	3	0,87
Способность быстро реагировать	3	1	0,87
Способность к концентрации и усидчивости	5	3	0,9
Практикоориентированность	5	2	0,9
Тактичность	5	3	0,9
Пространственное мышление	5	3	0,9
Способность к самообладанию	5	3	0,92

Обсуждение результатов

В результате апробации разработанной рекомендательной системы были выбраны предприятия, имеющие объекты КИИ. Для сотрудников вначале были разработаны профили компетенций к должностям, являющиеся критически важными для предприятия или несущие актуальные риски кадровой безопасности. Были выделены 4 категории должностей, занятых на объектах КИИ: пользователь, обслуживающий персонал объекта КИИ, системный администратор, администратор безопасности.

Для того чтобы охарактеризовать качество полученных оценок, необходимо осуществить проверку их согласованности. Для этого из общего множества результатов были выбраны компетенции, прошедшие оценку по трем методам (табл. 2).

Поскольку представленные данные не соответствуют нормальному распределению и при этом шкалы оценок имеют различные шаги, в работе был применен непараметрический коэффициент конкордации Кендалла [17]. В качестве нулевой гипотезы обозначим h_0: W = 0 – оценки, полученные разными методами, не согласованы, при альтернативной гипотезе h_1: W ≠ 0. Далее указание компетенций в таблицах опущено, поскольку не имеет значения для определения коэффициента конкордации (табл. 3).

Таблица 3

Расчет коэффициента конкордации

Оценка по модели компетенций	Оценка предприятия	Оценка, полученная при использовании системы кадровой безопасности предприятия	d_i	D_i	D_i^2
10	7,5	1,5	19	–21,5	462,25
3	2	1,5	6,5	–34	1156
10	19	4,5	33,5	–7	49
10	7,5	4,5	22	–18,5	342,25
10	7,5	4,5	22	–18,5	342,25
3	7,5	4,5	15	–25,5	650,25
3	19	8,5	30,5	–10	100
10	19	8,5	37,5	–3	9
3	2	8,5	13,5	–27	729
10	19	8,5	37,5	–3	9
10	7,5	11	28,5	–12	144
10	7,5	12,5	30	–10,5	110,25
20,5	19	12,5	52	11,5	132,25
10	19	14,5	43,5	3	9
20,5	19	14,5	54	13,5	182,25
20,5	7,5	17,5	45,5	5	25
20,5	19	17,5	57	16,5	272,25
20,5	19	17,5	57	16,5	272,25
20,5	19	17,5	57	16,5	272,25
20,5	19	20,5	60	19,5	380,25
3	2	20,5	25,5	–15	225
20,5	19	23,5	63	22,5	506,25
20,5	7,5	23,5	51,5	11	121
20,5	19	23,5	63	22,5	506,25
20,5	19	23,5	63	22,5	506,25
20,5	19	26	65,5	25	625

Коэффициент конкордации Кендалла для случая связанных рангов вычисляется по формулам:

$$W = \frac{12\sum_{i=1}^{n} D_i^2}{m^2(n^3-n) - m\sum_{j=1}^{m} T_j}, \qquad (1)$$

$$T_j = \sum_{k=1}^{l} t_k^3 - t_k \,, \quad (2)$$

$$D_i = d_i - \bar{d}, \quad (3)$$

$$\bar{d} = \frac{1}{n}\sum_{i=1}^{n} d_i \,, \quad (4)$$

$$d_i = \sum_{j=1}^{m} R_{ij} \,, \quad (5)$$

где t_k – число одинаковых значений в k-й группе (связке), l – число связок в ранговой последовательности j-го эксперта, n – число исследуемых объектов, m – количество экспертов.

Далее была рассчитана сумма корректирующих членов:

$$T_1 = (9^3 - 9) + (5^3 - 5) + (12^3 - 12) = 2556,$$

$$T_2 = (8^3 - 8) + (3^3 - 3) + (15^3 - 15) = 3888,$$

$$T_3 = 4(2^3 - 2) + 4(4^3 - 4) = 264,$$

$$\sum_{j=1}^{m} T_j = 2556 + 3888 + 264 = 6708. \quad (6)$$

Исходя из полученных данных, произведен расчет коэффициента конкордации Кендалла:

$$W = \frac{12\sum_{i=1}^{n} D_i^2}{m^2(n^3 - n) - m\sum_{j=1}^{m} T_j} = 0,70859, \quad (7)$$

$$\chi_p^2 = W(n-1)m = 53,14418. \quad (8)$$

Для проверки значимости коэффициента конкордации произведены расчет эмпирического значения критерия Пирсона χ^2 и его сравнение с табличными значениями (табл. 4).

Таблица 4

Определение значимости расчётного значения критерия Пирсона

Степень свободы $k = n - 1$	Уровень значимости α	χ_T^2	Значимость χ_p^2
25	0,05	37,65248	Значим
25	0,01	44,31410	Значим

Исходя из приведенных расчетов, исследуемый критерий значим, альтернативная гипотеза о наличии согласованности оценок по примененным методам оценки подтверждается и согласованность определяется как высокая.

Данный факт свидетельствует о достаточной валидности оценок. Таким образом, применение методов, используемых в системе кадровой безопасности предприятия, является допустимым, поскольку была показана их согласованность с оценкой компетенций, проводимой по фактическим результатам деятельности сотрудников.

Таким образом, основу кадровой безопасности составляет персонал предприятия, а именно компетентные и добросовестные сотрудники с высоким уровнем благонадежности. Оценка по данной системе является необходимой особенно для сотрудников, работающих на объектах КИИ.

Литература

1. Духновский С.В. Кадровая безопасность организации: учеб. и практикум для академического бакалавриата. – М.: Юрайт, 2019. – 245 с

2. Mugellini G. Employee offences: What strategy of prevention for what business? / G. Mugellini, G. Isenring, M. Killias // Security Journal. – 2017. – Vol. 30, No. 3. – P. 825–843.

3. Khando K. Enhancing employees information security awareness in private and public organisations: a systematic literature review / K. Khando, S. Gao, S. Islam, A. Salman // Computers and Security. – 2021. – Vol. 106. – P. 102267. – DOI: 10.1016/j.cose.2021.102267

4. Хрусталева С.П. Алгоритмы противодействия экономическим преступлениям и оценка уровня угроз экономической безопасности в контексте стратегического управления / С.П. Хрусталева, О.О. Шендрикова, К.С. Кривякин, М.С. Луценко // Вестник ВГУИТ. – 2019. – Т. 81, № 4. – С. 280–290.

5. Frempong L.N. The impact of job satisfaction on employees' loyalty and commitment: A comparative study among some selected sectors in Ghana / L.N. Frempong, W. Agbenyo, P.A. Darko // European Journal of Business and Management. – 2018. – Vol. 10, No. 12. – P. 95–105.

6. Nurliza N. A study on the effects of innovation marketing process for Indonesian SMEs' in food and beverage sector / N. Nurliza, W. Fitrianti // Fitrianti Management Science Letters. – 2021. – Vol. 11. – P. 1747–1754.

7. Egenius S. The Effect of Job Satisfaction on Employee Performance Through Loyalty at Credit Union (CU) Corporation of East Kutai District, East Kalimantan / S. Egenius, B. Triatmanto, N. Boge, M. Natsir // International Journal of Multicultural and Multireligious Understanding. – 2020. – Vol. 7. – P. 480. – DOI: 10.18415/ijmmu.v7i10.1891

8. Andrews S. Tackling Financial and Economic Crime through Strategic Intelligence: The EMPRISES Framework / S. Andrews, S. Polovina, S. Yates, B. Akhgar, P. Bayerl // The 2013 International Conference on Information and Knowledge Engineering (IKE 2013). – Las Vegas, USA: CSREA Press, 2013. – P. 114–118.

9. Roxas M.L. Financial Statement Fraud Detection Using Ratio and Digital Analysis // Journal of Leadership, Accountability, and Ethics. – 2011. – Vol. 8. – P. 56–66.

10. Krokhicheva G., Mezentseva Iu., Tian Yu. Corporate fraud as a threat to the company's economic security / G. Krokhicheva, I. Mezentseva, Y. Tian // International Conference on Economics, Management and Technologies (ICEMT 2021). – 2021. – P. 110. – DOI: 10.1051/shsconf/202111004011

11. Судакова Е.С. Управление развитием трудового потенциала персонала финансовых организаций: дис. … канд. экон. наук. – М.: Гос. ун-т управления, 2014. – 220 с.

12. Подвербных О.Е. Профессиональные стандарты в оценке персонала ракетно-космического предприятия / О.Е. Подвербных, А.И. Тихонов, С.Г. Кукушкин // Московский экономический журнал. – 2018. – № 5 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/professionalnye-standarty-v-otsenke-personala-raketno-kosmicheskogo-predpriyatiya, свободный (дата обращения: 05.12.2021).

13. Борисова Е.А. Оценка и аттестация персонала. – СПб.: Питер, 2002. – 288 с.

14. Карякин А.М. Развитие методов оценки профессиональной деятельности персонала / А.М. Карякин, А.В. Юникова // Изв. вузов ЭФиУП. – 2016. – № 4 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/razvitie-metodov-otsenki-professionalnoy-deyatelnosti-personala, свободный (дата обращения: 05.12.2021).

15. Глухарева С.В. Методика подбора персонала на должности, связанные с обработкой конфиденциальной информации // Безопасность информационного пространства – 2017: XVI Всерос. науч.-практ. конф. студентов, аспирантов, молодых ученых. Екатеринбург, 12 декабря 2017 г. – Екатеринбург: Изд-во Урал. ун-та, 2018. – С. 154–158.

16. Св-во о рег. программы для ЭВМ RU 2019616940, 30.05.2019. Система кадровой безопасности предприятия / С.В. Глухарева, А.А. Шелупанов, Е.В. Мареева, М.Е. Абросимова, А.С. Еременко, В.Е. Мальцев. Заявка № 2019616011 от 24.05.2019.

17. Knight W.A. Computer Method for Calculating Kendall's Tau with Ungrouped Data // Journal of the American Statistical Association. – 1996. – Vol. 61, No. 314. – P. 436–439.

Шелупанов Александр Александрович
Д-р техн. наук, проф., президент
Томского государственного университета
систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 90-71-55
Эл. почта: saa@tusur.ru

Глухарева Светлана Владимировна
Ст. преп. каф. комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)
ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-913-889-48-42
Эл. почта: gsv@fb.tusur.ru

Немирович-Данченко Михаил Михайлович
Д-р физ.-мат. наук, проф. каф. КИБЭВС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-906-199-99-95
Эл. почта: michnd@mail.ru

Shelupanov A.A., Glukhareva S.V.,
Nemirovich-Danchenko M.M.

Assessment of employee reliability in the human resources of the enterprise

The paper provides an assessment of the employee's reliability in the personnel security system of the enterprise. The analysis of existing solutions in various industries is carried out. The stages of assessment and levels of trustworthiness are shown.

Keywords: personnel security, reliability assessment, decision making, CII facilities.
DOI: 10.21293/1818-0442-2021-24-4-52-57

References

1. Dukhnovsky S.V. *Kadrovaja bezopasnost organsazii* [Personnel security of the organization] textbook and workshop for academic undergraduate. Moskow, Yurayt, 2019, 245 p. (in Russ.).

2. Mugellini G., Isenring G. L., & Killias M. [Employee offences: What strategy of prevention for what business?] *Security Journal,* 2017, vol. 30, no. 3, pp. 825–843.

3. Khando K., Gao S., Islam, S.M. and Salman A. [Enhancing employees information security awareness in private and public organisations: a systematic literature review], *Computers and Security,* 2021, vol. 106, p. 102267. Available at: https://doi.org/10.1016/j.cose.2021.102267, free (Accessed: December 1, 2021).

4. Khrustaleva S.P., Krivyakin K.S., Lutsenko M.S. Shendrikova O.O. *Algoritmi protivodeistvija economiseskim prestuplenijam i ocenka urovnja ugroz economiseskoi bezopasnosti v kontexte strategiseskogo upravlenija* [Algorithms for countering economic crimes and assessing the level of threats to economic security in the context of strategic management]. *Vestnik Proceedings of the Voronezh State University of Engineering Technologies*, 2019, vol. 81, no. 4, pp. 280–290 (in Russ.).

5. Frempong L.N., Agbenyo W., Darko P.A. [The impact of job satisfaction on employees' loyalty and commitment: A com-parative study among some selected sectors in Ghana]. *European Journal of Business and Management*, 2018, vol. 10, no. 12, pp. 95–105.

6. Nurliza N., Fitrianti W., Pamela P. [A study on the effects of innovation marketing process for Indonesian SMEs' in food and beverage sector]. *Management Science Letters, 2021*. Vol. 11, pp. 1747–1754. DOI: 10.5267/j.msl.2021.2.008.

7. Egenius S., Triatmanto B., Natsir M. [The Effect of Job Satisfaction on Employee Performance Through Loyalty at Credit Union (CU) Corporation of East Kutai District, East Kalimantan]. *International Journal of Multicultural and Multireligious Understanding*, 2020, vol. 7, pp. 480. DOI: 10.18415/ijmmu.v7i10.1891

8. Andrews S., Polovina S., Yates S., Akhgar B., Bayerl P.S. [Tackling Financial and Economic Crime through Strategic Intelligence: The EMPRISES Framework]. *The 2013 International Conference on Information and Knowledge Engineering* (IKE 2013), Las Vegas, USA, CSREA Press, 2013, pp. 114–118.

9. Roxas M.L. [Financial Statement Fraud Detection Using Ratio and Digital Analysis]. *Journal of Leadership*, *Accountability, and Ethics,* 2011, no 8, pp. 56–66.

10. Krokhicheva G., Mezentseva I., Tian Y. [Corporate fraud as a threat to the company's economic security]. *International Conference on Economics, Management and Technologies*, 2021, vol. 110.

11. Sudakova E.S. *Upravlenie razvitiem trudovogo potenziala personala finansovih organizazii* [Management of the development of the labor potential of the personnel of financial organizations]. Diss. on the receipt of the academic degree of Candidate of Economic Sciences. Moscow, State University of Management, 2014, 220 p. (in Russ.).

12. Podverbnykh O.E., Tikhonov A.I., Kukushkin S.G. *Professionalnie standarti v ocenke personala raketno-kosmiseskogo predprijatija* [Professional standards in personnel evaluation of a rocket and space enterprise]. *Moscow Economic Journal,* 2018, vol. 5, no 2. Available at: https://cyberleninka.ru/article/n/professionalnye-standarty-v-otsenke-personala-raketno-kosmicheskogo-predpriyatiya, free (Accessed: December 1, 2021) (in Russ.).

13. Borisova E.A. *Ocenka I attestazija personala* [Evaluation and certification of personnel]. St. Petersburg: Peter, 2002. 288 p. (in Russ.).

14. Karyakin A.M., Yunikova A.V. *Rasvitie metodov ocenki professionalnoi dejatelnosti personala* [Development of methods for assessing the professional activity of personnel]. *Proceedings of Universities of Ethiopia,* 2016, vol. 4, no. 30. Available at: https://cyberleninka.ru/article/n/razvitie-metodov-otsenki-professionalnoy-deyatelnosti-personala, free (Accessed: December 1, 2021) (in Russ.).

15. Glukhareva S.V. *Metodika podbora personala na dolshnosti, svjazannie sobrabotkoi konfidenzialnoi informazijei* [Methods of personnel selection for tasks related to the processing of confidential information]. *Security of the Information Space.* XVI All-Russian Scientific and Practical Conference of students, postgraduates, young scientists. Yekaterinburg, 2017. Ural University Publishing House, 2018, pp. 154–158 (in Russ.).

16. Certificate of registration of the computer program RU 2019616940, 30.05.2019. *Sistema kadrovoi bezopasnosti predprijatija* [Personnel security system of the enterprise] / Glukhareva S.V., Shelupanov A.A., Mareeva E.V., Abrosimova M.E., Eremenko A.S., Maltsev V.E. Application no. 2019616011, dated 24.05.2019 (in Russ.).

17. Knight W.A. [Computer Method for Calculating Kendall's Tau with Ungrouped Data]. *Journal of the American Statistical Association,* 1996, vol. 61, no 314, pp. 436–439. DOI: 10.2307/2282833. JSTOR 2282833.

Alexandr A. Shelupanov
Doctor of Science in Engineering, Professor,
President, Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 90-71-55
Email: saa@tusur.ru

Svetlana V. Glukhareva
Senior Lecturer, Department of Complex Information
Security of Computer Systems, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-913-889-48-42
Email: gsv@fb.tusur.ru

Mikhail M. Nemirovich-Danchenko
Doctor of Science in Physics and Mathematics, Professor,
Department of Complex Information Security
of Computer Systems TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: https://orcid.org/0000-0002-4510-8045
Phone: +7-906-199-99-95
Email: michnd@mail.ru

УДК 621.396.41

С.А. Землянский, С.В. Аксёнов, И.А. Лызин, О.Г. Берестнева

Тематическое моделирование в контексте медицинских текстов

Анализ текста – это важная область исследований, которая включает в себя несколько направлений, таких как информационный поиск, извлечение информации и категоризация текста. Анализ текста широко используется в области медицинских исследований из-за количества ежедневно публикуемых исследований, которые могут быть обработаны с такой скоростью только с помощью вычислительных ресурсов. В данной работе представлены результаты эксперимента по тематическому моделированию корпуса статей из базы данных PubMed с 2000 по 2020 г.

Ключевые слова: науки о здоровье, анализ текстов, латентное распределение Дирихле, научно-исследовательские тенденции, картирование знаний, обобщение знаний, PubMed.
DOI: 10.21293/1818-0442-2021-24-4-58-64

Ежегодно в области здравоохранения публикуется огромное количество исследований [1]. Однако нельзя сказать, что эта область полностью сформирована и может быть описана в терминах фиксированных определений, концепций и областей исследования [2] – это сильно затрудняет обработку и категоризацию всей генерируемой информации.

Чтобы преодолеть эти ограничения, в настоящее время для частичной автоматизации этого процесса используются современные вычислительные методы, такие как машинное обучение, а именно: интеллектуальный анализ текста (text mining), классификация текстов (text classification) и тематическое моделирование (topic modelling) [3]. Последнее предлагает вычислительный инструмент для автоматического поиска релевантных тем путем выявления значимой структуры среди коллекций документов [1]. В данной работе применен метод латентного размещения Дирихле (Latent Dirichlet Allocation, LDA) для автоматического определения тем в коллекции исследований из базы данных PubMed [4] за период с 2000 по 2020 г.

Тематическое моделирование

Огромное количество биомедицинских текстовых документов может служить важным источником информации для биомедицинских исследований. Биомедицинские текстовые документы характеризуются огромными объемами неструктурированной и разреженной информации в различных формах, таких как научные статьи, биомедицинские наборы данных и отчеты [5, 11].

В то же время выявление релевантных исследований для включения в систематические обзоры или для категоризации полученных знаний является сложной, трудоемкой и дорогостоящей задачей [3, 11]. Однако недавно ряд исследований [1, 2] показал, что использование методов машинного обучения и анализа текста для автоматического определения релевантных исследований и извлечения тем может значительно сократить объем ручной работы и существенно повысить ее качество. По этой причине автоматический тематический анализ в настоящее время набирает популярность в области анализа текста.

Анализ текста направлен на выявление ценной информации из неструктурированных текстовых документов с использованием инструментов и методов из нескольких дисциплин, таких как машинное обучение, информационный поиск и вычислительная лингвистика. Использование текстового анализа является одним из наиболее перспективных инструментов в биомедицинской области, который привлекает большой исследовательский интерес [5–9].

Тематическая модель описывает связи между словами и темами и таким образом выступает в качестве инструмента для обобщения и систематизации информации из больших текстовых коллекций, эта модель позволяет выявить скрытые структуры и неявные зависимости в данных. Тематическое моделирование широко используется при решении задач информационного поиска, автоматического аннотирования и индексирования документов, пополнения тоновых словарей, поиска классов переводческих эквивалентов, определения сопоставимости текстов в многоязычных корпусах текстов [6].

Анализ текста в биомедицинской области может успешно применяться для решения широкого круга задач, включая выявление знаний о конкретных заболеваниях, диагностику, лечение и профилактику рака, определение состояния ожирения у пациентов, выявление факторов риска сердечных заболеваний, аннотирование экспрессии генов и выявление мишеней и кандидатов в лекарственные препараты [5, 11].

Тематическая модель обычно определяется как подход для обнаружения скрытой информации в корпусе (hidden pattern) текстов [3].

Большинство методов обнаружения скрытой информации в совокупности текстов используют автоматическую или полуавтоматическую классификацию текстов [12]. Классификация текстов обычно выполняется с использованием модели «мешка слов» (bag-of-words, BOW). Эта модель предполагает, что слова в документах используются в качестве признаков для классификации, но их порядок игнорируется. Одна из проблем модели BOW заключается в том, что количество уникальных слов, которые появляются в полном корпусе документов,

может быть очень большим; использование такого большого количества признаков может быть проблематичным для некоторых алгоритмов. С другой стороны, существуют методы, позволяющие более компактно представлять документы. Например, LSA и LDA, а также улучшенная версия LDA-PTM (Parsimonious Topic Modeling) [5, 12].

Так, латентно-семантический анализ (LSA) использует сингулярное разложение (Singular Value Decomposition, SVD) для обнаружения семантической информации в корпусе текстов [3]. Этот метод сначала значительно снижает размерность матрицы слов до двух или трех измерений, затем определяет выпуклое множество этих слов. Слова в опорных точках рассматриваются как темы (topic, latent topic). Модель LDA (Latent Dirichlet Allocation, LDA), в свою очередь, использует модель распределения вероятностей для генерации тем [7]. Этот метод рассматривает отдельные темы как вероятностные распределения терминов, присутствующих в корпусе, или кластеры, которые определяют веса этих терминов [7].

Последняя описанная модель является своего рода стандартом во многих недавних исследованиях [2, 6, 8, 12, 15] и была выбрана нами для данного эксперимента.

Латентное размещение Дирихле

При проведении тематического моделирования наиболее широко используемыми в литературе методами обработки являются вероятностные тематические модели, включая LDA [9, 12]. LDA, или метод латентного размещения Дирихле, – это автоматический метод идентификации тем (в отличие от ручного или полуручного подхода) [9].

LDA является примером вероятностного метода моделирования тем, который предполагает, что документ охватывает ряд тем и каждое слово в документе выбирается из вероятностных распределений с различными параметрами. Каждое слово в LDA обозначается уникальным латентным вектором, указывающим на распределение, из которого оно взято [3]. Таким образом, документ содержит набор тем с различными вероятностями, а тема содержит набор слов с различными вероятностями.

Важным допущением модели LDA является гипотеза «взаимозаменяемости» (exchangeability), или «мешка слов», которая означает, что важность слова не связана с порядком его появления в документе, а скорее с частотой его появления [7]. Другим важным допущением этой модели является ненулевая вероятность принадлежности к теме для любого отдельного документа, что в сочетании с большим количеством скрытых параметров модели может приводить к переобучению [12].

