

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОЕКТИРОВАНИЕ, ТЕХНОЛОГИЯ ЭЛЕМЕНТОВ И УЗЛОВ КОМПЬЮТЕРНЫХ СИСТЕМ

УДК 004.42

ИСПОЛЬЗОВАНИЕ ОНТОЛОГИИ ПРИ УПРАВЛЕНИИ ДОСТУПОМ К ИНТЕЛЛЕКТУАЛЬНЫМ РЕСУРСАМ

В.Г. Варгин, И.А. Семерханов

Научный руководитель – к.т.н., доцент Д.И. Муромцев

В данной работе рассмотрена возможность использования онтологии при управлении доступом к интеллектуальным ресурсам и преимущества внедрения семантических сервисов.

Сегодня очень актуальна проблема обеспечения информационной безопасности. Опыт эксплуатации информационных систем и ресурсов в различных сферах жизнедеятельности показывает, что существуют различные и весьма реальные угрозы потери информации, приводящие к материальным и иным ущербам. В таких системах повышенное внимание уделяется управлению доступом к информации в целях обеспечения безопасности и удобства работы.

Приоритетными направлениями управления интеллектуальными ресурсами предприятия являются: сбор информации об имеющемся интеллектуальном потенциале предприятия; определение целесообразности привлечения дополнительных интеллектуальных ресурсов; оценка эффективности вложений в развитие интеллектуальных ресурсов; содействие повышению творческой и инновационной активности; организация процессов обучения персонала предприятия. Семантическое управление доступом – управление доступом, при котором решение о предоставлении прав доступа к объекту определяется смысловым содержанием объекта – семантикой объекта. Предлагаемый подход является основой для формирования корпоративной памяти, фиксирующей информацию из различных источников предприятия и делающей эту информацию доступной всем специалистам для решения производственных задач.

Управление доступом к интеллектуальным ресурсам можно осуществлять на различных уровнях реализации информационной системы: аппаратном, программном, телекоммуникационном. Предложение использовать онтологическую модель для управления доступом является очень перспективным. Онтология сможет определить различные области, представляющие интерес для информационной безопасности [1]. При проектировании такой онтологии представляется целесообразным создание web-онтологий – онтологий в контексте семантической паутины (web 3.0) на основе стандартов и рекомендаций консорциума W3C (TheWorldWideWebConsortium). Одной из таких рекомендаций является WebOntologyLanguage (OWL) – язык для представления онтологий и связанной информации в виде семантической сети. OWL использует язык описания метаданных ResourceDescriptionFramework (RDF), построенный на основе XML и, соответственно, совместимый с другими web-ориентированными языками, а также возможность импорта-экспорта моделей между приложениями, работающими с UML и OWL. Элементами онтологий OWL являются классы, их представители (индивиды), свойства и отношения между классами и/или их представителями. RDF Schema (RDFS) – семантическое расширение RDF, язык описания словарей RDF-терминов. RDFS позволяет определить уникальные классы ресурсов, представляющие модель предметной области, включая их атрибуты и отношения между классами. Кроме того, RDF Schema включает возможность

определения подклассов, а также представляет некоторое количество базовых классов и возможность определения некоторого количества ограничений [2].

Исследования авторов показали, что применение онтологии для семантического управления доступом к интеллектуальным ресурсам может значительно повысить защищенность информации.

Литература

1. Simmonds A.J., Sandilands P., Ekert L. van. An Ontology for Network Security Attacks // ААСС. – 2004. – Р. 317–323.
2. Андреева Н.В., Любимов