Основным недостатком тематической модели LDA является то, что она не способна автоматически определять оптимальное количество тем для коллекции текстов; другими словами, количество тем является настраиваемым гиперпараметром и точное количество тем должно определяться пользователем модели.

Метод LDA осуществляет мягкую кластеризацию и предполагает, что каждое слово в документе порождено некоторой латентной темой, определяемой распределением вероятности на множестве всех слов в тексте.

В нашем исследовании, основываясь на высокой оценке эффективности этого метода в других исследованиях и общей универсальности метода, решено использовать именно этот алгоритм (LDA) для проведения тематического моделирования.

Выбор количества тем

Вероятностные модели, такие как LDA, предлагают алгоритмы для сопоставления коллекций сообщений с наборами ключевых слов, которые представляют основные темы. В этих подходах, однако, выяснение того, сколько конкретных тем представляют наборы ключевых слов, остается отдельной задачей [9]. В то же время определение количества тем имеет решающее значение для тематического моделирования [7].

Существуют различные метрики, используемые при выборе количества тем, наиболее популярными из которых можно считать сложность (perplexity), изолированность (isolation), стабильность (stability) и согласованность (coherence). Можно сказать, что любая хорошая метрика, используемая для выбора оптимального количества тем, при применении должна создавать тематическую модель со следующими свойствами: хорошая предсказательная сила, высокая изолированность между темами, отсутствие перекрывающихся тем и воспроизводимость. В данной работе авторами используется метрика согласованности для выбора оптимального количества тем для каждого корпуса текстов (для каждого года отдельно).

Метрика согласованности может быть описана следующим образом (1):

$$c(t, W_t) = \sum_{\omega_1, \omega_2 \in W_t} \ln \frac{d(\omega_1, \omega_2) + e}{d(\omega_1)}, \qquad (1)$$

где t – это тема, W_t – набор ключевых слов темы, $d(\omega_i, \omega_j)$ – количество документов, в которых встречаются ключевые слова ω_i, ω_j; $d(\omega_i)$ – количество документов, в которых встречается ключевое слово ω_i; ω_1 – первое ключевое слово темы, ω_2 – второе ключевое слово темы.

Методика выбора оптимального количества тем для набора текстов на основе этой метрики заключается в последовательном обучении моделей с разным количеством тем. Для каждой модели рассчитывается метрика согласованности терминов для каждого выбранного кластера текстов (тем), а затем полученные метрики усредняются по всем темам. Полученное значение запоминается. После обучения всех моделей со всеми желаемыми наборами параметров выбирается лучшая модель из тех, которые имеют наибольшую среднюю согласованность внутри тем.

В данной работе обучено 160 тематических моделей с разным количеством тем (от 2 до 10) по 8 для каждого корпуса текстов (всего 20 корпусов,

по 1 на каждый год), для каждой из этих моделей подсчитана метрика согласованности (coherence score) и выбрано оптимальное количество тем для каждой коллекции текстов. На рис. 1 ниже показано значение метрики связности для всех моделей и всех значений гиперпараметров.

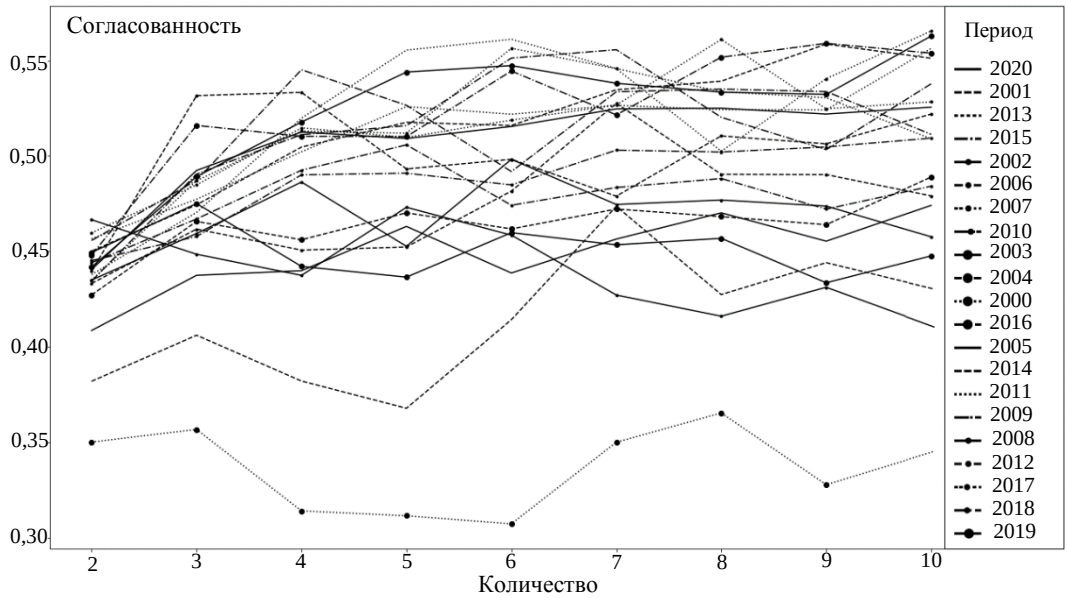

Рис. 1. Значение метрики согласованности для количества тем в модели для каждой коллекции текстов с 2000 по 2020 г.

На рис. 2 показано определенное количество тем в корпусах текстов.

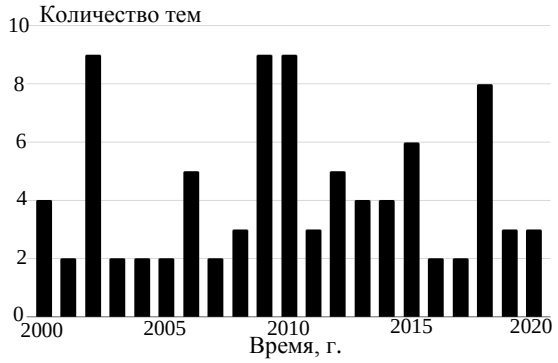

Рис. 2. Количество найденных тем в коллекциях текстов в период с 2000 по 2020 г.

Используемые данные

Входом практически любой тематической модели является корпус текстов, каждый из которых представляет собой отдельный документ. Результатом работы модели является список тем, выявленных в корпусе и представленных списком первых наиболее характерных слов для каждой рассматриваемой темы [6].

Для постановки эксперимента в данной работе были собраны аннотации статей из открытой базы данных PubMed за период с 2000 по 2020 г. При формировании корпуса текстов (в данной работе каждый временной период представлен как отдельный корпус текстов) использовался метод перекрестного включения [3]. Согласно этому методу, в корпусе текстов учитываются не только документы за исследуемый период, но и тексты, на которые ссылается работа. Таким образом, удалось собрать значительное количество записей (с повторами). Количество уникальных записей, в свою очередь, за каждый период времени показано ниже на рис. 3.

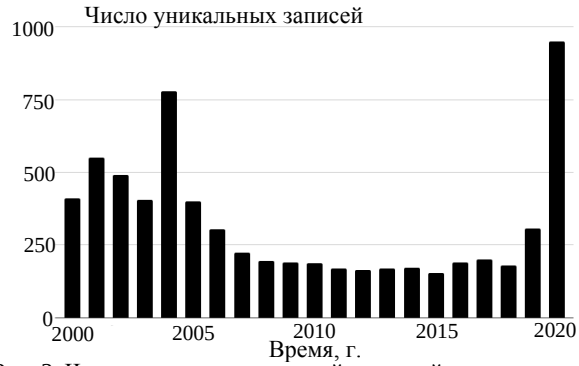

Рис. 3. Число уникальных записей в каждой из коллекции текстов в период с 2000 по 2020 г.

Предварительная обработка данных

Для того чтобы провести тематическое моделирование, собранные тексты были преобразованы в несколько этапов. Сначала были удалены знаки препинания и другие служебные символы. Далее была проведена лемматизация слов (lemmatisation), т.е. все словоформы всех наборов были приведены к лемме, другими словами, к словарной форме слова. После лемматизации были удалены часто используемые слова (также известные как «стоп-слова», stopwords), которые не вносят никакой качественной информации в рассматриваемый документ. Наконец, записи корпуса текстов были дополнены смысловыми биграммами, т.е. пары слов, образующие словосочетания, были идентифицированы и сгруппированы в единый набор значений (лексем).

Все перечисленные этапы обработки текста являются стандартными [12] и хорошо описанными этапами подготовки неструктурированных текстовых данных. Преобразование словоформ в леммы значительно снижает размерность, а удаление часто используемых слов также снижает уровень шума. Преобразование пар лексем, образующих словоформу, в одну лексему также считается обязательной процедурой для обеспечения более точного семантического представления [3]. Несмотря на глубину разработки проблемы предобработки текстовых данных [7, 9–10], многие вопросы до сих пор остаются открытыми. Например, в [6] исследователи предлагают не только объединять пары слов, составляющих фразу, в единый семантический токен, но и более широко использовать метод *n*-грамм, другими словами, использовать при построении модели биграммы и триграммы всех пар слов. Несмотря на значительные теоретические преимущества такого подхода, нельзя сказать, что использование наборов *n*-грамм решает проблему «мешка слов» в моделях вероятностного тематического моделирования, но значительно увеличивает размерность отдельной записи.

В данной работе было решено следовать только стандартной процедуре обработки для подготовки собранных аннотаций статей к дальнейшему тематическому моделированию.

Обучение тематической модели

Как уже упоминалось выше, для проведения качественного тематического моделирования с использованием метода латентного размещения Дирихле перед проведением обучения необходимо установить количество тем в исследуемом наборе данных. Однако, как уже отмечалось, область научных исследований, особенно медицинских, не может быть определена конечным набором направлений исследований. Таким образом, количество тем в наборе текстов не может быть определено заранее. Решением проблемы выбора количества тем становится метод последовательного оценивания модели при подборе гиперпараметров.

Для проведения тематического моделирования был использован пакет для интеллектуального анализа текстов Gensim [10, 12], обучали каждую тематическую модель отдельно от других «по сетке» из 8 значений гиперпараметров от 2 до 10 возможных тем для набора. После обучения всех моделей выбиралась лучшая модель для данного набора данных на основе учета метрики согласованности.

Другие параметры модели были одинаковыми для всех итераций для всех коллекций документов, а именно: количество эпох обучения составляло десять итераций, использовалось итеративное, а не пакетное обучение, также использовался параметр, позволяющий модели самой настраивать параметры априорного распределения вероятностей. Все остальные параметры были оставлены по умолчанию.

При построении графиков «облака слов» ключевые слова были отфильтрованы по частоте во время обучения модели, так что наиболее часто используемые слова с частотой более 50% во всех документах корпуса не учитывались.

Результаты

В вероятностном тематическом моделировании предполагается, что документы представляют собой мультиномиальную смесь латентных тем, а темы представлены в виде распределения вероятности по количеству слов.

Таким образом, LDA разделяет связанные слова на наборы, которые рассматриваются как темы. Однако определение основной концепции, связанной с наборами слов, полученными автоматически, обычно требует дополнительного – возможно, ручного – анализа [9, 11]. Поэтому в данной работе, как и во многих других [1, 8], необходимо вручную дополнить полученные результаты названиями тем после выполнения тематического моделирования. Список определенных тем в соответствии с ключевыми словами, рассчитанными обученной моделью для каждого периода, можно найти в таблице.

Распределение тем среди коллекций

Период	Темы, определённые из набора ключевых слов
2000	positive trends (increased rates), patient survival, data analysis/modeling, vaccine research
2001	positive trends (increased rates), patient survival
2002	positive trends (increased rates), water control, patient survival, data analysis/modeling, disability, clinical trials, surgery, mortality, production costs
2003	positive trends (increased rates), data analysis / modeling
2004	positive trends (increase in rates), patient survival
2005	positive trends (increased rates), patient survival,
2006	positive trends (increased rates), patient survival, data analysis/modeling, vaccine research, plants, cancer
2007	positive trends (increased rates), patient survival, water and plants
2008	positive trends (increased rates), patient survival, water, data analysis/modeling, cancer
2009	plants, national programs, positive trends (increased rates), production costs, data analysis/modeling, mortality, infection, vaccine research
2010	data analysis/modeling, positive trends (increased rates), water and plants, health workers/health system, clinical trials, mortality
2011	data analysis/modeling, positive trends (increased rates), mortality, viruses/ infection, plants
2012	data analysis/modeling, positive trends (increased rates), plants,viruses/ infection, population number
2013	infection, mortality, cancer, surgery, injury, production costs, databases
2014	health system, drugs, infection, data analysis
2015	health system, infection, data analysis, statistics, clinical trials
2016	positive trends (increased rates), plants and water, infection
2017	plants, population, positive trends (increased rates), data analysis
2018	health system, vaccine research, cancer drugs, population/region, data analysis, cancer, infection/virus, plants, clinical trials
2019	positive trends (increased rates), data analysis, patient survival, infection, covid, vaccine, population, health system
2020	positive trends (increased rates), population/region, surgery, data analysis, mortality, virus

Примечание: При выполнении работы использованы данные из открытой базы PubMed (в этой базе данные на англ. яз.).

Выводы

Метод тематического моделирования очень эффективен для извлечения знаний, содержащихся в неструктурированных больших данных, и широко используется в анализе биологических и медицинских документов [1–4, 8, 9, 11, 12]. Однако, как и при всех подходах к анализу текста, возникают трудности с интерпретацией и субъективной проверкой, поскольку вся информация, содержащаяся в этих документах (которая может содержаться), и количество релевантных тем априори неизвестны. Была определена лучшая модель, используя метод, основанный на вычислении метрики согласованности. Однако общее количество тем остается неизвестным и зависит от разумных умозаключений.

В данной работе использовался алгоритм LDA – вычислительный подход к тематическому моделированию без учителя (unsupervised task) для автоматического определения тем в коллекции текстов исследований. Это позволило извлечь ключевые термины и темы из огромного массива литературы в основном автоматическим способом. Таким образом, в данной работе можно проследить эволюцию тем исследований от прошлого к настоящему в портале PubMed, представлены результаты вместе с использованным подходом. В таблице показаны темы, извлеченные из набора ключевых слов для каждого корпуса текстов, на рис. 4, 5 представлены графики облаков ключевых слов за весь период и за 2018–2020 гг.

Рис. 4. Облако ключевых слов за весь период

На основании полученных результатов можно сделать вывод, что вероятностные автоматические модели для извлечения тем из корпуса текстов имеют один недостаток: большинство моделей сильно зависят от настройки гиперпараметров, а не от содержания корпуса. В то же время можно получить одинаковые результаты при различных уровнях частотной фильтрации. Тем не менее из полученных в результате экспериментов данных можно сделать выводы о соответствии определенных глобальных тем известным событиям (например, см. ключевое слово – «covid»); также можно наблюдать микроэволюцию тем, например «анализ данных и моделирование», которые со временем трансформируются в «анализ данных и базы данных», что можно связать с ростом информации в целом.

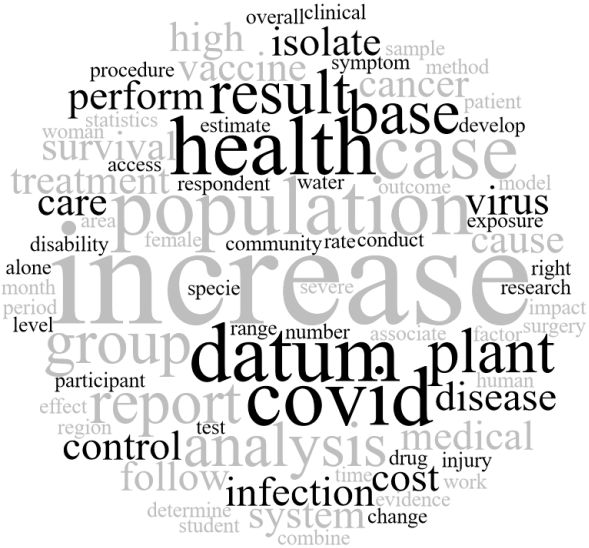

Рис. 5. Облако ключевых слов за 2018–2020 гг.

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках выполнения научного проекта № 19-37-90005.

Литература

1. Wang S.-H. Text mining for identifying topics in the literatures about adolescent substance use and depression / S.-H. Wang, Y. Ding, W. Zhao, Y.-H. Huang, R. Perkins, W. Zou, J. J. Chen // BMC public health. – 2016. – No. 16. – P. 279.

2. Cho S.M. The evolution of social health research topics: A data-driven analysis / S.M. Cho, C. Park, M. Song. – Social Science & Medicine. – 2020. – (265). – P. 113299.

3. Mo Y. Supporting systematic reviews using LDA-based document representations / Y. Mo, G. Kontonatsios, S. Ananiadou // Systematic reviews. – 2015. – No. 4. – P. 172.

4. PubMed: National Library of Medicine [Электронный ресурс]. – Режим доступа: https://pubmed.ncbi.nlm.nih.gov/, свободный (дата обращения: 16.12.2021).

5. Onan A. Biomedical Text Categorization Based on Ensemble Pruning and Optimized Topic Modelling // Computational and mathematical methods in medicine. – 2018. – P. 1–22.

6. Седова А. Тематическое моделирование русскоязычных текстов с опорой на леммы и лексические конструкции / А. Седова, О. Митрофанова // Компьютерная лингвистика и вычислительные онтологии. – 2018. – С. 132–144.

7. Gan J. Selection of the Optimal Number of Topics for LDA Topic Model-Taking Patent Policy Analysis as an Example / J. Gan, Y. Qi // Entropy (Basel, Switzerland). – 2021. – № 10 (23). – P. 1301.

8. Chandrasekaran R. Topics, Trends, and Sentiments of Tweets About the COVID-19 Pandemic: Temporal Infoveillance Study / R. Chandrasekaran V. Mehta, T. Valkunde, E. Moustakas // Journal of medical Internet research. – 2020. – № 10 (22). – P. e22624.

9. Yıldırım A. Identifying Topics in Microblogs Using Wikipedia / A. Yıldırım, S. Üsküdarlı, A. Özgür // PloS one. – 2016. – № 3 (11). – P. e0151885.

10. Rehurek R. Gensim-python framework for vector space modelling / R. Rehurek, P. Sojka // NLP Centre, Faculty of Informatics – Masaryk University, Brno, Czech Republic. – 2011. – № 2 (3). – P. 46–49.

11. Вафин Р.Р. Актуальные проблемы в области извлечения знаний из профессиональных медицинских текстов с применением интеллектуального анализа текста // Вестник Башкирского гос. мед. ун-та. – 2019. – С. 72–75.

12. Min J.-Y. Mining Hidden Knowledge About Illegal Compensation for Occupational Injury: Topic Model Approach / J.-Y. Min, S.-H. Song, H. Kim, K.-B. Min // JMIR medical informatics. – 2019. – № 3 (7). – P. e14763.

13. Wang H. Improved Parsimonious Topic Modeling Based on the Bayesian Information Criterion / H. Wang, D. Miller // Entropy (Basel, Switzerland). – 2020. – № 3 (22). – P. 326.

14. Liu L. An overview of topic modeling and its current applications in bioinformatics / L. Liu, L. Tang, W. Dong, S. Yao, W. Zhou // SpringerPlus. – 2016. – № 1 (5). – P. 1608.

15. Al Moubayed N. Beyond the topics: how deep learning can improve the discriminability of probabilistic topic modelling / N. Al Moubayed, S. McGough, B. Awwad Shiekh Hasan // PeerJ. Computer science. – 2020. – No. 6. – P. e252.

Землянский Сергей Александрович
Аспирант Национального исследовательского
Томского государственного университета (НИ ТГУ)
Ленина пр-т, 36, г. Томск, Россия, 634050
Тел.: +7-953-922-49-58
Эл. почта: qoelky@gmail.com

Аксёнов Сергей Владимирович
Канд. техн. наук, доцент отделения информационных технологий Инженерной школы информационных технологий и робототехники (ИШИТР)
Национального исследовательского
Томского политехнического ун-та (НИ ТПУ)
Ленина пр-т, 30, г. Томск, Россия, 634050
Доцент, каф. теоретических основ информатики НИ ТГУ
Ленина пр-т, 36, г. Томск, Россия, 634050
Тел.: +7-913-887-47-90
Эл. почта: axyonov@tpu.ru

Лызин Иван Александрович
Аспирант ИШИТР НИ ТПУ
Ленина пр-т, 30, г. Томск, Россия, 634050
ORCID: 0000-0003-2827-441X
Тел.: +7-923-498-70-30
Эл. почта: Lyzin@tpu.ru

Берестнева Ольга Григорьевна
Д-р техн. наук, профессор ИШИТР НИ ТПУ
Ленина пр-т, 30, г. Томск, Россия, 634050
Профессор каф. теоретических основ информатики НИ ТГУ
Ленина пр-т, 36, г. Томск, Россия, 634050
ORCID: 0000-0002-4243-0637
Тел.: +7-913-106-19-94
Эл. почта: ogb6@yandex.ru

Zemlyansky S.A., Axyonov S.V., Lyzin I.A., Berestneva O.G.

Topic Modeling in the Context of Medical Texts

Text analysis is an important area of research that includes several areas such as information retrieval, information extraction, and text categorization. Text analysis is widely used in the field of medical research because of the number of studies published daily, which can be processed at such a speed only with the help of computational resources. This paper presents the results of an experiment to thematically model a corpus of articles from the PubMed database from 2000 to 2020.

Keywords: health sciences, text analysis, latent Dirichlet distribution, research trends, knowledge mapping, knowledge synthesis, PubMed.
DOI: 10.21293/1818-0442-2021-24-4-58-64

References

1. Wang S.-H., Ding Y., Zhao W., Huang Y.-H., Perkins R. Text mining for identifying topics in the literatures about adolescent substance use and depression. *BMC public health*, 2016, (16), 279 p.

2. Cho S.M., Park C., Song M. The evolution of social health research topics: A data-driven analysis. *Social Science & Medicine*, 2020, (265), p. 113299.

3. Mo Y., Kontonatsios G., Ananiadou S. Supporting systematic reviews using LDA-based document representations // *Systematic Reviews*. 2015 (4), p. 172.

4. PubMed: National Library of Medicine [Online]. Available at: https://pubmed.ncbi.nlm.nih.gov/, free. (Accessed: December 16, 2021).

5. Onan A. Biomedical Text Categorization Based on Ensemble Pruning and Optimized Topic Modelling // *Computational and Mathematical Methods in Medicine*, 2018. pp. 1–22.

6. Sedova A., Mitrofanova O. *Tematičeskoe modelirovanie russkojazyčnyh tekstov s oporoj na lemmy i leksičeskie konstrukcii* [Thematic modeling of Russian-language texts based on lemmas and lexical constructions] *Computational Linguistics and Computational Ontologies*, 2018, pp. 132–144 (in Russ.).

7. Gan J., Qi Y. Selection of the Optimal Number of Topics for LDA Topic Model-Taking Patent Policy Analysis as an Example. *Entropy* (Basel, Switzerland), 2021, no. 10 (23), p. 1301.

8. Chandrasekaran R., Mehta V., Valkunde T., Moustakas E. Topics, Trends, and Sentiments of Tweets About the COVID-19 Pandemic: Temporal Infoveillance Study. *Journal of Medical Internet Research*, 2020, no. 10 (22), p. e22624.

9. Yıldırım A., Üsküdarlı S., Özgür A. Identifying Topics in Microblogs Using Wikipedia // PloS one. 2016, no. 3 (11), p. e0151885.

10. Rehurek R., Sojka P. Gensim–python framework for vector space modelling // NLP Centre, Faculty of Informatics, Masaryk University, Brno, Czech Republic. 2011. no. 2 (3), pp. 46–49.

11. Vafin R.R. *Aktual'nye problemy v oblasti izvlečenija znanij iz professional'nyh medicinskih tekstov s primeneniem intellektual'nogo analiza teksta* [Actual problems in the field of knowledge extraction from professional medical texts using text mining]. *Bulletin of Bashkir State Medical University*, 2019, pp. 72–75 (in Russ.).

12. Min J.-Y., Song S.-H., Kim H., Min K.-B. Mining Hidden Knowledge About Illegal Compensation for Occupational Injury: Topic Model Approach // *JMIR Medical Informatics*. 2019, no. 3 (7), p. e14763.

13. Wang H., Miller D. Improved Parsimonious Topic Modeling Based on the Bayesian Information Criterion // *Entropy* (Basel, Switzerland). 2020, no. 3 (22), p. 326.

14. Liu L., Tang L., Dong W., Yao S., Zhou W. An overview of topic modeling and its current applications in bioinformatics // SpringerPlus. 2016, no. 1 (5), p. 1608.

15. Al Moubayed N., McGough S., Awwad Shiekh Hasan B. Beyond the topics: how deep learning can improve the discriminability of probabilistic topic modelling // *PeerJ Computer Science*. 2020, (6), p. e252.

Sergey A. Zemlyansky
Postgraduate student, Tomsk State University (NI TSU)
36, Lenin pr., Tomsk, Russia, 634050
Phone: +7-953-922-49-58
Email: qoelky@gmail.com

Sergey V. Axyonov
Candidate of Science in Engineering, Assistant Professor,
Department of Information Technology,
School of Engineering Information Technology and Robotics
Tomsk Polytechnic University (NI TPU)
30, Lenin pr., Tomsk, Russia, 634050
Phone: +7-913-887-47-90
Email: axyonov@tpu.ru

Ivan A. Lyzin
Postgraduate student, Department of Information Technology,
School Engineering Information Technology and Robotics,
NI TPU
30, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0003-2827-441X
Phone: +7-923-498-70-30
Email: Lyzin@tpu.ru

Olga G. Berestneva
Doctor of Science in Engineering, Professor,
Department of Information Technology,
School of Engineering Information Technology
and Robotics, NI TPU
30, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-4243-0637
Phone: +7-913-106-19-94
Email: ogb6@yandex.ru

УДК 519.8 :378.16

А.В. Городович, В.В. Кручинин, М.Ю. Перминова

Система оценивания электронных учебно-методических комплексов дисциплин

Рассматриваются вопросы построения системы оценивания электронных учебно-методических комплексов дисциплин (ЭУМКД) факультета дистанционного обучения (ФДО) Томского государственного университета систем управления и радиоэлектроники (ТУСУР) с помощью инструментальной системы построения процедуры оценивания, разработанной в ТУСУРе. Описаны основные мероприятия: выбор критериев из базы знаний, запись новых критериев в базу знаний в форме анкет, установка коэффициентов важности, выявление согласованности экспертов, построение обобщённых критериев, получение рейтинга множества ЭУМКД. Приведены результаты построения рейтинга ЭУМКД 10 технических, 10 гуманитарных и 10 физико-математических дисциплин ФДО ТУСУР.

Ключевые слова: система оценивания, электронный образовательный ресурс, электронный учебно-методический комплекс дисциплины, критерий, база знаний, рейтинг.
DOI: 10.21293/1818-0442-2021-24-4-65-72

В настоящее время системы дистанционного обучения (СДО) вуза являются одним из важнейших элементов системы обучения студентов, в которой содержится большое число разнообразных электронных учебных ресурсов. Так, например, в Томском университете систем управления и радиоэлектроники (ТУСУР) на факультете дистанционного обучения (ФДО) в настоящее время имеется свыше 2 400 учебно-методических материалов, пособий, онлайн-курсов и тестов, представленных в электронной форме [1]. Оценивание качества учебно-методических комплексов дисциплин (УМКД), в том числе и электронных (ЭУМКД), осуществляют учебно-методические подразделения вуза, которые формируют оценки на основе рецензий экспертов и требований нормативно-правовых актов и инструкций. Необходимо отметить, что все ЭУМКД ФДО ТУСУРа соответствуют нормативным документам и прошли экспертизу, одним из критериев которой является соответствие принципам и нормам дидактики. С другой стороны, наличие большого числа электронных образовательных ресурсов ставит задачу улучшения их качества. В этом случае рецензии позволяют определить направление улучшения лишь частично. Поэтому для оценки качества ЭУМКД с целью их модернизации предложено построение информационной системы оценки качества, в основе которой лежат: прикладная лингвистика [2], психодидактика [3], теория принятия решений [4] и методы квалиметрии [5]. Для построения такой системы необходимо получить и исследовать систему критериев оценки качества ЭУМКД, которая строится на основе анализа множества электронных методических материалов и 20-летнего опыта их модернизации на ФДО ТУСУРа. Были выявлены следующие базовые элементы оценивания:

1. Учебный текст.
2. Креолизованный учебный текст.
3. Иллюстрация.
4. Аудиофайл.
5. Видеофайл.
6. Тестовые вопросы и задания.
7. Организация навигации, поиска и справочной информации.

Учебный текст является основой представления учебной информации, поэтому его качество является важной характеристикой. Имеется огромное число параметров текста, используемых при его оценке [6]. В ходе исследования ЭУМКД ФДО ТУСУРа были выделены следующие показатели качества текста: информационная насыщенность; абстрактность; удобочитаемость; водность; плотность ключевых слов [7], которые, с одной стороны, характеризуют сложность понимания текста, с другой – наличие новой информации.

В ходе исследований было выявлено 52 разнообразных критерия. Наличие большого числа критериев натолкнуло на идею создания инструментальной системы (ИС), которая по запросам методистов или по требованию текущей ситуации анализа ЭУМКД позволяла бы строить систему оценки качества учебного контента.

Для решения этой задачи были построены онтологическая модель процесса оценивания ЭУМКД и пополняемая база знаний критериев [8–10]. Данная ИС позволяет выполнить следующее: построить процедуру оценивания, выполнить оценивание элемента ЭУМКД, произвести обработку результатов оценивания, построить итоговый рейтинг множества ЭУМКД.

Для построения системы оценивания была разработана соответствующая методика оценивания [11], которая с помощью инструментальной системы обеспечивает:

1) выбор множества критериев оценивания,
2) установку коэффициентов предпочтения для построения итоговой оценки.

Критерии в инструментальной системе делятся на автоматические, значения которых определяются на основе алгоритма, и критерии, значения которых определяются на основе экспертного опроса. Причем при построении процедуры оценивания автоматические критерии выбираются из базы знаний, а критерии экспертного опроса могут как выбираться,

так и создаваться новые. Автоматические критерии делятся на следующие группы [11]: текстовые критерии, критерии оценки креолизации текста, критерии оценки иллюстраций, критерии организации справочной информации и поиска.

Для построения системы оценивания можно выделить следующую последовательность мероприятий:

1. Выявление множества автоматических критериев оценивания ЭУМКД. На данном этапе методист просматривает базу знаний критериев и выбирает наиболее значимые критерии для оценки определенного набора ЭУМКД. Например, если множество ЭУМКД не будет иметь объектов креолизации в тексте, то критерии оценки креолизации текста не надо включать в систему оценки [12]. Для определения способности оценивания автоматических критериев для данного класса ЭУМКД необходимо выбрать некоторое множество ЭУМКД, построить процедуру оценивания, содержащую только автоматические критерии, запустить систему анализа и получить оценки для выделенного множества ЭУМКД, провести анализ, например, получить среднее и среднеквадратическое отклонение.

2. Выявление множества критериев, значения которых определяются на основе опросных анкет. В процессе оценивания производится формирование анкет и рассылка этих анкет и элементов оценивания ЭУМКД экспертам. Каждый вопрос в анкете имеет шкалу оценивания. В процессе построения процедуры оценивания методист может создавать свои собственные анкеты. Методика построения анкет основана на использовании Google Forms. Она включает:

1) запись названия анкеты и оцениваемого элемента ЭУМКД,
2) получение совокупности вопросов,
3) получение шкал для каждого вопроса,
4) формирование комментариев и подсказок,
5) использование конструктора анкет.

На данный момент в базе знаний имеется 30 анкет, например, анкета на соответствие ЭУМКД нормативно-правовому обеспечению или анкета для оценки учебного видео. Для создания и проведения экспертных опросов также используется сервис Google Forms [13–15].

3. После получения множества критериев оценивания производится формирование коэффициентов важности. Каждый индивидуальный критерий (автоматический и экспертный) в системе имеет коэффициент важности. Имеется огромное число методов определения коэффициентов важности [16, 17]. В настоящее время в инструментальной системе реализован метод приписывания баллов [18]. При получении коэффициентов важности определяется согласованность мнений экспертов на основе коэффициента конкордации Кендалла [19]. При слабой согласованности (коэффициент менее 0,4) необходимо проводить мероприятия по повышению согласованности экспертов, применяя методы и алгоритмы повышения согласованности данных [20, 21].

4. Производится формирование обобщённых критериев путем объединения нескольких локальных критериев в виде процедуры оценивания. Например, все локальные текстовые критерии объединяются в один обобщённый текстовый критерий:

$$C_i = \sum_{j \in \mathrm{ord}(V)} \alpha_j Y_j, \qquad (1)$$

где α_j – коэффициент значимости для j-го критерия; Y_j – нормализованное значение критерия.

5. Формируются коэффициенты важности для обобщённых критериев (аналогично методам приписывания баллов), вычисляются коэффициенты согласованности экспертов и при необходимости проводятся мероприятия для повышения согласованности мнений экспертов.

6. Формируется единая процедура оценивания ЭУМКД:

$$R_{\text{ЭУМКД}} = \sum_{i \in \mathrm{ord}(V_o)} w_i C_i, \qquad (2)$$

где w_i – коэффициент значимости для i-го обобщенного критерия; C_i – нормализованное значение обобщённого критерия.

На каждом этапе инструментальная система формирует таблицы в формате Microsoft Excel, что позволяет воспользоваться программным обеспечением других систем обработки экспертной информации.

Рассмотрим построение системы оценивания электронных учебно-методических комплексов дисциплин факультета дистанционного обучения (ФДО) ТУСУРа. С 2018 г. ключевым компонентом ЭУМКД ФДО является электронный курс, в рамках которого публикуются все учебно-методические материалы. В данной статье понятия электронного курса и ЭУМКД употребляются в качестве синонимов.

Условно электронный курс можно разделить на несколько блоков: информационно-организационный, учебный, текущий контроль, промежуточная аттестация. В информационно-организационном блоке представлена информация, которая помогает организовать самостоятельное освоение дисциплины и дает общее представление о ней, например, аннотация курса, рабочая программа, информация об авторе курса и т.п. В учебном блоке находится теоретический материал по дисциплине, который может быть представлен в виде текстово-графических материалов, слайд-лекций (иногда комбинированных с аудио или видео), видео- и аудиолекций, вебинаров, интерактивных тренажеров и т.п. В блоке текущего контроля размещаются тесты и задания для самоконтроля, тесты и задания на контрольные и лабораторные работы, курсовые работы и проекты, требования к их оформлению, критерии оценивания работ и т.п. В блоке промежуточной аттестации находятся тесты и задания для зачета с оценкой или экзамена.

Все ЭУМКД ФДО можно разделить по условным категориям:

- гуманитарные – 43%,
- инженерные – 26%,
- физико-математические – 15%.

Оставшиеся 16% – это прочие ЭУМКД, которые нельзя отнести к данным категориям (например, ЭУМКД по физической культуре, практикам, государственной итоговой аттестации и т.п.).

На первом шаге из базы знаний критериев было выбрано 9 автоматических критериев:

- информационная насыщенность,
- абстрактность,
- удобочитаемость,
- водность,
- плотность ключевых слов,
- степень креолизации учебного текста,
- объем иллюстраций,
- равномерность распределения иллюстраций,
- справка и навигация.

Данные критерии позволяют получить высокую точность оценки и основаны на основных проблемах, которые возникают у студентов при изучении электронных курсов дисциплин [7, 22].

На втором шаге выделены критерии, значения которых определяются на основе экспертного опроса. Эксперту выдаются один или несколько элементов ЭУМКД, которые необходимо оценить, из списка:

- учебное пособие/курс лекций (может быть из электронно-библиотечных систем),
- учебно-методическое пособие,
- методические указания (по курсовому проекту/работе, контрольной/лабораторной работе, самостоятельной работе),
- банк тестовых заданий (для контрольной работы, экзамена).

Формируется анкета для опроса эксперта. Критерии оценки ЭУМКД:

1. Тестовые задания (ТЗ).

Вопросы анкеты:

- Оцените, проверяют ли ТЗ степень сформированности и уровень освоения закрепленных за дисциплиной компетенций (шкала, поле ввода).
- Оцените степень соответствия ТЗ теоретическому материалу (шкала, поле ввода).
- Имеются требования к формированию билета (сколько ТЗ выдавать обучающемуся по каждой главе или теме) (шкала, поле ввода).
- Оцените распределение ТЗ по главам (модулям) (шкала, поле ввода).
- Оцените количество ТЗ генераторного типа (шкала, поле ввода).

2. Учебное видео.

Вопросы анкеты:

- Оцените степень соответствия учебного видео теме модуля (шкала, поле ввода).
- Оцените качество учебного видео (шкала, поле ввода).

Подобным образом формируется анкета для оценки учебного аудио.

3. Учебное пособие/курс лекций:

- Оцените степень соответствия объема пособия общей трудоемкости дисциплины (шкала, поле ввода).
- Оцените степень соответствия содержания пособия целям и задачам дисциплины (шкала, поле ввода).
- Оцените степень соответствия содержания пособия результатам освоения дисциплины (компетенции, знания, умения и навыки) (шкала, поле ввода).
- Оцените степень соответствия названий глав пособия названиям разделов дисциплины (шкала, поле ввода).
- Оцените степень соответствия объема глав пособия часам, отведенным на их изучение (шкала, поле ввода).

4. Учебно-методическое пособие:

- Оцените степень соответствия содержания пособия целям и задачам дисциплины (шкала, поле ввода).
- Оцените степень соответствия заданий теоретическому материалу курса (шкала, поле ввода).
- Оцените систему оценивания (критерии оценивания) заданий (шкала, поле ввода).
- Оцените список источников литературы (с теоретическим и/или практическим материалом), необходимых для выполнения заданий (шкала, поле ввода).
- Оцените требования к структуре и оформлению отчетов, которые пишут обучающиеся по итогу выполнения текстовой работы (шкала, поле ввода).
- Оцените количество исходных вариантов тем/заданий (шкала, поле ввода).

5. Учебная презентация:

- Оцените содержательную часть презентаций на соответствие теме модуля (шкала, поле ввода).
- Оцените качество графической части презентаций (иллюстрации, таблицы, схемы и т.п.) (шкала, поле ввода).
- Оцените баланс текстовой и графической (иллюстрации, таблицы, схемы и т.п.) частей презентаций (шкала, поле ввода).

Указанные критерии получены на основе анализа базы ЭУМКД ФДО и локальных нормативных актов ТУСУР и других образовательных организаций высшего образования с учетом основных проблем, которые возникают у студентов при изучении электронных курсов дисциплин [23–25].

Анкеты для опроса эксперта вводятся как критерии оценки в базу знаний инструментальной системы и рассматриваются системой как критерий. Например, анкета для оценки учебного пособия на соответствие РПД состоит из следующих вопросов:

1. Оцените степень соответствия объема пособия общей трудоемкости дисциплины по шкале от 0 до 2, где: 0 – не соответствует; 1 – частично соответствует; 2 – соответствует.
2. Оцените степень соответствия содержания пособия целям и задачам дисциплины по шкале от 0 до 2, где: 0 – не соответствует; 1 – частично соответствует; 2 – соответствует.
3. Оцените степень соответствия содержания пособия результатам освоения дисциплины (компетенции, знания, умения и навыки) по шкале от 0 до 2, где: 0 – не соответствует; 1 – частично соответствует; 2 – соответствует.
4. Оцените степень соответствия названий глав пособия названиям разделов дисциплины по шкале

от 0 до 2, где: 0 – не соответствует; 1 – частично соответствует; 2 – соответствует.

5. Оцените степень соответствия объема глав пособия часам, отведенным на их изучение по шкале от 0 до 2, где: 0 – не соответствует; 1 – частично соответствует; 2 – соответствует.

6. Поле для ввода особого мнения.

Выявленное и построенное множество критериев в системе записывается как процедура оценивания, причем эта процедура оценивания может содержать другие процедуры оценивания. Для нашего случая формируется пять обобщенных критериев:

1. Текстовые критерии объединены в процедуру оценивания текста.

2. Критерии оценки иллюстраций объединены в процедуру оценки иллюстраций.

3. Критерии оценки креолизации объединены в процедуру оценки креолизации.

4. Критерии оценки справки и навигации объединены в процедуру оценки справки и навигации.

5. Анкетные критерии объединены в процедуру оценки на основе экспертного опроса.

В процессе формирования множества критериев можно проводить предварительный анализ групп ЭУМКД, воспользовавшись модулем анализа инструментальной системы. Например, для предварительной оценки качества текста по текстовым параметрам для группы ЭУМКД можно запустить процедуру оценивания текста (табл. 1). У каждого критерия в скобках указан рекомендуемый диапазон значений.

Таблица 1

Предварительное оценивание качества ЭУМКД ФДО по текстовым критериям

Отметка времени	Система дистанционного обучения	Идентификатор курса	Абстрактность (5–20)	Информационная насыщенность (30–100)	Плотность ключевых слов (5–7)	Удобочитаемость (0–20)	Водность (0–30)
20.08.2021 9:23:40	new-online	4	24,97	13,51	31,53	6,84	3,58
20.08.2021 9:27:33	new-online	238	24,92	16,24	36,5	8,74	2,66
20.08.2021 9:29:27	new-online	422	28,22	1,91	71,54	10,59	1,69
20.08.2021 9:33:26	new-online	164	23,14	1,58	35,43	8,62	2,44
20.08.2021 9:37:19	new-online	89	27,41	16,38	40,63	9,52	2,35
20.08.2021 9:38:05	new-online	284	25,32	4,48	30,63	7,4	2,86
20.08.2021 9:39:00	new-online	234	25,75	6,6	25,98	7,73	3,54
20.08.2021 9:39:49	new-online	155	26,39	2,99	37,13	7,63	2,75
20.08.2021 9:41:31	new-online	154	27,67	7,39	31,19	7,33	2,21
20.08.2021 9:43:46	new-online	254	25,31	21,42	34,48	7,65	2,99
20.08.2021 9:44:52	new-online	153	22,22	16,25	26,72	4,95	4,72
20.08.2021 9:47:05	new-online	106	25,18	14,69	44,01	8,58	1,66
20.08.2021 9:49:47	new-online	97	20,48	90,13	36,06	5,8	4,28

Следующим этапом формируется множество коэффициентов важности для локальных и обобщенных критериев. Это происходит методом приписывания баллов: 4 экспертам был предоставлен набор критериев, важность которых они оценили по шкале от 0 до 10. При этом разрешалось оценивать важность дробными величинами или приписывать одну и ту же величину из выбранной шкалы нескольким критериям.

Все оценки экспертов были объединены в таблицу в формате Microsoft Excel. В табл. 2 приведены оценки экспертов по текстовым критериям.

Далее, воспользовавшись модулем обработки данных инструментальной системы, были получены весовые коэффициенты и коэффициент конкордации.

Для текстовых критериев:

- Абстрактность – 0,273.
- Информационная насыщенность – 0,219.
- Плотность ключевых слов – 0,13.
- Удобочитаемость – 0,274.
- Водность – 0,104.
- Коэффициент конкордации – 0,9125.

Таблица 2

Таблица для определения коэффициентов важности текстовых критериев

	Абстрактность	Инф. насыщенность	Плотность ключевых слов	Удобочитаемость	Водность
Эксперт 1	8	6	4	9	2
Эксперт 2	9	7	5	8	4
Эксперт 3	10	8	4	9	3
Эксперт 4	9	8	4	10	5

Для критериев оценки иллюстраций:

- Число иллюстраций – 0,402.
- Среднее число иллюстраций на странице – 0,598.
- Коэффициент конкордации – 1.

Для критериев оценки креолизации:

- Выделение фоновым цветом – 0,109.
- Выделение жирным шрифтом – 0,166.
- Выделение рамкой – 0,05.
- Выделение курсивом – 0,161.
- Выделение ссылкой – 0,168.
- Выделение пиктограммой – 0,251.
- Выделение подчёркиванием – 0,095.
- Коэффициент конкордации – 0,9245.

Для критериев справки и навигации:

- Список литературы – 0,418.
- Список формул – 0,145.
- Глоссарий – 0,202.
- Среда ссылок – 0,123.
- Список таблиц – 0,113.
- Коэффициент конкордации – 0,926.

Для обобщенных критериев были выявлены следующие коэффициенты важности:

- Текст – 0,323.
- Рисунки – 0,26.
- Креолизация – 0,244.
- Справка – 0,173.
- Коэффициент конкордации – 0,97368.

Для экспертных критериев:

- Критерий 1 – 0,091.
- Критерий 2 – 0,091.
- Критерий 3 – 0,084.
- Критерий 4 – 0,023.
- Критерий 5 – 0,059.
- Критерий 6 – 0,058.
- Критерий 7 – 0,049.
- Критерий 8 – 0,061.
- Критерий 9 – 0,056.
- Критерий 10 – 0,058.
- Критерий 11 – 0,035.
- Критерий 12 – 0,026.
- Критерий 13 – 0,019.
- Критерий 14 – 0,03.
- Критерий 15 – 0,023.
- Критерий 16 – 0,082.
- Критерий 17 – 0,045.
- Критерий 18 – 0,038.
- Критерий 19 – 0,048.
- Критерий 20 – 0,017.
- Критерий 21 – 0,026.
- Критерий 22 – 0,028.
- Коэффициент конкордации – 0,6497.

Для автоматических и экспертных критериев:

- Автоматические критерии – 0,468.
- Экспертные критерии – 0,532.
- Коэффициент конкордации – 0,5.

Коэффициент конкордации во всех случаях имеет значение больше или равное 0,5, что говорит о наличии высокой степени согласованности мнений экспертов.

Оценка по каждому обобщенному критерию рассчитывается по формуле (1). Основными требованиями к такой обобщающей функции являются:

1) изменяемость всех значений критериев в единой шкале [0,1];

2) монотонный рост при увеличении значения частного критерия при фиксированных остальных частных критериях;

3) независимость частных критериев [4].

Эти требования были учтены в системе оценивания. Критерии независимы, что следует из формул, по которым рассчитываются их значения [7].

Оценка по обобщенным автоматическим критериям имеет вид выражения

$$Кр_{ав} = \begin{pmatrix} К_{текст} \times Кр_{ав1} + \\ +К_{иллюстр} \times Кр_{ав2} + К_{креолиз} \times Кр_{ав3} + \\ +К_{справ\ и\ навиг} \times Кр_{ав4} \end{pmatrix},$$

где $К_{текст}$, $К_{иллюстр}$, $К_{креолиз}$, $К_{справ\ и\ навиг}$ – значения коэффициента важности соответствующего обобщённого критерия (текста, иллюстраций, креолизации, справки и навигации), $Кр_{ав i}$ – значение соответствующего обобщённого критерия.

Оценка по обобщенному критерию, значение которого определяется на основе опросных анкет, имеет вид

$$Кр_{эксп} = \begin{pmatrix} К_1 \times Кр_{эксп1} + \\ +К_2 \times Кр_{эксп2} + К_3 \times Кр_{эксп3} + ... \\ +К_{22} \times Кр_{эксп22} \end{pmatrix},$$

где $К_i$ – значение коэффициента важности соответствующего критерия опросной анкеты экспертов, $Кр_{эксп i}$ – значение соответствующего критерия опросной анкеты экспертов.

Итоговая оценка ЭУМКД рассчитывается по формуле (2).

В табл. 3 приведен итоговый рейтинг группы из 30 ЭУМКД ФДО, причем 10 из них относятся к техническим дисциплинам (T), 10 – к гуманитарным (G), 10 – к физико-математическим (F).

Таблица 3

Итоговый рейтинг ЭУМКД

Код УМКД	$Кр_{сум}$	Категория ЭУМКД
1	2	3
287	0,45223	T
153	0,41125	F
266	0,37745	T
95	0,37704	F
97	0,37673	F
422	0,35449	G
238	0,35094	T
284	0,34591	G
4	0,33549	T
282	0,33257	G
289	0,31916	F
164	0,31847	T
271	0,31309	F
234	0,30312	T
52	0,30068	F

Продолжение табл. 3

1	2	3
205	0,28756	F
89	0,27117	T
197	0,26202	T
189	0,26169	T
254	0,26154	G
106	0,25903	F
154	0,2562	G
74	0,24985	F
140	0,23329	G
155	0,22725	G
75	0,21929	G
62	0,21391	T
34	0,20079	F
46	0,19412	G
40	0,18924	G

Выводы

1. Представленная система оценивания качества ЭУМКД ориентирована на решение проблемы модернизации электронного учебного контента и не исключает традиционные методы оценивания методического обеспечения.

2. Наличие пополняемой базы знаний критериев оценивания обеспечивает возможность внесения изменений в имеющуюся систему оценки качества или создание новой системы оценивания для использования в иных целях.

3. Анализ таблицы итогового рейтинга показывает, что:

- суммарное значение обобщенных критериев $Кр_{сум}$ для представленного множества ЭУМКД составляет 8,8556, или 29,5% от максимального значения (30), это свидетельствует о потенциальной возможности улучшения их качества;
- отсутствует группирование по типу ЭУМКД, что дает возможность сравнивать между собой гуманитарные, технические и физико-математические учебные материалы.

В настоящее время система оценивания проходит опытную эксплуатацию на ФДО. Экспериментальные данные, полученные с помощью этой системы, согласуются с мнением экспертного сообщества.

Литература

1. Городович А.В. Текущее состояние и проблемы модернизации контента в системе электронного обучения ТУСУР / А.В. Городович, В.В. Кручинин, М.Ю. Перминова // Современное образование: качество образования и актуальные проблемы современной высшей школы: матер. междунар. науч.-метод. конф. – Томск: ТУСУР, 2019. – С. 109–111.

2. Майер Р.В. Дидактическая сложность учебных текстов и ее оценка. – Глазов: ГГПИ, 2020. – 148 с.

3. Савенков А.И. Психодидактика. – М.: Национальный книжный центр, 2012. – 360 с.

4. Микони С.В. Теория принятия управленческих решений. – СПб.: Лань, 2015. – 448 с.

5. Субетто А.И. Квалиметрия: малая энциклопедия. – СПб.: ИПЦ СЗИУ – фил. РАНХиГС, 2015. – Вып. 1. – 244 с.

6. Кротова И.В. Оптимизация совместимости учебной наглядности (на примере учебников средней школы): автореф. дис. … д-ра пед. наук. – Чита, 2009. – 39 с.

7. Морозова Ю.В. Методика анализа электронного учебного контента / Ю.В. Морозова, И.А. Уртамова // Открытое и дистанционное образование. – 2017. – № 4 (68). – С. 38–44.

8. Городович А.В. Инструментальная система анализа и оценивания учебного контента / А.В. Городович, И.А. Кречетов, В.В. Кручинин, М.Ю. Перминова // Доклады ТУСУР. – 2020. – Т. 23, № 2. – С. 81–87.

9. Городович А.В. Задача и алгоритмы формирования плана мероприятий модернизации учебного контента / А.В. Городович, В.В. Кручинин, С.П. Сущенко // Доклады ТУСУР. – 2019. – Т. 22, № 4. – С. 69–74.

10. Свидетельство о регистрации программы для ЭВМ №2020618144. Система анализа и оценивания учебного контента / А.В. Городович, И.А. Кречетов, В.В. Кручинин, М.Ю. Перминова. – Заявка № 2020616899. Дата поступления 07 июля 2020 г. Зарегистрировано в Реестре программ для ЭВМ 20 июля 2020 г.

11. Городович А.В. Методика построения системы оценивания электронных учебно-методических комплексов дисциплин / А.В. Городович, В.В. Кручинин, М.Ю. Перминова // Современное образование: повышение конкурентоспособности университетов: матер. междунар. науч.-метод. конф. – Томск: Изд-во ТУСУР, 2021. – Ч. 1. – С. 216–222.

12. Городович А.В. Метод определения степени креолизации учебного текста в электронных системах обучения / А.В. Городович, В.В. Кручинин, М.Ю. Перминова // Современные тенденции развития непрерывного образования: вызовы цифровой экономики: матер. междунар. науч.-метод. конф. – Томск: ТУСУР, 2020. – С. 74–75.

13. Raju N.V. Online survey tools: A case study of Google Forms / N.V. Raju, N.S. Harinara-yana [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/326831738_Online_survey_tools_A_case_study_of_Google_Forms, свободный (дата обращения: 30.11.2021).

14. Kishore K. How to create an online survey by using Google Forms / K. Kishore, L. Naik [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/333369585_HOW_TO_CREATE_AN_ONLINE_SURVEY_BY_USING_GOOGLE_FORMS, свободный (дата обращения: 30.11.2021).

15. Using Google Forms for Medical Survey: A Technical Note / H. Mondal, S. Mondal, T. Ghosal, S. Mondal // International Journal of Clinical and Experimental Physiology, 5(4), 216–218 [Электронный ресурс]. – Режим доступа: https://doi.org/10.5530/ijcep.2018.5.4.26, свободный (дата обращения: 27.11.2021).

16. Спиридонов С.Б. Анализ подходов к выбору весовых коэффициентов критериев методом парного сравнения критериев / С.Б. Спиридонов, И.Г. Булатова, В.М. Постников // Интернет-журнал «Науковедение». – 2017. – Т. 9, № 6 [Электронный ресурс]. – Режим доступа: https://naukovedenie.ru/PDF/16TVN617.pdf, свободный (дата обращения: 28.11.2021).

17. Постников В.М. Методы выбора весовых коэффициентов локальных критериев / В.М. Постников, С.Б. Спиридонов // Наука и образование МГТУ им. Н.Э. Баумана. – 2015. – № 6. – С. 267–287 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/metody-vybora-vesovyh-koeffitsientov-lokalnyh-kriteriev (дата обращения: 16.11.2021).

18. Корячко В.П. Теоретические основы САПР: учеб. для вузов / В.П. Корячко, В.М. Курейчик, И.П. Норенков. – М.: Энергоатомиздат, 1987. – 400 с.

19. Фёрстер Э. Методы корреляционного и регрессионного анализа. Руководство для экономистов /

Э. Фёрстер, Б. Рёнц (пер. с нем. и предисл. В.М. Ивановой). – М.: Финансы и статистика, 1983. – 304 с.

20. Огурцов А.Н. Алгоритм повышения согласованности экспертных оценок в методе анализа иерархий / А.Н. Огурцов, Н.А. Староверова // Вестник ИГЭУ. – 2013. – № 5 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/algoritm-povysheniya-soglasovannosti-ekspertnyh-otsenok-v-metode-analiza-ierarhiy (дата обращения: 02.12.2021).

21. Постников В.М. Подход к увеличению уровня согласованности мнений экспертов при выборе варианта развития системы обработки информации / В.М. Постников, С.Б. Спиридонов // Наука и образование МГТУ им. Н.Э. Баумана. – 2013. – № 06 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/podhod-k-uvelicheniyu-urovnya-soglasovannosti-mneniy-ekspertov-pri-vybore-varianta-razvitiya-sistemy-obrabotki-informatsii, свободный (дата обращения: 01.12.2021).

22. Уртамова И.А. Критерии анализа электронного учебного контента / И.А. Уртамова, Ю.В. Морозова // Матер. междунар. науч.-метод. конф. «Современное образование: развитие технологий и содержания высшего профессионального образования как условие повышения качества подготовки выпускников». – Томск: ТУСУР, 2017. – С. 186–187.

23. Положение об электронном курсе в ТУСУРе [Электронный ресурс]. – Режим доступа: https://regulations.tusur.ru/documents/1134, свободный (дата обращения: 01.10.2021).

24. Эрганова Н.Е. Практикум по методике профессионального обучения: учеб. пособие / Н.Е. Эрганова, М.Г. Шалунова, Л.В. Колясникова. – 2-е изд., пересмотр. и доп. – Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2011. – 89 с.

25. Требования к структуре и содержанию онлайн-курсов и методические рекомендации по разработке онлайн-курсов в системе управления электронным обучением LMS MOODLE [Электронный ресурс]. – Режим доступа: https://portal.tpu.ru/f_el/pdf/2019/tr_k_strsodok2019.pdf, свободный (дата обращения: 10.10.2021).

Городович Андрей Викторович
И.о. директора Института инноватики (ИИ)
Томского государственного ун-та систем управления и радиоэлектроники (ТУСУР),
ассистент каф. технологий электронного обучения (ТЭО) факультета дистанционного обучения (ФДО) ИИ ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 90-01-88
Эл. почта: gaw@2i.tusur.ru

Кручинин Владимир Викторович
Д-р техн. наук, доцент, зав. каф. ТЭО ФДО ИИ ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0001-5564-2797
Тел.: +7 (382-2) 70-15-52
Эл. почта: kru@2i.tusur.ru

Перминова Мария Юрьевна
Канд. техн. наук, доцент каф. ТЭО ФДО ИИ ТУСУР
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-52
Эл. почта: pmy@2i.tusur.ru

Gorodovich A.V., Kruchinin V.V., Perminova M.Yu.

Evaluation system for electronic educational-methodical complexes of disciplines

The article describes the design of evaluation system for electronic educational-methodical complexes of disciplines (EEMCD) applied at the Faculty of Distance Learning of Tomsk State University of Control Systems and Radioelectronics (TUSUR). The design technique developed at TUSUR involves a tool system to evaluate the procedure. The following main activities are described: selection of criteria from knowledge base, introducing new criteria into knowledge base in form of questionnaires, setting importance coefficients, identification of experts' consistency, construction of generalized criteria, obtaining the rating of EEMCD set. The results of computerized multimedia subjects rating on 10 engineering disciplines, 10 disciplines in the field of physics and mathematics taught at TUSUR Faculty of Distance Learning are given.

Keywords: evaluation system, electronic educational resource, electronic educational-methodical complex of discipline, criterion, knowledge database, rating.
DOI: 10.21293/1818-0442-2021-24-4-65-72

References

1. Gorodovich A.V., Kruchinin V.V., Perminova M.Yu. *Tekushchee sostoyanie i problemy modernizacii kontenta v sisteme elektronnogo obucheniya TUSUR* [Current state and problems of content modernization in the e-learning system of TUSUR University]. Sovremennoye obrazovaniye: kachestvo obrazovaniya i aktual'nyye problemy sovremennoy vysshey shkoly. Materialy mezhdunarodnoi nauchno-metodicheskoy konferentsii [*Modern education: the quality of education and current problems of modern higher education*. Proc. of the International scientific and methodological conference]. Tomsk, TUSUR Publ., 2019, pp. 109–111 (in Russ.).

2. Majer R.V. Didakticheskaja slozhnost' uchebnyh tekstov i ee ocenka: monografija [Didactic complexity of educational texts and its evaluation]. – Glazov: GGPI, 2020, 148 p. (in Russ.).

3. Savenkov A.I. Psihodidaktika [Psychodidactics]. M.: Nacional'nyj knizhnyj centr, 2012, 360 p. (in Russ.).

4. Mikoni S.V. Teoriya prinyatiya upravlencheskih reshenij [Theory of managerial decision making]. St. Petersburg: Lan' Publ., 2015, 448 p. (in Russ.).

5. Subetto A. I. *Kvalimetriya : malaya enciklopediya* [Qualimetry : a small encyclopedia]. St. Petersburg: IPC SZIU Publ. fil. RANHiGS, 2015, 244 p. (in Russ.).

6. Krotova I.V. *Optimizaciya sovmestimosti uchebnoj naglyadnosti (na primere uchebnikov srednej shkoly)* [Optimizing the compatibility of educational visuals (the example of secondary school textbooks). Thesis of Doctor of Science in Didactics]. CHita, 2009, 39 p. (in Russ.).

7. Morozova Ju.V., Urtamova I.A. Metodika analiza jelektronnogo uchebnogo kontenta [Metodology of analysis of electronic educational content]. *Open and Distance Education*, 2017, vol. 68, no 4, pp. 38–44 (in Russ.).

8. Gorodovich A.V., Krechetov I.A., Kruchinin V.V., Perminova M.Ju. [Tool system for analysis and evaluation of learning content]. *Proceedings of TUSUR University*, 2020, vol. 23, no. 2, pp. 81–87 (in Russ.).

9. Gorodovich A.V., Kruchinin V.V., Suschenko S.P. [Task and algorithms to conceive an action plan for the updating of learning content]. *Proceedings of TUSUR University*, 2019, vol. 22, no. 4, pp. 69–74 (in Russ.).

10. Gorodovich A.V., Krechetov I.A., Kruchinin V.V., Perminova M.Ju. *Sistema analiza i ocenivanija uchebnogo*

kontenta [Learning content analysis and evaluation system]. Program Registration Certificate for JeVM (no. 2020618144, 2020) (in Russ.).

11. Gorodovich A.V. *Metodika postroenija sistemy ocenivanija jelektronnyh uchebno-metodicheskih kompleksov disciplin* [Methods for building a system for evaluating electronic educational and methodical complexes of disciplines]. Sovremennoe obrazovanie: povyshenie konkurentosposobnosti universitetov [*Modern education: increasing the competitiveness of universities*. Proceedings of the International scientific and methodological conference]. Tomsk, TUSUR Publishing Office, 2021, pp. 216–222 (in Russ.).

12. Gorodovich A.V., Kruchinin V.V., Perminova M.Yu. *Metod opredelenija stepeni kreolizacii uchebnogo teksta v jelektronnyh sistemah obuchenija* [Method for determining the degree of creolisation of educational text in electronic learning systems]. Sovremennye tendencii razvitija nepreryvnogo obrazova-nija: vyzovy cifrovoj jekonomiki : materialy mezhd. nauch.metod. konf. [*Current trends in continuing education: challenges of the digital economy*. Proceedings of the International scientific and methodological conference]. Tomsk, TUSUR Publishing Office, 2020, pp. 74–75 (in Russ.).

13. Vasantha Raju N., Harinarayana N.S. Online survey tools: A case study of Google Forms. Available at: https://www.researchgate.net/publication/326831738_Online_survey_tools_A_case_study_of_Google_Forms, free (Accessed: November 30, 2021).

14. Kumar, Kishore, Naik, Lokesha How to create an online survey by using Google forms. *International Journal of Library and Information Studies*, 2016, vol. 6, no. 3, pp. 118–126. Available at: https://www.researchgate.net/publication/333369585_HOW_TO_CREATE_AN_ONLINE_SURVEY_BY_USING_GOOGLE_FORMS, free (Accessed: November 30, 2021).

15. Mondal H., Mondal S., Ghosal T., Mondal S. Using Google Forms for Medical Survey: A Technical Note. *International Journal of Clinical and Experimental Physiology*, 2019, vol. 4, no. 5, pp. 216–218. Available at: https://doi.org/10.5530/ijcep.2018.5.4.26, free (Accessed: November 27, 2021).

16. Spiridonov S.B., Bulatova I.G., Postnikov V.M. Analysis of approaches to the choice of weighting criteria method of pair comparison of criteria. Internet-zhurnal «Naukovedenie», 2017, vol. 9, no. 6 (in Russ.). Available at: https://naukovedenie.ru/PDF/16TVN617.pdf, free (Accessed: November 28, 2021).

17. Postnikov V.M., Spiridonov S.B. Selecting Methods of the Weighting Local Criteria. *Science&Education of the Bauman MSTU*, 2015, no. 6, pp. 267–287 (in Russ.). Available at: https://cyberleninka.ru/article/n/metody-vybora-vesovyh-koeffitsientov-lokalnyh-kriteriev, free (Accessed: November 16, 2021).

18. Korjachko V.P., Kurejchik V.M., Norenkov I.P. Teoreticheskie osnovy SAPR [Theoretical foundations of CAD]. Moscow, Jenergoatomizdat Publ., 1987, 400 p. (in Russ.).

19. Fjorster Je., Rjonc B. Metody korreljacionnogo i regressionnogo analiza [Methods of correlation and regression analysis] (translation from German and epilogue by V.M. Ivanova). Moscow, Finansy i statistika Publ., 1983, 304 p. (in Russ.).

20. Ogurcov A.N., Staroverova N.A. Algorithm of improving expert assessment consistency in hierarchy analysis method. *Vestnik of Ivanovo State Power Engineering University*, 2013, no. 5 (in Russ.). Available at: https://cyberleninka.ru/article/n/algoritm-povysheniya-soglasovannosti-ekspertnyh-otsenok-v-metode-analiza-ierarhiy, free (Accessed: December 2, 2021).

21. Postnikov V.M., Spiridonov S.B. Approach to increasing the level of consistency of expert opinion when selecting the variant of development of the data processing. *Science&Education of the Bauman MSTU*, 2013, no. 06 (in Russ.). Available at: https://cyberleninka.ru/article/n/podhod-k-uvelicheniyu-urovnya-soglasovannosti-mneniy-ekspertov-pri-vybore-varianta-razvitiya-sistemy-obrabotki-informatsii, free (Accessed: December 1, 2021).

22. Morozova Ju.V., Urtamova I.A. *Kriterii analiza jelektronnogo uchebnogo kontenta* [Criteria for analyzing e-learning content]. Sovremennoe obrazovanie: razvitie tehnologij i soderzhanija vysshego professional'nogo obrazovanija kak uslovie povyshenija kachestva podgotovki vypusknikov [*Modern Education: development of technology and content of higher professional education as a condition for improving the quality of graduates.* [Proc. of the International scientific and methodological conference *«Modern Education: development of technology and content of higher professional education as a condition for improving the quality of graduates»*]. Tomsk, TUSUR Publishing Office, 2017, pp. 186–187 (in Russ.).

23. Polozheniye ob elektronnom kurse v TUSURe. Available at: https://regulations.tusur.ru/documents/1134, free (Accessed: December 1, 2021) (in Russ.).

24. Erganova N.E., Shalunova M.G., Kolyasnikova L.V. Praktikum po metodike professionalnogo obucheniya [Workshop on the methodology of vocational training]. Ekaterinburg: Ros. gos. prof.-ped. un-ta Publ., 2011, 89 p. (in Russ.).

25. Trebovaniya k strukture i soderzhaniyu onlayn-kursov i metodicheskiye rekomendatsii po razrabotke onlayn-kursov v sisteme upravleniya elektronnym obucheniyem. Available at: https://portal.tpu.ru/f_el/pdf/2019/tr_k_strsodok 2019.pdf, free (Accessed: October 10, 2021).

Andrey V. Gorodovich
Acting Director, Institute of Innovations (II),
Assistant, Department of e-Learning Technology (ELT),
Faculty of Distance Learning (DL)
Tomsk State University of Control Systems
and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 90-01-88
Email: gaw@2i.tusur.ru

Vladimir V. Kruchinin
Doctor of Science in Engineering, Assistant Professor,
Head, Department of e-Learning Technology (ELT),
Faculty of Distance Learning (DL) TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0001-5564-2797
Phone: +7 (382-2) 70-15-52
Email: kru@2i.tusur.ru

Maria Yu. Perminova
Candidate of Science in Engineering, Assistant Professor,
Department of e-Learning Technology (ELT),
Faculty of Distance Learning (DL) TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 70-15-52
Email: pmy@2i.tusur.ru

УДК 004.42:631

М.Ю. Катаев, Е.Ю. Карташов, Д.С. Смирнов

Методика и программа атмосферной коррекции изображений беспилотных летательных аппаратов в задаче безопасной локации растительности

Беспилотные летательные аппараты (БПЛА) с установленной на них аппаратурой представляют собой способ сбора информации в виде изображений с высоким пространственным разрешением при относительно простом управлении аппарата, что делает его экономически эффективным. За последние 10 лет технология измерений с помощью БПЛА существенно изменилась и стала популярной благодаря своей универсальности и легкости применения в коммерческих и научных исследованиях. Надо отметить, что способы обработки разово получаемых изображений позволяют решать различного рода научные и практические задачи, однако при мониторинге, когда изучается динамика состояния объектов (типов поверхности) одной и той же территории, методическое и программное наполнение пока остается слабо решенным вопросом. Одной из проблем, мешающих изучению динамики, например состояния объектов сельскохозяйственных полей, является радиометрическая точность получаемых изображений БПЛА. Учет на практике радиометрической точности измерений позволяет учитывать различные условия освещения в разное время дня, месяце, типами применяемых цифровых датчиков (цифровых камер). Настоящее исследование направлено на снижение зависимости при изучении динамики состояния объектов одной и той же территории в различное время за счет учета радиометрических ошибок изображений БПЛА при картировании состояния растительности. Для исследований применяются реальные изображения БПЛА, которые получены в период июнь–август 2019 г. для сельскохозяйственного поля с озимой пшеницей.

Ключевые слова: беспилотные летательные аппараты, изображение, атмосферная коррекция, картографирование растительности, индексы растительности.
DOI: 10.21293/1818-0442-2021-24-4-73-78

Беспилотные летательные аппараты (БПЛА) позволяют получать изображения с установленных на них камер, имеющих высокое пространственное разрешение. БПЛА летают по заранее проработанному маршруту в автоматическом режиме или под управлением оператора, что является экономически выгодным способом сбора информации по сравнению с другими [1]. За последнее время появились коммерческие и свободно распространяемые технологии автоматизированной обработки множества изображений, получаемых за время облета маршрута, например: Geoscan [2], Agisoft [3], Dronmap [4], Pix4d [5] и др.

При всей проработанности методик обработки остаются проблемы радиометрической коррекции изображений и решения задач мониторинга. Особенно эту коррекцию важно сделать перед тем, как изображения будут сшиваться в общее изображение территории (мозаику). При оценке состояния, например, растительности на сельскохозяйственном поле важно применять не классические методики коррекции изображений («серый мир» [6]), а физически обоснованные, учитывающие такие факторы, как учет освещенности солнцем (высота и зенитный угол), рельеф и т.д. Радиометрическая коррекция позволяет учитывать взаимосвязь между значениями пикселей и естественной яркостью [7].

Настоящее исследование направлено на уменьшение радиометрических ошибок изображений, полученных при помощи БПЛА для картирования растительности. Картирование растительности – это ряд действий, связанных с получением изображений, предварительной обработкой, обработкой и последующим отображением растительного покрова на определенной территории. Эта задача крайне важна и необходима для наблюдения, интерпретации и описания окружающей среды, поскольку растительность связана с почвами, на которых она произрастает, климатом и экологическими факторами [8].

Знание состояния растительности представляет собой ценную информацию для специалистов в одном из важнейших для человечества направлении – сельском хозяйстве. Известно, что для создания карт растительности широко используются методы дистанционного зондирования Земли (ДЗЗ), которые связаны с данными, получаемыми с различного типа датчиков, установленных стационарно на спутниках, самолетах или БПЛА [9]. Каждая из традиционных технологий ДЗЗ, применяемая для картирования растительности, имеет пространственно-временные, технологические, эксплуатационные и экономические ограничения.

Спутниковые датчики одновременно позволяют отображать большие территории, однако пространственное разрешение полученных данных невысокое для свободно распространяемых данных (10 м), а коммерческие (0,5 м) данные достаточно дороги для широкого применения [10]. Кроме того, оптические многоспектральные датчики не позволяют получить изображение поверхности Земли ввиду наличия сплошного или разорванного облачного покрова. Это приводит к ограничениям в привязке времени получения спутникового изображения к фазам фенологического цикла из-за, в принципе, случайного времени сбора данных.

Самолетные исследования можно планировать более гибко, привязывая даты вылета к фазам фенологического цикла растений, однако для таких измерений необходимы большие площади, которые все же приводят к измерениям, которые оказываются сложными и дорогостоящими. В этом плане БПЛА имеют определенные преимущества по сравнению со спутниковыми или самолетными технологиями измерений, обеспечивая безоблачные изображения с очень высоким пространственным разрешением, относительно простой работой, экономичностью, надежностью, мобильностью и безопасностью [11]. Однако при всех плюсах есть и недостаток, связанный с тем, что измерения можно проводить на относительно небольших площадях с определенной зависимостью от погодных условий (например, ветер до 10 м/с). Тем не менее беспилотные летательные аппараты позволяют планировать однотипные маршруты для одного и того же места, в результате чего получаются данные, которые позволяют выявлять динамику состояния растительности.

При картировании растительности беспилотные летательные аппараты могут применять классические цифровые RGB-датчики или мультиспектральные камеры, которые позволяют рассчитывать различные индексы растительности (Greenness, NDVI и др.) [12]. Эти расчеты позволяют выполнять пространственно-временной анализ и получать количественную оценку состояния растительного покрова, определение видового состава и структуры растений. Для формирования карт растительности необходимо решить основные проблемы, связанные с учетом условий получения изображений с БПЛА, а именно, геометрии (изменение формы изображения при наклоне) и радиометрии (изменение освещенности, шумы и др.). Поскольку БПЛА имеют небольшие размеры (относительно самолетного или вертолетного типа БПЛА), то они имеют меньшую стабильность пространственного положения датчика во время полетов. Отчасти при этом проблема геометрической точности совмещения изображений в мозаику решена за счет большого количества перекрывающихся изображений между собой (от 50 до 80%) и современных математических алгоритмов.

Одной из менее изученных сторон коррекции изображений, полученных с БПЛА, являются радиометрические и атмосферные искажения, которые могут возникать по разным причинам, например, использование датчиков получения изображений с широким полем зрения, учета движения солнца в зависимости от времени дня, что приводит к разному уровню освещенности изображений, прозрачности атмосферы или наличия облачности, которая влияет на уровень освещения территории, где проходят измерения, а отдельные облака могут приводить к изменению цвета пикселей на изображениях за счет темных пятен на поверхности.

По этой причине необходимо перед тем, как будет создана мозаика изображений, применять методы атмосферной коррекции, которая включает изменение коэффициента отражения поверхности, который зависит от положения солнца (зенитный угол и азимут), типа поверхности, рельефа (топографии), и атмосферную поправку на прозрачность атмосферы. Для решения этих задач необходимо применить методы, которые позволят повысить точность картирования растительности.

Методика атмосферной коррекции

Важно заметить, что любое изображение, полученное с помощью БПЛА оптическими датчиками, заставляет учитывать радиометрические характеристики, поскольку получаемые изображения зависят от яркости солнечного света, типа поверхности, высоты полета и др. На рис. 1 показана упрощенная схема того, как оптический датчик, установленный на БПЛА, находящийся на определенной высоте, получает информацию, которая представляется в виде RGB-изображения.

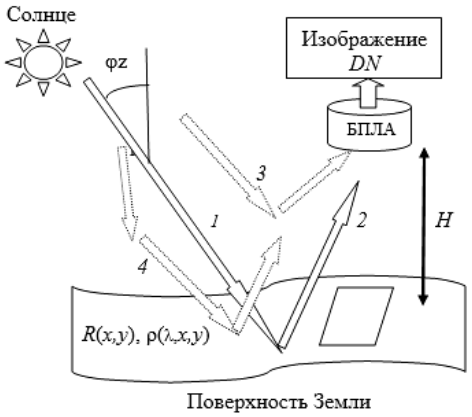

Рис. 1. Схема видов излучения, достигающих цифровую камеру, установленную на БПЛА: *1* – падающее солнечное излучение; *2* – отраженное от поверхности солнечное падающее излучение; *3* – рассеянное излучение атмосферой; *4* – диффузное излучение

На рис. 1 показано прямое направление распространения солнечного излучения сквозь толщу атмосферы (путь *1*), которое при этом частично поглощается и рассеивается атмосферой, затем отражается от поверхности (путь *2*) и в дальнейшем попадает в поле зрения камеры и на матрицу RGB (величина *DN*). На значения *DN* влияет изменение факторов окружающей среды, таких как атмосферные условия (например, прозрачность атмосферы за счет туманов или аэрозолей, пожаров и др.), отражательная способность соседних объектов, а также φ*z* зенитный угол солнца (см. рис. 1). Если не учитывать эти факторы, тогда данные эффекты попадут в полученные результаты, которые будут, во-первых, случайными, во-вторых, зависимыми от погодных условий. По этой причине необходимо выполнить преобразование значений *DN* с учетом атмосферной коррекции в отражательную способность поверхности, что представляет собой основу калибровки, которая выполняется перед другими процессами обработки изображений.

Атмосферная коррекция особенно важна для сравнения изображений поверхности Земли, полу-

ченных за несколько периодов времени одним и тем же датчиком, но при различных условиях освещения и атмосферных условиях (погода). Необходимо это сделать и для сшивки изображений, при получении мозаики, так как каждое изображение будет отличаться по уровню освещенности ввиду изменения положения солнца и состояния погоды. Эта разница и влияет на длительность процесса сшивания перекрывающихся изображений или получения неоднородной мозаики (ортофотоплана). Это же приводит и к снижению точности оценки отражательной способности, а значит, расчета индексов растительности и последующих результатов классификации (определения типов поверхности [10]).

Выпишем основные уравнения, которые позволяют увидеть взаимосвязь измеряемых показателей *DN*, и уравнения переноса солнечного излучения в атмосфере и для простоты будем считать, что поверхность создает ламбертовскую яркость отраженного солнечного излучения на входе в объектив датчика $E(\lambda)$. Учитывая, что высота полета БПЛА в типичных условиях измерений (получения изображений) не превышает 100–200 м, прозрачность атмосферы между поверхностью Земли (см. рис. 1, путь *2*) и БПЛА равна единице и влияние остальных факторов минимально за счет того, что размер апертуры A незначителен, и тогда можно записать:

$$E(\lambda,\varphi_z) = E_o(\lambda)\cdot\cos(\varphi_z)\cdot\rho(\lambda,x,y)\cdot R(x,y)\cdot\tau_1(\lambda,\varphi_z)/(d\cdot\pi), \quad (1)$$

где φ_z – зенитный угол; $E_o(\lambda)$ – внеатмосферное солнечное излучение на длине волны λ; $\tau_1(\lambda)$ – коэффициенты пропускания атмосферы по направлениям от солнца к поверхности (см. рис. 1, путь *1*) соответственно; $\rho(\lambda,x,y)$ – спектральный коэффициент отражения для точки на поверхности (x,y); $R(x,y)$ – коэффициент, учитывающий рельеф поверхности; d – относительное расстояние Солнце–Земля.

Согласно выражению (1), отраженное излучение, падающее на объектив цифровой камеры БПЛА, зависит от времени дня (определяется зенитным углом, который зависит от широты и долготы местности), времени года (определяется величиной d). Измеренный сигнал цифровой камерой может быть записан в виде

$$DN(i) = C\cdot\int E(\lambda,\theta,\varphi_z)\cdot S_i(\lambda))\cdot d\lambda, \quad (2)$$

где C – коэффициент, связанный с характеристиками камеры; $S_i(\lambda)$ – спектральная функция канала RGB (рис. 2).

На рис. 2 приведены кривые спектральных функций каналов RGB, применяемые цифровой камерой (Sony 6000A). Из рис. 2 видно, что амплитуды каналов имеют различную величину и крылья кривых спектральных каналов пересекаются между собой, что влияет на межканальное влияние измеряемого отраженного солнечного излучения.

Учитывая уравнения (1) и (2), появляется возможность оценить отражательную способность в точке пространства (x,y) по формуле

$$\rho(\lambda(i)) = (d\cdot\pi\cdot DN(i))/\{\int E_o(\lambda)\cdot\cos(\varphi_z)\cdot R\cdot\tau_1(\lambda,\varphi_z)\cdot d\lambda\}. \quad (3)$$

Оптические цифровые камеры, установленные на БПЛА, регистрируют значения *DN* вместо коэффициента отражения поверхности, и поэтому необходимо выполнить коррекцию измерений (полученного изображения). К сожалению, производители цифровых камер не всегда предоставляют информацию о характеристиках матриц цифровых камер и особенно спектральных функций каналов S_i, что затрудняет процесс коррекции коэффициента отражения. Другой аспект коррекции связан с атмосферной поправкой, т.е. учетом атмосферных эффектов, которые зависят от высоты полета и погодных условий района измерений (величина τ_1). Воздействие атмосферы на солнечное излучение связано с рассеянием аэрозолями и молекулами, а также поглощением газов атмосферы. Поглощение газами в видимой области связано с малыми компонентами по содержанию O_3, NO_2, SO_2 и др., а также водяным паром и углекислым газом. Поэтому любые изменения погоды вызывают вариации содержания газовых и аэрозольных компонентов, особенно водяного пара (например, до и после дождя), что ведет к изменению прозрачности атмосферы. И в этом плане возникает необходимость учитывать эти изменения, так как они влияют на расчет индексов Greenness (таблица).

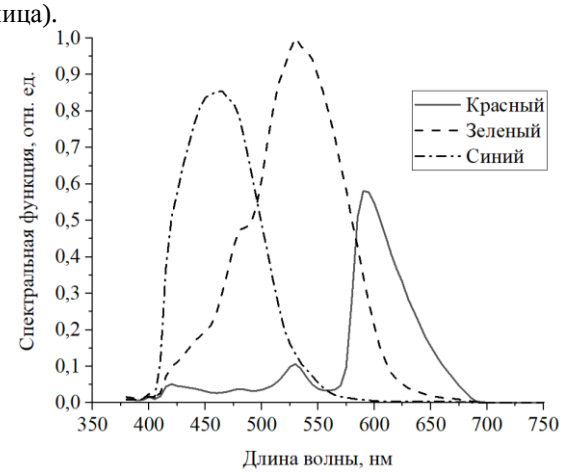

Рис. 2. Спектральные функции каналов RGB (R – красный, G – зеленый и B – синий) цифровой камеры

Индексы растительности Greenness

Название индекса	Формула
Coloration Index (CI)	$(R - B)/R$
Brightness Index (BI)	$\sqrt{((R^{**}2 + G^{**}2 + B^{*}2)/3}$
Soil Colour Index (SGI)	$(R–G)/(R + G)$
Green leaf index (GLI)	$(2^{*}G – R – B)/(2^{*}G + R + B)$
Green-Red Vegetation Index (GRVI)	$(G – R)/(G + R)$

Как было сказано выше, важными для практического применения изображений, полученных с помощью цифровой камеры, установленной на БПЛА, после коррекции и построения мозаики являются индексы растительности (Greenness). Для расчета индексов растительности используют два (как правило, R и G) спектральных канала или более (R, G, B). По величине вычисленного соотношения между каналами можно изучать характеристики растительности и обеспечивать сравнение этих характеристик в различные моменты времени. Так,

например, база данных Indexdatabase [13] содержит более 500 формул индексов растительности. В таблице приведены некоторые индексы Greenness.

Полученные результаты

Для применения предлагаемого способа было разработано программное обеспечение, структура основных блоков которого представлена на рис. 3. При вычислении уравнения (3) необходимо для изображения, которое имеет определенные географические координаты, учитывать метеорологические данные (профиль температуры и влажности), которые нами берутся с ресурса [14]. Данные профилей температуры и влажности необходимы для расчета пропускания атмосферы по программе 6S [15]. Программа 6S для расчета использует фиксированные модели атмосферы для трех климатических зон: тропических, средних и полярных, а также двух периодов года (зима и лето), что делает их неточными для применения в конкретной географической точке и дате года. Поэтому нами текущие данные погоды передаются в программу 6S для расчета пропускания. Координаты поля необходимы для учета рельефа $R(x,y)$, характеристики которого рассчитываются на основе базы данных SRTM [16]. Внеатмосферный спектр солнца E_o берется нами из ресурса [17].

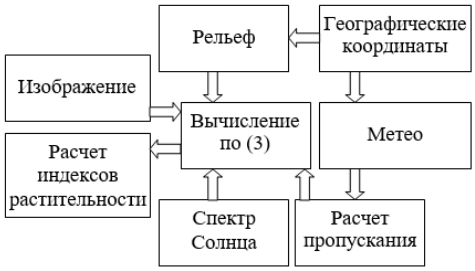

Рис. 3. Структура основных блоков программы

Для тестирования разработанной программы нами были взяты восемь изображений, полученных с помощью камеры, установленной на БПЛА, для изучаемого поля, которое находится в Заречном участке Томской области в период с июня по август 2019 г., на котором выращивалась озимая пшеница. Конкретные даты получения изображений в 2019 г.: 1) 01.06; 2) 08.06; 3) 06.07; 4) 13.07; 5) 27.07; 6) 03.08; 7) 10.08; 8) 24.08.

На рис. 4 показаны гистограммы распределения значений индекса BI (см. таблицу) для трех дат в 2019 г. (06.06; 13.07 и 10.08) и для двух случаев, когда взяты исходные изображения, скорректированные по формуле (3).

Из рис. 4 видно, что гистограммы исходных изображений отличаются от скорректированных центром максимума в сторону уменьшения и незначительного возрастания. Также надо отметить, что центры максимумов гистограмм соответствуют основному фенологическому циклу роста озимой пшеницы [18], что показано на рис. 5, где приведены значения максимумов для всех восьми дат полученных изображений.

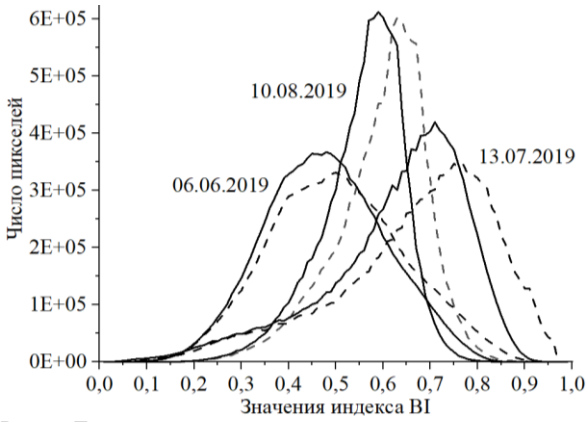

Рис. 4. Гистограммы распределения значений индекса BI для трех дат исходных изображений (пунктирная кривая) и коррекция по формуле (3) (сплошная кривая)

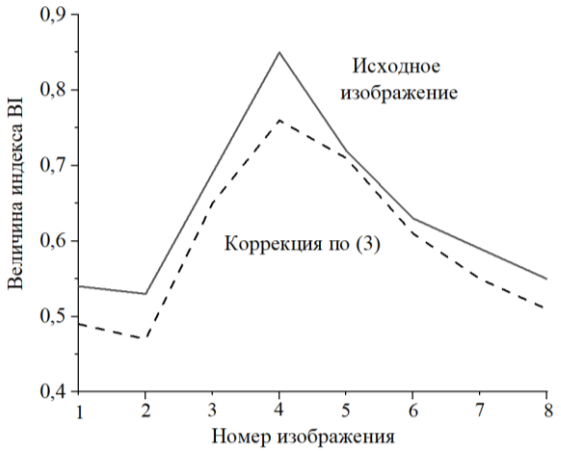

Рис. 5. Максимумы гистограмм значений индекса растительности BI для восьми дат получения изображений

Из рис. 5 видно, что коррекция получаемых изображений на атмосферные эффекты составляет около 10%, что важно для решения разнообразных практических задач сельского хозяйства. В данной работе получены результаты, которые определяют методику атмосферной коррекции изображений, полученных цифровыми камерами, установленными на беспилотных летательных аппаратах, в задаче изучения растительности.

Заключение

В статье рассмотрено влияние изменений падающего солнечного излучения во время полетов БПЛА в разное время суток и дней года, которые вызваны изменением солнечного излучения и факторами погоды (наличием облаков и/или прозрачностью атмосферы), на изображение. Разница в величине излучения влияет на однородность яркости изображений цифровых камер, установленных на БПЛА, что вызывает необходимость выполнить радиометрическую коррекцию. Особенно это важно в дни, когда часть изображений получена при ясном небе, где преобладает прямое солнечное излучение в изображении, а другая – при наличии облаков, когда преобладают эффекты рассеяния. В таком случае средняя яркость изображения будет меняться, что приведет к изменению величины индекса расти-

тельности, а значит, неточному пониманию состояния растений. Процесс радиометрической коррекции выполняется для каждого спектрального канала RGB в отдельности, что позволяет более точно оценивать индекс растительности, а значит, и состояние растений. Полученные результаты обработки реальных изображений показывают применимость предлагаемой методики на практике при решении разнообразных задач.

Литература

1. Рэндл У. Малые беспилотные летательные аппараты. Теория и практика / У. Рэндл, Т. Биард. – М.: Радар ММС, 2014. – 184 с.

2. Компания Геоскан [Электронный ресурс]. – Режим доступа: https://www.geoscan.aero/ru, свободный (дата обращения: 01.10.2021).

3. Компания Agisoft [Электронный ресурс]. – Режим доступа: https://www.agisoft.com, свободный (дата обращения: 01.10.2021).

4. Компания Dronemapper [Электронный ресурс]. – Режим доступа: https://dronemapper.com, свободный (дата обращения: 01.10.2021).

5. Компания Pix4d [Электронный ресурс]. – Режим доступа: https://www.pix4d.com, свободный (дата обращения: 01.10.2021).

6. Mohammed A.B.E.A. Color balance for panoramic images / A.B.E.A. Mohammed, F. Ming, F. Zhengwei // Modern Applied Science. – 2015. – Vol. 9, No. 13. – P. 140–147.

7. Катаев М.Ю. Коррекция освещённости многовременных RGB-изображений, получаемых с помощью беспилотного летательного аппарата / М.Ю. Катаев, М.М. Дадонова, Д.С. Ефременко // Светотехника. – 2020. – № 6. – С. 19–25.

8. Катаев М.Ю. Оценка состояния хвойных растений методами компьютерного зрения / М.Ю. Катаев, А.В. Кислов, Е.А. Самохин // Доклады ТУСУР. – 2020. – Т. 23, № 1. – С. 70–75.

9. Катаев М.Ю. Методы технического зрения для картирования состояния сельскохозяйственных полей / М.Ю. Катаев, К.С. Ёлгин, И.Б. Сорокин // Доклады ТУСУР. – 2018. – Т. 21, № 4. – С. 75–80.

10. Шовенгердт Р.А. Дистанционное зондирование. Модели и методы обработки изображений. – М.: Техносфера, 2010. – 560 с.

11. Фетисов В.С. Беспилотная авиация: терминология, классификация, современное состояние / В.С. Фетисов, Л.М. Неугодникова, В.В. Адамовский, Р.А. Красноперов. – Уфа: ФОТОН, 2014. – 217 с.

12. Rasmussen J. Are vegetation indices derived from consumer-grade cameras mounted on UAVs sufficiently reliable for assessing experimental plots? /J. Rasmussen, G. Ntakos, J. Nielsen, J. Svensgaard, R.N. Poulsen, S. Christensen // Eur. J. Agron. – 2017. – Vol. 74. – P. 75–92.

13. База данных Indexdatabase [Электронный ресурс]. – Режим доступа: https://www.indexdatabase.de/db/i.php, свободный (дата обращения: 01.10.2021).

14. Метеорологический онлайн ресурс Ventusky [Электронный ресурс]. – https://www.ventusky.com, свободный (дата обращения: 01.10.2021).

15. Vermote E.F. Second Simulation of the Satellite Signal in the Solar Spectrum, 6S: An Overview / E.F. Vermote, D. Tanre, J.L. Deuze, M. Herman, J.-J. Morcrette // IEEE Trans. Geosci. Remote Sens. – 1997. – Vol. 35, No. 3. – P. 675–686.

16. Космическое агентство NASA [Электронный ресурс]. – Режим доступа: https://www2.jpl.nasa.gov/srtm, свободный (дата обращения: 01.10.2021).

17. Компания NREL [Электронный ресурс]. – https://www.nrel.gov/grid/solar-resource/spectra.html, свободный (дата обращения: 01.10.2021).

18. Tao F. Spatiotemporal changes of wheat phenology in China under the effects of temperature, day length and cultivar thermal characteristics / F. Tao, S. Zhang, Z. Zhang // Europ. J. Agronomy. – 2012. – No. 43. – P. 201–212.

Катаев Михаил Юрьевич
Д-р техн. наук, профессор каф. автоматизированных систем управления (АСУ) Томского государственного университета систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-36, +7-960-975-27-85
Эл. почта: kmy@asu.tusur.ru

Карташов Евгений Юрьевич
Канд. техн. наук, доцент каф. машин и аппаратов химических и атомных производств
Северского технологического института Национального исследовательского ядерного университета «МИФИ»
Коммунистический пр-т, 65, г. Северск, Россия, 636036
Тел.: (382-3) 78-02-40, +7-905-991-66-92
Эл. почта: kart.62@yandex.ru

Смирнов Дмитрий Сергеевич
Магистрант каф. АСУ ТУСУРа
Ленина пр-т., 40, г. Томск, Россия, 634050
Тел.: +7 (382-2) 70-15-36
Эл. почта: the.smd.public@gmail.com

Kataev M.Yu., Kartashov E.Yu., Smirnov D.S.

Methodology and software for atmospheric correction of images obtained with unmanned aircraft to allow the safe location of vegetation

Unmanned aerial vehicles (UAV) provide a way to obtain images with high spatial resolution with relatively simple control of the vehicle and economic efficiency. Over the past 10 years, UAV measurement technology has changed significantly and has become popular due to its versatility and ease of use in commercial and scientific research. It should be noted that the methods of processing one-time received images allow solving various scientific and practical problems, however, during monitoring, when the dynamics of the state of objects (surface types) of the same territory is studied, the methodology and software remain questionable. One of the problems that hinder the study, for example, the dynamics of the state of objects on an agricultural field, is the radiometric accuracy of the obtained UAV images. In practice, the radiometric accuracy of measurements allows considering various lighting conditions at different periods of the day and year, by relevant types of digital sensors (digital cameras) used. The study is aimed at enabling a better flexibility when studying the dynamics of the state of objects located on the same territory at different times by taking into account the radiometric errors of UAV images when mapping the state of vegetation.

The research methodology uses the real images of the UAV obtained from June to August 2019 for an agricultural field with winter wheat.

Keywords: unmanned aerial vehicles, image, atmospheric correction, vegetation mapping, vegetation indices.
DOI: 10.21293/1818-0442-2021-24-4-73-78

References

1. Randle W., Bard T. *Small unmanned aerial vehicles. Theory and practice*. Moscow, Radar MMS, 2014. 184 p. (in Russ.)

2. Company Geoscan. Available at: https://www.geoscan.aero/ru, free (Accessed: October 01, 2021) (in Russ.).

3. Agisoft company. Available at: https://www.agisoft.com, free/ (Accessed: October 01, 2021) (in Russ.).

4. Company Dronemapper. Available at: https://dronemapper.com, free (Accessed: October 01, 2021) (in Russ.).

5. Company Pix4d Available at: https://www.pix4d.com, free (Accessed: October 01, 2021) (in Russ.).

6. Mohammed A.B.E.A., Ming F., Zhengwei F. Color balance for panoramic images. *Modern Applied Science*, 2015, vol. 9, no. 13, pp. 140–147.

7. Kataev M.Yu., Dadonova M.M., Efremenko D.S. Illumination correction of multi-time RGB images obtained using an unmanned aerial vehicle. *Lighting*, 2020, no. 6, pp. 19–25 (in Russ.)

8. Kataev M.Yu., Kislov A.V., Samokhin E.A. Assessment of the state of coniferous plants by computer vision methods. *Proceedings of TUSUR University*, 2020, vol. 23, no. 1, pp. 70–75 (in Rus.).

9. Kataev M.Yu., Yolgin K.S., Sorokin I.B. Methods of technical vision for mapping the state of agricultural fields. *Proceedings of TUSUR University*, 2018, vol. 21, no. 4, pp. 75–80 (In Russ.).

10. Shovengerdt R.A. *Remote sensing. Models and Methods of Image Processing*. Moscow, Technosphere, 2010. 560 p. (in Russ.).

11. Fetisov V.S., Neugodnikova L.M. *Unmanned Aircraft: Terminology, Classification, Current State*. Ufa. FOTON, 2014. 217 p. (in Russ.).

12. Rasmussen J., Ntakos J., Nielsen J., Svensgaard J., Poulsen R.N., Christensen S. Are vegetation indices derived from consumer-grade cameras mounted on UAVs sufficiently reliable for assessing experimental plots? *European Journal of Agronomy*, 2017, vol. 74, pp. 75–92.

13. Database Indexdatabase. Available at: https://www.indexdatabase.de/db/i.php, free (Accessed: October 01, 2021) (in Russ.).

14. Meteorological online resource Ventusky. Available at: https://www.ventusky.com, free (Accessed: October 01, 2021) (in Russ.).

15. Vermote E.F., Tanre D., Deuze J.L., Herman M., Morcrette J.-J. Second Simulation of the Satellite Signal in the Solar Spectrum, 6S. An Overview. *IEEE Transactions on Geoscience and Remote Sensing*, 1997, vol. 35, no. 3, pp. 675–686.

16. Space Agency NASA Available at: https://www2.jpl.nasa.gov/srtm, free (Accessed: October 01, 2021) (in Russ.).

17. Company NREL Available at: https://www.nrel.gov/grid/solar-resource/spectra.html, free (Accessed: October 01, 2021) (in Russ.).

18. Tao F., Zhang S., Zhang Z. Spatiotemporal changes of wheat phenology in China under the effects of temperature, day length and cultivar thermal characteristics *European Journal of Agronomy*, 2012, vol. 43, pp. 201–212.

Mikhail Yu. Kataev
Doctor of Science in Engineering, Professor
Department of Automated Control Systems (ACS),
Scientific Director of the Center for Space Monitoring
of the Earth from Space, Tomsk State University
of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 70-15-36, +7-960-975-27-85
Email: kmy@asu.tusur.ru

Evgeny Yu. Kartashov
Candidate of Science in Engineering, Associate Professor,
Department of Machines and Devices of Chemical
and Nuclear Production, Seversk Technological Institute,
National Research Nuclear University «MEPhI»
65, Kommunistichesky pr., Seversk, Russia, 636036
Phone: +7 (382-3) 78-02-40, +7-905-991-66-92
Email: kart.62@yandex.ru

Dmitry S. Smirnov
Master student Department of ACS TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7 (382-2) 70-15-36
Email: the.smd.public@gmail.com

УДК 681.523.4

В.Т. Тран, А.М. Кориков, Т.Т. Нгуен

Выбор регулятора, работающего в скользящем режиме, для автоматизированной транспортной системы

Выполнен синтез скользящих регуляторов для возвратно-поступательной гидравлической системы с сервоклапаном. Такие регуляторы работают на нижнем (первом) уровне интеллектуальной системы навигации и управления автоматизированной транспортной системы. Предложено два типа скользящих регуляторов: статический и динамический. В программной среде MatLab SIMULINK выполнено моделирование статического и динамического скользящих регуляторов. Оба регулятора работают эффективно и устойчиво. Однако при наличии помех динамический скользящий регулятор показал превосходство над статическим скользящим регулятором по помехоустойчивости и точности стабилизации.

Ключевые слова: автоматизированная транспортная система, синтез, скользящий режим, скользящий регулятор, статический скользящий регулятор, динамический скользящий регулятор, моделирование, выбор регулятора.
DOI: 10.21293/1818-0442-2021-24-4-79-84

Автоматизированные транспортные системы (АТС) широко используются в промышленности и во многих других отраслях экономики для решения задач логистики, организации и реализации материальных грузопотоков [1]. В истории развития АТС известны периоды подъема (и даже эйфории), спада (например, в ФРГ в конце 1980 г. было много сообщений о практических случаях использования АТС, когда они не оправдали себя с точки зрения логистики, гибкости и экономичности). Затем изготовители АТС доказали, что АТС надежно функционируют, их новые компоненты (например, в сфере навигации и передачи информации по радио) освоены, а требуемая безопасность персонала и оборудования при эксплуатации достигнута. В настоящее время АТС известны во многих вариантах исполнения, и их применение выходит за пределы производственных корпусов и складских помещений [1].

Однако работа АТС на открытых производственных территориях (вне производственных корпусов) порождает проблемы, многие из которых не решены до настоящего времени: например, на этих территориях возможны вибрации транспортного оборудования и, в частности, транспортной (грузовой) платформы, возможны различного рода шумы и помехи, возникающие из-за метеоусловий и других внешних факторов. Решение этих проблем для АТС возможно с помощью системы автоматической стабилизации (САС), расположенной на нижнем (первом) уровне интеллектуальной системы навигации и управления (ИСНУ) АТС [2]. САС обеспечивает горизонтальную стабилизацию транспортной (грузовой) платформы АТС, что является актуальной задачей при работе АТС за пределами производственных корпусов и складских помещений [1]. Для практики АТС представляют интерес гидравлические САС. Гидравлические САС обладают известными достоинствами [3, 4]: компактная конструкция, высокая производительность, быстрая реакция, надежная работа в сочетании со скользящим контроллером с широким диапазоном регулирования, высокая помехоустойчивость и высокая точность расчета управляющего сигнала [5, 6]. Выбор скользящего режима работы контроллера (регулятора) САС обусловлен тем, что этот режим управления обладает свойством независимости управления от характеристик неизменяемой части САС [7–10]. В этой связи актуальность решения задачи выбора регулятора САС, работающего в скользящем режиме, для нижнего уровня ИСНУ АТС становится очевидной.

Постановка задачи

Для задачи выбора регулятора, работающего в скользящем режиме, для нижнего уровня ИСНУ АТС выберем модель гидравлической САС, представленную на рис. 1.

Эта модель представляет собой возвратно-поступательную гидравлическую автоматическую систему с сервоклапаном, на которую действуют переменные нагрузки.

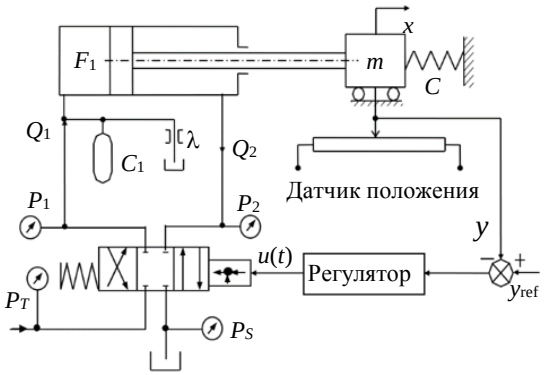

Рис. 1. Модель гидравлической САС

Параметры модели: m – движущаяся масса; F_1 – площадь поршня; P_1 – перепад давления в 2 камерах цилиндра; K_A – коэффициент усиления усилителя; K_V – коэффициент усиления клапана; I – управляющий ток сервоклапана; $u(t)$ – напряжение сигнала управления; y – расстояние перемещения объекта, м; K_0 – коэффициент слива масла сервоклапана; C – жесткость пружины; λ – коэффициент потерь пото-

ка; V – объем масла в гидравлической камере; B – модуль упругости масла; f – коэффициент вязкого трения масла.

Предполагая линейность исследуемой системы, в ней рассматривается вертикальное движение массы m с учетом влияния силы тяжести $P = mg$, представим её математическую модель в виде уравнений:

$$\begin{cases} K_V I - K_0 P_1 = F_1 \dfrac{dy}{dt} + \dfrac{V}{2B}\dfrac{dP_1}{dt} + \lambda P_1, \\ F_1 P_1 = m\dfrac{d^2y}{dt} + Cy + f\dfrac{dy}{dt} + mg. \end{cases} \quad (1)$$

Выполним синтез скользящего закона управления для описанной модели гидравлической САС.

Синтез регулятора, работающего в скользящем режиме

Введем переменные состояния системы [11–13]:

$$x_1 = y; \quad x_2 = \frac{dy}{dt}; \quad x_3 = P_1 .$$

Тогда система уравнений (1) перепишется следующим образом:

$$\begin{cases} \dot{x}_1 = x_2, \\ \dot{x}_2 = -g - \dfrac{C}{m}x_1 - \dfrac{f}{m}x_2 + \dfrac{F_1}{m}x_3 + dt, \\ \dot{x}_3 = \dfrac{2BK_v I}{V} - \dfrac{2F_1 B}{V}x_2 - \left(\dfrac{2BK_0}{V} + \dfrac{2B\lambda}{V}\right)x_3. \end{cases} \quad (2)$$

Задача состоит в том, чтобы определить управляющий сигнал $u(t) = K_A I$ так, чтобы выходной сигнал $y(t)$ соответствовал установленному сигналу $y_{\text{ref}}(t)$. Решение данной задачи возможно в двух вариантах: синтез статического и синтез динамического регуляторов скольжения. Рассмотрим последовательно эти задачи.

Синтез статического ползункового регулятора

Выберем уравнение поверхности скольжения [7] в виде

$$S(e) = k_1 e + k_2 \dot{e} + \ddot{e}, \quad (3)$$

где $e = x_1 - y_{\text{ref}}$, k_1, k_2 – константы, выбранные таким образом, что характеристический многочлен уравнения $S(e) = 0$ удовлетворяет критерию устойчивости Гурвица [12].

Подставляя $e = x_1 - y_{\text{ref}}$ в уравнение (3), получим

$$S(e) = k_1(x_1 - y_{\text{ref}}) + k_2\dot{x}_1 + \ddot{x}_1. \quad (4)$$

Из (2) и (4) имеем

$$S(t) = \left(k_1 - \frac{C}{m}\right)x_1 + \left(k_2 - \frac{f}{m}\right)x_2 + \frac{F_1}{m}x_3 - k_1 y_{\text{ref}} - g + dt, \quad (5)$$

$$\dot{S}(e) = \left(k_1 - \frac{C}{m}\right)\dot{x}_1 + \left(k_2 - \frac{f}{m}\right)\dot{x}_2 + \frac{F_1}{m}\dot{x}_3. \quad (6)$$

Из (2) и (6) имеем

$$\dot{S}(e) = \frac{gf}{m} - k_2 g + \left(k_2 - \frac{f}{m}\right)dt + \left(\frac{Cf}{m^2} - \frac{Ck_2}{m}\right)x_1 +$$

$$+\left(k_1 - \frac{k_2 f}{m} + \frac{f^2}{m^2} - \frac{2F_1^2 B}{mV} - \frac{C}{m}\right)x_2 -$$

$$-\left(\frac{2BK_0F_1}{mV} + \frac{F_1 f}{m^2} + \frac{2B\lambda F_1}{mV} - \frac{F_1 k_2}{m}\right)x_3 + \frac{2BK_v F_1}{mK_A V}u. \quad (7)$$

Для ошибки $e \to 0$ ($y \to y_{\text{ref}}$), тогда $\dot{S}S < 0$ или $\dot{S}$ имеет знак, противоположный S:

$$\dot{S} = -K\text{sign}(S). \quad (8)$$

Комбинируя (7) и (8), получим следующее выражение для управляющего напряжения:

$$u = \frac{mK_A V}{2BK_v F_1}\left[k_2 g - \frac{gf}{m} - \left(\frac{Cf}{m^2} - \frac{Ck_2}{m}\right)x_1 - \left(k_1 - \frac{k_2 f}{m} + \frac{f^2}{m^2} - \right.\right.$$

$$\left. - \frac{2F_1^2 B}{mV} - \frac{C}{m}\right)x_2 + \left(\frac{2BK_0F_1}{mV} + \frac{F_1 f}{m^2} + \frac{2B\lambda F_1}{mV} - \frac{F_1 k_2}{m}\right)x_3 -$$

$$\left. - K\,\text{sign}(s)\right]. \quad (9)$$

Тогда $u = K_A I$.

Синтез динамического ползункового регулятора

Выберем уравнение поверхности скольжения [7] в виде

$$S(e) = k_3 e + k_2 \dot{e} + k_1 \ddot{e} + \dddot{e}, \quad (10)$$

где $e = x_1 - y_{\text{ref}}$, k_1, k_2, k_3 – константы, выбранные так же, как и в уравнении (3), т.е. $S(e) = 0$ удовлетворяет критерию устойчивости Гурвица.

Подставляя $e = x_1 - y_{\text{ref}}$ в уравнение (10), получим

$$S(e) = \dddot{x}_1 + k_1\ddot{x}_1 + k_2\dot{x}_1 + k_3 x_1 - k_3 y_{\text{ref}}, \quad (11)$$

где

$$\dddot{x}_1 = \ddot{x}_2 = \frac{2BK_v F_1 I}{mV} + \frac{gf}{m} - \frac{f}{m}dt + \frac{Cf}{m^2}x_1 +$$

$$+\left(\frac{f^2}{m^2} - \frac{2F_1^2 B}{mV} - \frac{C}{m}\right)x_2 - \left(\frac{2BK_0F_1}{mV} + \frac{F_1 f}{m^2} + \frac{2B\lambda F_1}{mV}\right)x_3. \quad (12)$$

Из (2), (11) и (12) имеем

$$S(e) = \frac{2BK_v F_1}{K_A mV}u + \left(\frac{Cf}{m^2} + k_3\right)x_1 +$$

$$+\left(\frac{f^2}{m^2} - \frac{2F_1^2 B}{mV} - \frac{C}{m} - \frac{k_1 f}{m} + k_2\right)x_2 +$$

$$+\left(\frac{k_1 F_1}{m} - \frac{2BK_0F_1}{mV} - \frac{F_1 f}{m^2} - \frac{2B\lambda F_1}{mV}\right)x_3 +$$

$$+\frac{gf}{m} - k_1 g - k_3 y_d - \frac{f}{m}dt + k_1 dt. \quad (13)$$

Введем обозначения:

$$b = \frac{2BK_v F_1}{K_A mV}; \quad a_1 = \frac{Cf}{m^2} + k_3 - \frac{Ck_1}{m};$$

$$a_2 = \frac{f^2}{m^2} - \frac{2F_1^2 B}{mV} - \frac{C}{m} - \frac{k_1 f}{m} + k_2;$$

$$a_3 = \frac{k_1 F_1}{m} - \frac{2BK_0F_1}{mV} - \frac{F_1 f}{m^2} - \frac{2B\lambda F_1}{mV};$$

$$a_4 = \frac{gf}{m} - k_1 g - k_3 y_d - \frac{f}{m}dt + k_1 dt .$$

Тогда уравнение (13) будет переписано так:

$$S(e) = bu + a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 , \quad (14)$$

$$\dot{S}(e) = b\dot{u} + a_1 \dot{x}_1 + a_2 \dot{x}_2 + a_3 \dot{x}_3 . \quad (15)$$

Из (2) и (15) имеем

$$\dot{S}(e) = b\dot{u} + b_1 u + c_1 x_1 + c_2 x_2 + c_3 x_3 - a_2 (g - dt), \quad (16)$$

где

$$b_1 = \frac{2a_3 B K_v}{K_A V}; \; c1 = -\frac{a_2 C}{m}; \; c_2 = a_1 - \frac{a_2 f}{m} - \frac{2a_3 F_1 B}{V};$$

$$c_3 = \frac{a_2 F_1}{m} - \frac{2a_3 B K_0}{V} - \frac{2a_3 B\lambda}{V} .$$

Для ошибки $e \to 0$ ($y \to y_{\text{ref}}$) тогда $\dot{S}S < 0$ или $\dot{S}$ имеет знак, противоположный S:

$$\dot{S} = -K \operatorname{sign}(S) \quad (17)$$

Из (16) и (17) имеем

$$b\dot{u} + b_1 u + c_1 x_1 + c_2 x_2 + c_3 x_3 - a_2 g = -K \operatorname{sign}(S),$$

$$\dot{u} = -\frac{1}{b}((b_1 u + c_1 x_1 + c_2 x_2 + c_3 x_3 - a_2 g) + K \operatorname{sign}(S)) . \quad (18)$$

Моделирование и оценка результатов

Вычислительными и экспериментальными методами выбираем следующие параметры моделирования: движущаяся масса m = 500 (кг); площадь поршня F_1 = 31.2 (см^2); коэффициент усиления усилителя K_A = 500; коэффициент усиления клапана K_V = 10; коэффициент усиления обратной связи K_C = 5; коэффициент слива масла сервоклапана K_0 = 2,58·10^{-12} м^{3}с$^{-1}$Па$^{-1}$; жесткость пружины C = 0,1 Нм$^{-1}$; коэффициент потерь потока λ = 5,10^{-3}; объем масляной камеры V = 652,8 см^3; модуль упругости масла B = 0,1; коэффициент вязкого трения масла f = 588 (Нсм$^{-1}$).

Моделирование статического регулятора скольжения

Уравнение поверхности скольжения (6) и уравнение управляющего напряжения (9) используются при моделировании в программной среде MatLab SIMULINK [13] с коэффициентами k_1 = 21,5; k_2 = 6,8; K = 100|S|. Начальное положение объекта m 15 см, на рис. 2 показана, что система сходится к нулю примерно за 2 с, на рис. 3 – давление в полости цилиндра вернулось к своему исходному давлению, т.е. система устойчивая. На рис. 4 показан сигнал управляющего напряжения, управляющее напряжение перешло в 0, когда система находится в установившемся режиме, колебания управляющего напряжения довольно малы, потому что мы выбрали коэффициент K = 100|S|.

Таким образом, при статическом скользящем регуляторе с выбранным коэффициентом система приходит в установившийся режим примерно через 2 с, управляющее напряжение достаточно стабильно, но для гидравлической системы желательно, чтобы сигнал управления уменьшал колебательность.

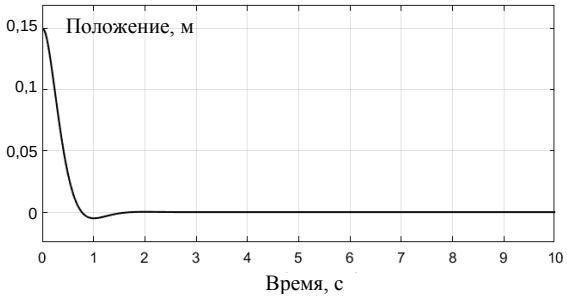

Рис. 2. Стабилизация положения для статического скользящего регулятора

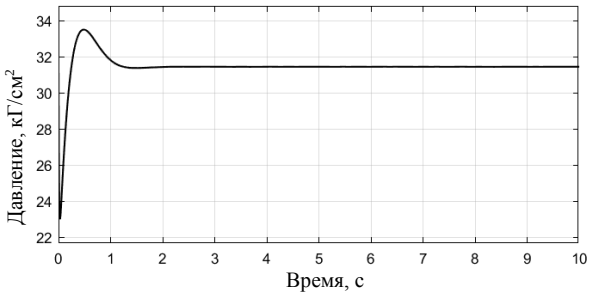

Рис. 3. Стабилизация давления для статического скользящего регулятора

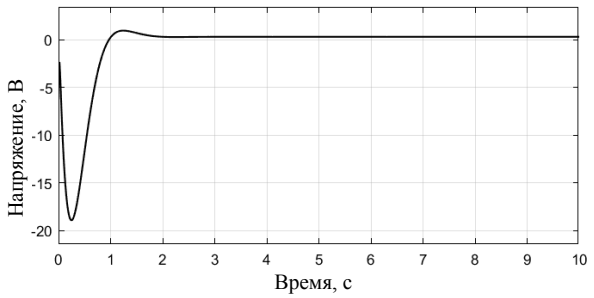

Рис. 4. Реакция на управляющий сигнал для статического скользящего регулятора

Моделирование динамического регулятора скольжения

Уравнение поверхности скольжения (14) и уравнение управляющего напряжения (18) используются при моделировании в программной среде MatLab SIMULINK [13] с коэффициентами k_1 = 25, k_2 = 300, k_3 = 1000, K = 100|S|. Начальное положение объекта m 15 см, на рис. 5 показано, что система сходится к нулю примерно за 1,5 с. На рис. 6 – давление в полости цилиндра вернулось к своему исходному давлению, т. е. система устойчивая. На рис. 7 показан сигнал управляющего напряжения, управляющее напряжение перешло в 0, когда система находится в установившемся режиме, колебания управляющего напряжения малы, так как выбрали коэффициент K = 100|S|.

Таким образом, при статическом скользящем регуляторе с выбранным коэффициентом система приходит в установившийся режим примерно через 1,5 с, управляющее напряжение стабильно.

Сравнение контроллеров

Моделирование в программной среде MatLab SIMULINK показало, что как статические, так и ди-

намические регуляторы работают эффективно, из рис. 8 и 9 видно, что система сходится и стабилизируется через 1,5–2 с. Однако из рис. 10 следует, что скорость схождения регулятора динамического скольжения стабильна и менее изменчива в точке равновесия (0,0).

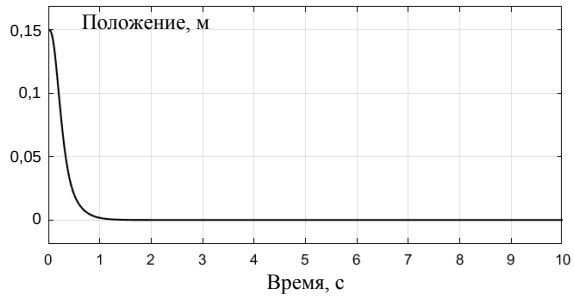

Рис. 5. Стабилизация положения для динамического скользящего регулятора

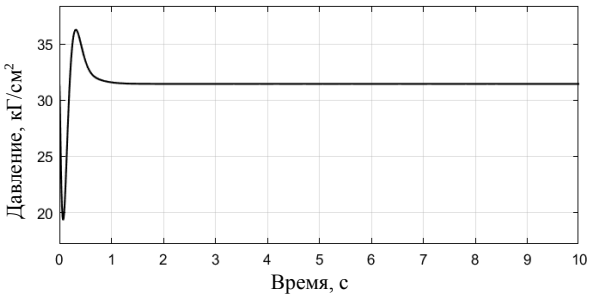

Рис. 6. Стабилизация давления для динамического скользящего регулятора

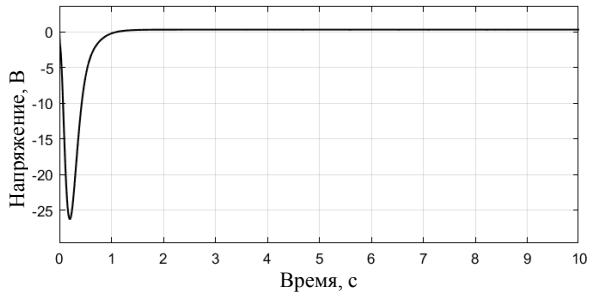

Рис. 7. Реакция на управляющий сигнал для динамического скользящего регулятора

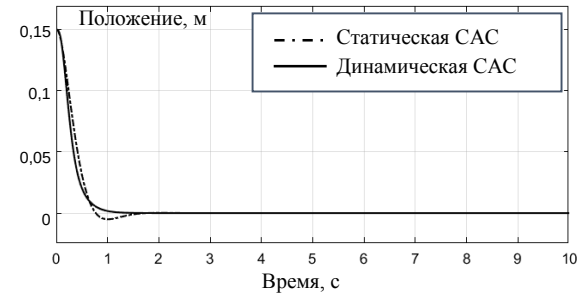

Рис. 8. Стабилизация положения для статического и динамического скользящего регулятора

Для гидравлических и механических систем, работающих в условиях помех, воздействие шума и колебаний управляющего сигнала вокруг плоскости скольжения влияет на стабильность системы и может повредить механические соединения. Следовательно, желательно уменьшить амплитуду зашумленного сигнала, а также колебания управляющего сигнала вокруг плоскости скольжения.

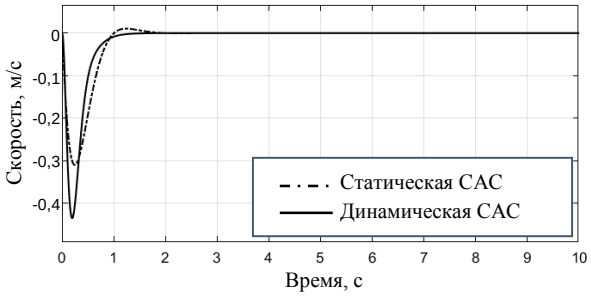

Рис. 9. Стабилизация скорости для статического и динамического скользящего регулятора

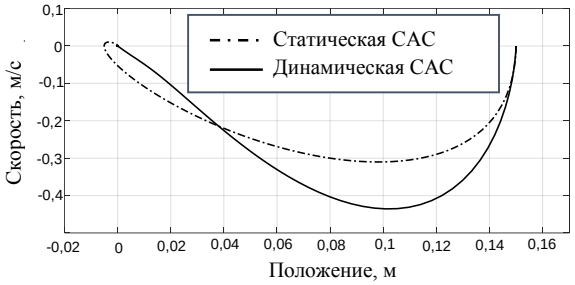

Рис. 10. Реакция на $x_1(t)\to 0$, $x_2(t)\to 0$, $S(x_1, x_2)\to 0$ для статического и динамического скользящего регулятора

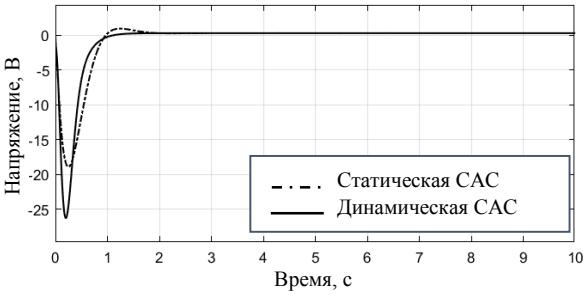

Рис. 11. Реакция на управляющий сигнал для статического и динамического скользящего регулятора

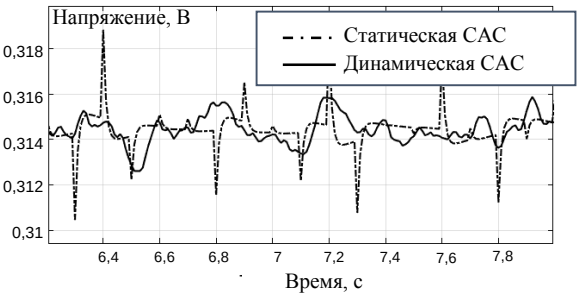

Рис. 12. Реакция на управляющий сигнал для статического и динамического скользящего регулятора

Из рис. 11 видно, что при выборе коэффициента $K = 100\ |S|$ колебания управляющего сигнала вокруг скользящей плоскости обоих контроллеров умень-

шены, но из рис. 12 следует, что амплитуда шумовой составляющей управляющего сигнала меньше для динамического скользящего контроллера. Это показывает значительное преимущество динамического скользящего контроллера для гидромеханической системы.

Из результатов моделирования скользящих регуляторов следует, что амплитуда колебаний давления в полости цилиндра гидравлической системы под действием шума также значительно уменьшается, если используется динамический скользящий регулятор, а это уменьшает нежелательные вибрации на механических соединениях, что увеличивает их срок службы.

Таким образом, сравнивая качество работы статического скользящего регулятора и динамического скользящего регулятора для возвратно-поступательной гидравлической системы с сервоклапанами, мы обнаруживаем, что динамический скользящий регулятор имеет выдающиеся преимущества, такие как: стабильная работа, уровень колебаний управляющего сигнала вокруг плоскости скольжения мал, амплитуда колебаний шумового сигнала значительно снижена. Это приводит к повышению качества работы системы и увеличению срока работы механических соединений.

Заключение

Выполнен синтез скользящих регуляторов для возвратно-поступательной гидравлической системы с сервоклапаном. Предложено два типа скользящих регуляторов: статический и динамический. В программной среде MatLab Simulink выполнено моделирование статического и динамического скользящих регуляторов. Оба регулятора работают эффективно и устойчиво. Однако при наличии помех динамический скользящий регулятор показал превосходство над статическим скользящим регулятором по помехоустойчивости и точности стабилизации. Отметим, что синтез скользящих регуляторов выполнен в предположении линейности исследуемой САС. Учет нелинейностей, присущих любой реальной системе [14, 15], существенно усложняет исследование.

Литература

1. Автоматизированные транспортные системы [Электронный ресурс]. – Режим доступа: https://sitmag.ru/article/10545-kamo-gryadeshi-ats, свободный (дата обращения: 02.12.2021).

2. Кориков А.М. Интеллектуальное управление в технических системах // Научный вестник НГТУ. – 2014. – № 1 (54). – С. 18–26.

3. Хохлов В.А. Электрогидравлические следящие системы / В.А. Хохлов, В.Н. Прокофьев. Н.А. Борисова, В.И. Гусаков, В.М. Чуркин. – М.: Машиностроение, 1971. – 432 с.

4. Bessa W.M. Slidingmode control with adaptive fuzzy dead-zone compen-sation of an electro-hydraulic servo-system / W.M. Bessa, M.S. Dutra, E. Kreuzer // Journalof Intelligent and Robotic Systems. – 2010. – Vol. 58, No. 1. – P. 3–16.

5. Bartolini G. Modern Sliding Mode Control Theory: New Perspectives and Applications / G. Bartolini, L. Fridman, A. Pisano, E. Usai. – Berlin: Heidelberg: Springer, 2008. – 468 p.

6. Sliding Mode Control Methodology in the Applications of Industrial Power Systems / J. Liu, Y. Gao, Y. Yin, J. Wang, W. Luo, G. Sun. – Springer Nature Switzerland, 2020. – 205 p.

7. Теория систем с переменной структурой / под ред. С.В. Емельянова. – М.: Наука. Гл. ред. физ.-мат. лит., 1970. – 592 с.

8. Zhou Z. Mimo fuzzy sliding mode control for three-axis inertially stabilizedplatform / Z. Zhou, B. Zhang, D. Mao // Sensors. – 2019. – Vol. 19, No. 7. – P. 1658.

9. Qian D. Hierarchical sliding mode control for a class of simo under-actuated systems / D. Qian, J. Yi, D. Zhao // Control and cybernetics. – 2008. – Vol. 37, No. 1. – P. 159.

10. Almutairi N.B. On the sliding mode control of a ball on a beam system / N.B. Almutairi, M. Zribi // Nonlinear dynamics. – 2010. – Vol. 59, No. 1. – P. 221–238.

11. Справочник по теории автоматического управления / под ред. А.А. Красовского. – М.: Наука. Гл. ред. физ.-мат. лит., 1987. – 712 с.

12. Кориков А.М. Основы теории управления: учеб. пособие. – 2-е изд. – Томск: Изд-во НТЛ, 2002. – 392 с.

13. Дорф Р. Современные системы управления / Р. Дорф, Р. Бишоп. – М.: Лаборатория базовых знаний, 2004. – 832 с.

14. Попов Е. П. Прикладная теория процессов управления в нелинейных системах. – М.: Наука, 1973. – 584 с.

15. Алфёров С.М. Манометры: моделирование и автоматизация процессов градуировки / С.М. Алфёров, А.М. Кориков. – Томск: Изд-во ТУСУРа, 2017. – 147 с.

Тран Ван Трук
Аспирант каф. каф. автоматизированных систем управления (АСУ) Томского государственного университета систем управления и радиоэлектроники (ТУСУР)
Ленина прт, 40, г. Томск, Россия, 634050
Тел.: +7-923-428-02-82
Эл. почта: att82glass@gmail.com

Кориков Анатолий Михайлович
Д-р техн. наук, проф. каф. АСУ ТУСУРа,
вед. науч. сотр. Томского ф-ла
Федерального исследовательского центра
информационных и вычислительных технологий СО РАН
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-913-869-96-37
Эл. почта: korikov@asu.tusur.ru.

Нгуен Тхань Тьен
Д-р, доцент технического университета «Ле Куи Дон» и Института военной механики, г. Ханой, Вьетнам
Тел.: +8-439-744-98-15
Эл. почта: ngttienktd@gmail.com

Tran V.T., Korikov A.M., Nguyen T.T.

Selection of a sliding mode controller for an automated transport system

The article presents the synthesis of sliding regulators for a reciprocating hydraulic system with a servo valve. Such regulators operate at the lower (first) level of the intelligent navigation and control system of the automated transport system. Two types of sliding regulators are proposed: static and

dynamic. Static and dynamic sliding regulators are simulated in the MatLab SIMULINK software environment. Both regulators work efficiently and steadily. However, in the presence of interference, the dynamic sliding controller showed superiority over the static sliding controller in terms of noise immunity and stabilization accuracy.

Keywords: automated transport system, synthesis, sliding mode, sliding controller, static sliding controller, dynamic sliding controller, simulation, controller selection.
DOI: 10.21293/1818-0442-2021-24-4-79-84

References

1. Avtomatizirovannye transportnye sistemy. [Automated transportation systems] Available at: https://sitmag.ru/ article/10545-kamo-gryadeshi-ats, free (Accessed: December 02, 2021).

2. Korikov A.M. *Intellektualnoe upravlenie v tehnicheskih sistemah* [Intelletual control in technical systems]. *Nauchny vestnik NGTU*. 2014, № 1 (54), pp. 18–26.

3. Khohlov V.A., Prokofev V.N., Borisova N.A., Gusakov V.I., Churkin V.M., *Elektrogidravlicheskie sledyashhie sistemy* [Electro-hydraulic servo systems]. Moscow, Mashinostroenie, 1971, 432 p.

4. Bessa W.M., Dutra M.S., Kreuzer E. Slidingmode control with adaptive fuzzy dead-zone compensation of an electro-hydraulic servo-system. *Journal of Intelligent and Robotic Systems,* 2010, vol. 58, no. 1, pp. 3–16.

5. Bartolini G., Fridman L., Pisano A., Usai E. Modern Sliding Mode Control Theory: New Perspectives and Applications. – Berlin, Heidelberg: Springer, 2008, 468 p.

6. Liu J., Gao Ya., Yin Yu., Wang J., Luo W., Sun G. Sliding Mode Control Methodology in the Applications of Industrial Power Systems. – Springer Nature Switzerland, 2020, 205 p.

7. *Teoriya sistem s peremennoj strukturoj* [Systems theory with an established structure]. Ed. S.V. Emel`yanova. – Moscow, Nauka. Gl. red. fiz.-mat. lit., 1970, 592 p.

8. Zhou Z., Zhang B., Mao D. Mimo fuzzy sliding mode control for three-axis inertially stabilizedplatform. *Sensors*, 2019, vol. 19, no. 7, pp. 1658.

9. Qian D., Yi J., Zhao D. Hierarchical sliding mode control for a class of simo under-actuated systems. *Control and cybernetics*, 2008, vol. 37, no. 1, p. 159.

10. Almutairi N.B., Zribi M. On the sliding mode control of a ball on a beam system. *Nonlinear dynamics*, 2010, vol. 59, no. 1, pp. 221–238.

11. Spravochnik po teorii avtomaticheskogo upravleniya [Handbook of Automatic Control Theory]. Ed. A.A. Krasovskogo. Moscow, Nauka. Glavnaya redaktsiya fiziko-matematicheskoy literatury, 1987, 712 p.

12. Korikov A.M. *Osnovy teorii upravleniya: uchebn. posobie* [Fundamentals of Control Theory: Study Guide]. 2nd ed. Tomsk, NTL publ., 2002, 392 p.

13. Dorf R., Bishop R. *Sovremennye sistemy upravleniya* [Modern control systems]. Moscow, Laboratoriya bazovyh znanij, 2004, 832 p.

14. Popov E.P. *Prikladnaya teoriya processov upravleniya v nelinejnyh sistemah* [Applied theory of control processes in nonlinear systems]. Moscow, Nauka, 1973, 584 p.

15. Alfyorov S.M., Korikov A.M. Manometry`: Modelirovanie i avtomatizaciya processov graduirovki [Pressure gauges: simulation and automation of calibration processes]. Tomsk, TUSUR Publishing Office, 2017, 147 p.

Van Truc Tran
Postgraduate student, Department of Automated Control Systems Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050;
Phone: +7-923-428-02-82
Email: att82glass@gmail.com

Anatoly M. Korikov
Doctor of Science in Engineering, Professor,
Department of Automated Control Systems TUSUR
40, Lenin pr., Tomsk, Russia, 634050;
Leading Researcher, Tomsk Branch of the Institute of Computing Technologies of the Siberian Branch of Russian Academy of Sciences
Phone: +7 (382-2) 70-15-36
Email: korikov@asu.tusur.ru

Thanh Tien Nguyen
Ph. D, Associate Professor,
Le Quy Don Technical University and Military Institute of Mechanical Engineering, Hanoi, Vietnam
Phone: +8-439-744-98-15
Email: ngttienktd@gmail.com

УДК 519.111.3+004.823

Д.В. Кручинин

База знаний коэффициентов k-степени производящих функций двух переменных

Рассматриваются вопросы построения базы знаний коэффициентов степеней производящих функций двух переменных, явные выражения которых описываются алгеброй биномиальных коэффициентов. Предлагается методика получения таких выражений. Описывается структура элементов базы знаний. Представлена структура программной системы. Описаны примеры.

Ключевые слова: производящая функция, коэффициент, числовая пирамида, база знаний, методика получения пирамид, программная система.

DOI: 10.21293/1818-0442-2021-24-4-85-89

Развитие систем компьютерной алгебры требует создания математических баз знаний, позволяющих организовать поиск и манипулирование сложными математическими объектами. Производящие функции являются одним из таких объектов, которые находят применение в различных прикладных математических дисциплинах: перечислительная комбинаторика, статистика, теория чисел, комбинаторная генерация, теория ортогональных полиномов, анализа алгоритмов и т.д.

Существующие базы знаний направлены на получение новых знаний конкретных чисел или последовательностей чисел, например, можно выделить www.worldofnumbers.com [1] или oeis.org [2–4]. В системах компьютерной алгебры имеются программные модули для работы с производящими функциями. Однако они имеют ограниченные возможности по выполнению операций нахождения явных выражений композиции, обращения производящих функций и решения функциональных уравнений. Для выполнения операции композиции производящих функций одной переменной известна реализация модуля в системе Maxima [5]. Однако выполнение указанных операций для производящих функций многих переменных не реализовано.

Недавние исследования математического аппарата композиции производящих функций многих переменных [7–12] позволили решить указанные задачи по получению явных выражений коэффициентов производящих функций многих переменных и найти подходы и алгоритмы для реализации этой операции в системах компьютерной алгебры. Важнейшее значение при выполнении этих операций играют коэффициенты *k*-степени производящих функций многих переменных. Первым шагом в этом направлении является создание соответствующей базы знаний для производящих функций одной и двух переменных и их коэффициентов *k*-степени, описываемых алгеброй биномиальных коэффициентов.

Основные понятия и методы

Переход на исследование коэффициентов степеней производящих функций многих переменных открыл новые возможности для решения задач, основанных на применении композиции производящих функций многих переменных и решения смежных задач. Для описания численного представления коэффициентов *k*-степени производящих функций двух переменных воспользуемся понятием тензора как многомерной таблицы [6].

Запишем основные соотношения для коэффициентов степеней производящих функций двух переменных.

Пусть задана производящая функция вида

$$U_{num}(x,y)=\sum_{n\geqslant 0}\sum_{m\geqslant 0}u(n,m)x^n y^m.$$

Тогда пирамидой будем называть трехмерный тензор, формируемый выражением

$$T_{num}(n,m,k)=[x^n y^m]U_{num}(x,y)^k,$$

где $T_{num}(n,m,k)$ описывается выражением, состоящим из произведения или деления биномиальных коэффициентов, а также рациональных выражений, состоящих из переменных n, m, k и констант. Например, для производящей функции

$$U(x,y)=\frac{1}{1-x-y}$$

описываемая ею пирамида будет задана формулой

$$T(n,m,k)=[x^n y^m]U(x,y)^k=\binom{n+m}{n}\binom{n+m+k-1}{n+m}.$$

Производящая функция для тензора $T(n,m,k)$ будет иметь вид

$$F(x,y,z)=\sum_{n,m,k}T(n,m,k)x^n y^m z^k=\frac{1}{1-zU(x,y)}.$$

Для всех пирамид выполняются условия:

$$T(0,0,0)=1,\quad m=0,n=0,$$
$$T(n,m,0)=0,\quad m>0,n>0,$$
$$T(n,m,k)=0,\quad m<0 \text{ или } n<0 \text{ или } k<0.$$

Пирамида является коэффициентами *k*-степени производящей функции $U(x,y)$. Тогда для пирамиды можно записать рекуррентное выражение вида

$$T(n,m,k)=\sum_{i=0}^{n}\sum_{j=0}^{m}T(i,j,k-1)u\left(n-i,m-j\right).$$

Основные соотношения для пирамид

Пусть задана взаимная производящая функция

$$U_r(x,y)=\frac{1}{U(x,y)},$$

где известна пирамида $T_{num}(n,m,j)$. Тогда пирамида для взаимной функции будет иметь выражение [12]

$$T_r(n,m,k)=\sum_{j=0}^{n+m}U_0^{-k-j}(-1)^j\binom{k+j-1}{j}T_U(n,m,j)\binom{n+m+k}{n+m-j},$$

где $U_0=U(0,0)$.

На основании использования теоремы Лагранжа об обращении рядов двух переменных [13, 14] запишем функциональное уравнение

$$A(x,y)=U(xA(x,y),y).$$

Для $U(x,y)$ известна пирамида $T(n,m,k)$. Тогда для пирамиды, описываемой функцией $A(x,y)$, будет справедлива формула

$$T_A(n,m,k)=\frac{k}{n+k}T_U(n,m,n+k),$$

где $T_A(n,m,k)=[x^n y^m]A(x,y)^k$.

Представленные формулы для взаимной и реверсивной пирамид позволяют получить следующую схему отношений между пирамидами:

$$\begin{array}{ccccc}\rightarrow & T_U(n,m,k) & \rightarrow & T_A(n,m,k) & \rightarrow\\ & \updownarrow & & \updownarrow & \\ \leftarrow & T_U^R(n,m,k) & \leftarrow & T_A^R(n,m,k) & \leftarrow\end{array}$$

Пусть задано уравнение реверсии

$$A_r(x,y)U(xA_r(x,y),y)=x.$$

Тогда

$$T_{rev}(n,m,k)=\frac{k}{n+k}\sum_{j=0}^{n+m}(0,0,1)^{-n-k-j}(-1)^j T(n,m,j)\times$$
$$\times T\binom{n+k+j-1}{j}\binom{2n+m+k}{n+m-j}.$$

Аналогично будет выражение для реверсии по переменной y:

$$yA_r(x,y)U(x,yA_r(x,y))=y.$$

Реверсивная пирамида будет иметь вид

$$T_{rev}(n,m,k)=\frac{k}{m+k}\sum_{j=0}^{n+m}U_0^{-m-k-j}(-1)^j T(n,m,j)\times$$
$$\times\binom{m+k+j-1}{j}\binom{2m+n+k}{n+m-j}.$$

Взаимная рекурсивная пирамида по переменной x задается уравнением

$$\frac{x}{A_r(x,y)U(xA_r(x,y),y)}=x.$$

Тогда пирамида описывается следующей формулой:

$$T_{rrx}(n,m,k)=k\sum_{j=1}^{n+m}\frac{U_0^{-n+k-j}}{j}(-1)^{j-1}T(n,m,j)\times$$
$$\times\binom{n-k+j-1}{j-1}\binom{2n+m-k}{n+m-j},$$

где $U_0=U(0,0),T_{rrx}(0,0,k)=T(0,0,k),k>0.$

Методика получения пирамид

Рассмотрим методику получения пирамид. Для этого запишем множество производящих функций одной переменной и соответствующее множество явных выражений коэффициентов k-степени. Пусть имеется множество $G=\{g_i(x)\}_{i=1}^N$ производящих функций. Коэффициенты k-степени описываются биномиальными коэффициентами, представленными треугольниками $\{T_i(n,k)\}_{i=1}^N$. Пример такого множества приведен в таблице. Необходимо отметить, что данная таблица существенно ограничена и используется в качестве примера. Выбираем $g_1(x)\in G$ и $g_2(x)\in G$ и строим новую функцию двух переменных. Можно предложить два способа получения пирамид производящей функции двух переменных:

1. На основе произведения и композиции производящих функций $g_1(x)\in G$ и $g_2(x)\in G$;

2. На основе решения уравнения Лагранжа для функций $g_1(x)\in G$ и $g_2(x)\in G$.

Рассмотрим первый метод получения пирамид. Выбираем $g_1(x)\in G$ и $g_2(x)\in G$ и строим новую производящую функцию двух переменных вида

$$U(x,y)=g_1(x\cdot g_2(y)).$$

Тогда пирамида функции $U(x,y)$ будет иметь выражение

$$T_U(n,m,k)=T_1(n,k)\cdot T_2(m,n).$$

В общем случае можно записать функцию

$$U(x,y)=g_1(x\cdot g_2(y)^a)^b g_2(y)^c,$$

где $a,b,c\in N$.

Тогда пирамида функции $U(x,y)$ будет иметь выражение

$$T_U(n,m,k)=T_1(n,bk)\cdot T_2(m,an+ck).$$

Рассмотрим второй метод, основанный на уравнении Лагранжа. Выбираем $g_1(x)\in G$ и $g_2(x)\in G$. Записываем уравнение общего вида

$$U(x,y)=g_1{}^a\left(xU(x,y)g_2{}^b(y)\right)g_2{}^c(y),$$

где $a,b,c\in N$.

Тогда

$$T_U(n,m,k)=\frac{k}{n+k}T_1(n,a(n+k))\cdot T_2(m,bn+c(n+k)).$$

Как видим, можно получить неограниченное число пирамид. Однако, ограничив параметры a,b,c, получим фиксированное число пирамид.

Структура системы поддержки базы знаний

База знаний производящих функций, их коэффициентов и тензорных представлений имеет следующую структуру:

1) десятичный четырехзначный номер производящей функции;

2) явное выражение производящей функции;

3) явное выражение тензора производящей функции;

4) программа генерации представления выражения производящей функции в формате Latex;

5) программа генерации представления выражения производящей функции в формате Maxima;

6) программа генерации представления выражения тензора в формате Latex;

7) программа генерации представления выражения тензора функции в формате Maxima;

8) URL-ссылки на последовательности онлайн-энциклопедии целых последовательностей;

9) ссылки на другие производящие функции.

Множество производящих функций и их тензоры

Производящая функция $G(x)$	Треугольник $T(n,k)$
$g_1(x)=1+x$	$T(n,k)=\binom{k}{n}$
$g_2(x)=\frac{1}{1-x}$	$T(n,k)=\binom{n+k-1}{n}$
$g_3(x)=\frac{1-\sqrt{1-4x}}{2x}$	$T(n,k)=\frac{k}{n+k}\binom{2n+k-1}{n}$
$g_4(x,y)=\frac{1+\sqrt{1+4x}}{2}$	$T(n,k)=\frac{k(-1)^{n-1}\binom{2n-k-1}{n-1}}{n}$
$g_5(x)=\frac{2}{\sqrt{3x}}\sin\left(\frac{\arcsin\left(\frac{\sqrt{27x}}{2}\right)}{3}\right)$	$T(n,k)=\frac{k\binom{3n+k-1}{n}}{2n+k}$
$g_6(x)=\left(\frac{\sqrt{x(27x+4)}}{23^{\frac{3}{2}}}+\frac{x}{2}+\frac{1}{27}\right)^{\frac{1}{3}}+\frac{1}{9\left(\frac{\sqrt{x(27x+4)}}{23^{\frac{3}{2}}}+\frac{x}{2}+\frac{1}{27}\right)^{\frac{1}{3}}}+\frac{1}{3}$	$T(n,k)=\frac{k(-1)^{n-1}\binom{3n-k-1}{n-1}}{n}$
$g_7(x)=\sqrt{\frac{1-\sqrt{1-16x}}{8x}}$	$T(n,k)=\begin{cases}\frac{k4^n\binom{\frac{4n+k}{2}-1}{n}}{2n+k}, & k\ even,\\ \frac{k\binom{\frac{4n+k-1}{2}}{n}\binom{4n+k-1}{\frac{4n+k-1}{2}}}{(2n+k)\binom{2n+k-1}{\frac{2n+k-1}{2}}}, & k\ odd.\end{cases}$

На рис. 1 представлена структура программной системы поддержки базы знаний коэффициентов *k*-степени производящих функций двух переменных. Рассмотрим описание модулей системы.

1. Модуль управления базой пирамид обеспечивает ввод / редактирование данных и программ пирамиды.

2. Модуль поиска запроса производит синтаксический анализ запроса пользователя, при неверном запросе формирует сообщение об ошибке, при верном запросе производит его преобразование для дальнейшей обработки, поиск подходящей пирамиды в базе знаний и формирует список пирамид. Если в результате поиска список пуст, то формируется соответствующее сообщение.

3. Модуль определения отношений для заданной пирамиды производит вычисление взаимной, инверсной, реверсной и обратной инверсной пирамид и поиск их в базе знаний. Кроме того, он вычисляет свойства пирамиды, такие как симметрия.

4. Модуль тестирования и редактирования производит по запросу пользователя редактирование элементов базы знаний и их тестирование. Производится два вида тестирования:

1) проверка на дублирование элементов базы знаний, дублирование не допустимо;

2) проверка на соответствие производящей функции и ее тензора, проверка производится следующим образом: *k*-степень производящей функции разлагается в ряд Тейлора, извлекаются значения

коэффициентов и записываются в соответствующий тензору массив, затем производится вычисление тензора по явной формуле и сравниваются два полученных тензора.

5. Модуль генерации производит построение энциклопедии производящих функций и их тензоров и записывает их в формате Latex.

Программная реализация данной базы знаний осуществлена на языке системы компьютерной алгебры Maxima, который содержит свыше 600 специальных функций для символьных вычислений и преобразования математических выражений. Разработанная система содержит свыше 6 000 функций и математических выражений. В ходе создания программного обеспечения и создания базы знаний были выявлены программные ошибки в системах компьютерной алгебры Maxima и пакете символьных вычислений Sympy для языка Python.

В настоящее время в базе знаний насчитывается 1 502 производящих функций и их тензорных представлений.

На рис. 2 приведен пример вывода страницы пирамиды под номером 77. На ней отображены:

1) формула производящей функции;

2) явная формула пирамиды $T_{77}(n,m,k)$;

3) таблица разложения производящей функции $U_{77}(x,y)$;

4) ссылки на связанные пирамиды. Здесь левая пирамида под номером 76 и пирамида с переменой мест *x* и *y* под номером 71;

5) текст программ на языке Maxima.

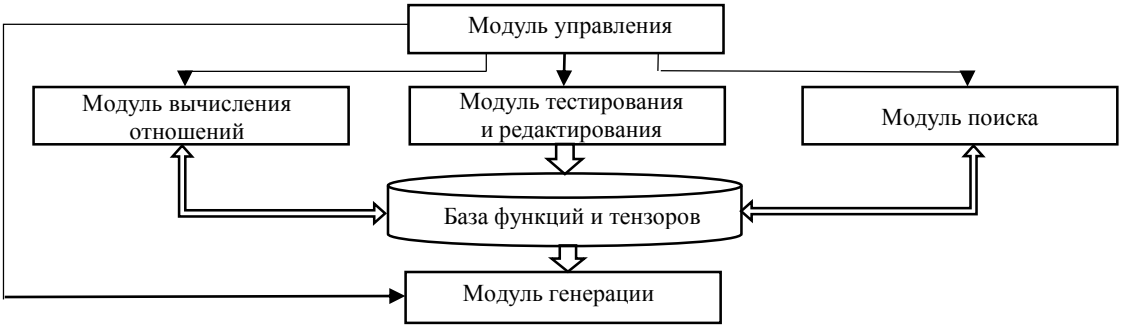

Рис. 1. Структура электронной энциклопедии пирамид

1.2.77 Pyr77

Generating function:

$$U_{77}(x,y)=\frac{1-2x+x^2-\sqrt{1-4x+6x^2-4x^3+x^4-4y}}{2y}$$

Formula:

$$T_{77}(n,m,k)=\frac{k\binom{2m+k-1}{m}\binom{n+2(2m+k)-1}{n}}{m+k}$$

Data:

1	1	2	5	14	42	132
2	6	20	70	252	924	3432
3	21	110	525	2394	10626	46332
4	56	440	2800	15960	85008	432432
5	126	1430	11900	83790	531300	3135132
6	252	4004	42840	368676	2762760	18810792
7	462	10010	135660	1413258	12432420	97189092

Left on y: UU0076(x,y)
Change x y: UU0071(x,y)

(Maxima)	Programm Code
UU0077(x,y):=	((-sqrt((-4*y)+x^4-4*x^3+6*x^2-4*x+1))+x^2-2*x+1) /(2*y)
Tuu0077(n,m,k):=	(k*binomial(2*m+k-1,m)*binomial(n+2*(2*m+k)-1,n)) /(m+k)

Рис. 2. Пример фрагмента вывода информации, описывающей пирамиду 77

Выводы

Построенная база знаний база знаний коэффициентов степеней производящих функций двух переменных станет инструментом проведения теоретических и прикладных исследований в областях перечислительной комбинаторики, комбинаторной генерации, теории специальных полиномов и др. Предложенная база знаний позволит развить возможности систем компьютерной алгебры в части выполнения операций композиции и обращения производящих функций многих переменных. Послужит развитию математического онлайн-образования.

Литература

1. World!Of numbers. – URL: http://www.worldofnumbers.com (дата обращения: 12.02.2022).

2. Sloane N.J.A. A handbook of integer sequences. – USA, New York: Academic Press, 1973. – 206 p.

3. Sloane N.J.A. The encyclopedia of integer sequences / N.J.A. Sloane, S. Plouffe. – USA, San Diego: Academic Press, 1995. – 587 p.

4. Sloane N.J.A. The on-line encyclopedia of integer sequences // Notices of the American Mathematical Society. – 2018. – Vol. 65, No. 9. – P. 1063–1074.

5. Перминова М.Ю. Программный модуль получения явных выражений коэффициентов производящих функций, основанных на использовании композиции // Доклады ТУСУР. – 2017. – Т. 20, № 1. – С. 65–69.

6. Оселедец И.В. Рекурсивное разложение многомерных тензоров / И.В. Оселедец, Е.Е. Тыртышников // Доклады Академии наук. – 2009. – Т. 427, № 1. – С. 14–16.

7. Kruchinin D. Method for obtaining coefficients of powers of bivariate generating functions / D. Kruchinin, V. Kruchinin, Y. Shablya // Mathematics. – 2021. – Vol. 9, No. 4. – Article 428.

8. Kruchinin D.V. Application of a composition of generating functions for obtaining explicit formulas of polynomials / D.V. Kruchinin, V.V. Kruchinin // Journal of Mathematical Analysis and Applications. – 2013. – Vol. 404, No. 1. – P. 161–171.

9. Kruchinin V.V. Composita and its properties / V.V. Kruchinin, D.V. Kruchinin // Journal of Analysis & Number Theory. – 2014. – Vol. 2, No. 2. – P. 37–44.

10. Kruchinin D. A method for obtaining generating functions for central coefficients of triangles / D. Kruchinin, V. Kruchinin // Journal of Integer Sequences. – 2012. – Vol. 15, No. 9. – Article 12.9.3.

11. Kruchinin D.V. On solving some functional equations // Advances in Difference Equations. – 2015. – Vol. 2015, No. 1.

12. Kruchinin D.V. Explicit formula for reciprocal generating function and its application / D.V. Kruchinin, V.V. Kruchinin // Advanced Studies in Contemporary Mathematics (Kyungshang). – 2019. – Vol. 29, No. 3. – P. 365–372.

13. Gessel I.M. A combinatorial proof of the multivariable Lagrange inversion formula // Journal of Combinatorial Theory, Series A. – 1987. – Vol. 45, No. 2. – P. 178–195.

14. Stanley R.P. Enumerative combinatorics. – Vol. 2. – USA: Cambridge University Press, 2001. – 595 p.

Кручинин Дмитрий Владимирович
Канд. физ.-мат. наук, доцент каф. компьютерных систем в управлении и проектировании (КСУП)
Томского государственного ун-та систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0003-3412-432X
Тел.: +7 (382-2) 41-47-17
Эл. почта: kruchinindm@gmail.com

Kruchinin D.V.

Knowledge base for coefficients of k-power on generating functions in two variables

The questions of building a knowledge base of the coefficients of the powers of generating functions in two variables are considered, their explicit expressions are described by the algebra of binomial coefficients. A method to obtain such expressions is proposed. Both the structure of knowledge base elements and the structure for the software system are presented, illustrated with examples.

Keywords: generating function, coefficient, numerical pyramid, knowledge base, method for obtaining pyramids, software system.

DOI: 10.21293/1818-0442-2021-24-4-85-89

References

1. World!Of numbers. Available at: http://www.worldofnumbers.com (Accessed: February 12, 2022).

2. Sloane N.J.A. *A handbook of integer sequences*. USA, New York, Academic Press, 1973, 206 p.

3. Sloane N.J.A., Plouffe S. *The encyclopedia of integer sequences*. USA, San Diego, Academic Press, 1995, 587 p.

4. Sloane N.J.A. The online encyclopedia of integer sequences. *Notices of the American Mathematical Society*, 2018, vol. 65, no. 9, pp. 1063–1074.

5. Perminova M.Yu. [Software module to obtain explicit expressions for generating functions coefficients based on use of composition]. *Proceedings of TUSUR University*, 2017, vol. 20, no. 1, pp. 65–69 (in Russ.).

6. Oseledets I.V., Tyrtyshnikov E.E. [Recursive decomposition of multidimensional tensors]. Proceedings of the Russian Academy of Science, 2009, vol. 427, no. 1, pp. 14–16 (in Russ.).

7. Kruchinin D., Kruchinin V., Shablya Y. Method for obtaining coefficients of powers of bivariate generating functions. *Mathematics*, 2021, vol. 9, no. 4, article 428.

8. Kruchinin D.V., Kruchinin V.V. Application of a composition of generating functions for obtaining explicit formulas of polynomials. *Journal of Mathematical Analysis and Applications*, 2013, vol. 404, no. 1, pp. 161–171.

9. Kruchinin V.V., Kruchinin D.V. Composita and its properties. *Journal of Analysis & Number Theory*, 2014, vol. 2, no. 2, pp. 37–44.

10. Kruchinin D., Kruchinin V. A method for obtaining generating functions for central coefficients of triangles. *Journal of Integer Sequences*, 2012, vol. 15, no. 9, article 12.9.3.

11. Kruchinin D.V. On solving some functional equations. *Advances in Difference Equations*, 2015, vol. 2015, no. 1.

12. Kruchinin D.V., Kruchinin V.V. Explicit formula for reciprocal generating function and its application. *Advanced Studies in Contemporary Mathematics (Kyungshang)*, 2019, vol. 29, no. 3, pp. 365–372.

13. Gessel I.M. A combinatorial proof of the multivariable Lagrange inversion formula. *Journal of Combinatorial Theory, Series A*, 1987, vol. 45, no. 2, pp. 178–195.

14. Stanley R.P. *Enumerative combinatorics.* Vol. 2. USA, Cambridge University Press, 2001, 595 p.

Dmitry V. Kruchinin
Candidate of Science in Mathematics and Physics,
Associated Professor, Department of Computer Control and Design Systems, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0003-3412-432X
Тел.: +7 (382-2) 41-47-17
Email: kruchinindm@gmail.com

Требования к подготовке рукописей статей,

представляемых для публикации в журнале
«Доклады Томского государственного университета систем управления и радиоэлектроники»

1. Электронный вариант статьи должен быть представлен в виде файла, названного по-русски фамилией первого автора, на дискете или диске в формате Word 2003–2016. Предпочтительнее представить его по электронной почте.

2. Оригинал на бумажном носителе должен полностью соответствовать электронному варианту.

3. Статья должна иметь (в порядке следования): УДК; И.О. Фамилии авторов; заглавие; аннотация (не реферат); ключевые слова; основной текст статьи; список библиографий под подзаголовком «Литература»; сведения об авторах; далее на английском языке: Фамилии авторов И.О., заглавие статьи, аннотацию, ключевые слова. Сведения об авторах включают в себя фамилию, имя, отчество, ученую степень, ученое звание, должность, место работы, телефон, электронный адрес.

4. Текст статьи должен быть размещен в две колонки без принудительных переносов через один интервал шрифтом Times New Roman 10 кегля на одной стороне листа белой писчей бумаги формата А4, без помарок и вставок. Для облегчения форматирования прилагается **шаблон статьи**, который размещен на сайте: **journal.tusur.ru.** Размер статьи со всеми атрибутами должен быть, как правило, не более пяти страниц.

5. Одни и те же символы в тексте, формулах, таблицах и рисунках должны быть единообразными по написанию. Русские буквы и греческие символы набираются прямым шрифтом, а переменные, обозначенные латинскими – курсивом, кроме слов, их сокращений, имен функций, программ, фирм и химических формул.

6. Формулы должны быть набраны в формульном редакторе (MathType) программы Word. Русские буквы, греческие символы, математические знаки (+, –, ×, ∈, =, скобки, …) и цифры всегда набираются прямым не жирным шрифтом, а переменные (и кривые на графиках), обозначенные латинскими буквами или цифрами – курсивом, кроме англ. слов, их сокращений, имен функций, программ, фирм и химических формул (const, input; $\sin x(t_1)$; U_{in}; $I_{вх}$; T_z; β_2; H_2O, Adobe Acrobat, Cisco и т.д.); векторные величины – жирным, прямо (не курсив) – $\mathbf{A}_1$, $\mathbf{M}(f)$, $\boldsymbol{\beta}_x$. Шаблоны для набора формул необходимо взять на сайте из шаблона статьи.

7. Все употребляемые обозначения и сокращения должны быть пояснены.

8. Единицы измерения физических величин должны соответствовать Международной системе единиц (СИ) и написаны по-русски через пробел (*x*, ГГц; 20 ГГц; *T*, град; 7 °С). Десятичные числа пишутся через запятую (не точку).

9. Таблицы и рисунки должны иметь тематические заголовки (не повторяющие фразы-ссылки на них в тексте). (Рис. 1. Название рисунка; Таблица 1. Название таблицы). Большие блоки расшифровки условных обозначений лучше приводить в тексте. Подписи и надписи на рис. – Times New Roman, 9 пт (после масштабирования), не жирным, не курсивом, переменные – также, как и в тексте. На все рисунки и таблицы должны быть ссылки в тексте (… на рис. 3, … в табл. 2).

10. Рисунки и фотографии должны быть **черно-белыми**, четкими, контрастными, аккуратными, сгруппированными. Графики – не жирно, сетка – четко. Единицы измерения – на русском. Десятичная запятая (не точка). Рисунки могут быть выполнены в программах CorelDraw, Illustrator, Word, Visio и должны давать возможность внесения исправлений.

11. Иллюстрации, должны быть разрешением не менее 600 dpi. Масштаб изображения – 8 или 16,7 см по ширине (при условии читаемости всех надписей, выполненных шрифтом Times New Roman, после масштабирования – 9 кегль).

12. На все источники, указанные в списке литературы, должны быть ссылки по тексту (нумерация в порядке упоминания, например, [1, 2], [5–7]). Описание источников должно соответствовать ГОСТ 7.1–2003 и ГОСТ Р 7.0.5–2008 и содержать всю необходимую для идентификации источника информацию, а именно: *для непериодических изданий* – фамилию и инициалы автора, полное название работы, место издания, название издательства, год издания, количество страниц; *для периодических изданий* – фамилию, инициалы автора, полное название работы, название журнала, год выпуска, том, номер, номера страниц (см. примеры оформления библиографий).

Бумажный вариант рукописи статьи должен быть подписан авторами и (для сторонних авторов) иметь сопроводительное письмо на бланке организации.

Плата за публикацию рукописей не взимается.

Материальные претензии авторов, связанные с распространением материалов их статей после опубликования, не принимаются.

Авторы несут полную ответственность за содержание статей и за последствия, связанные с их публикацией.

Контактная информация
Адрес: 634050, Томск, пр. Ленина, 40.
Эл. почта: vnmas@tusur.ru. Тел.: +7 (382-2) 51-21-21

9 771818 044708 02007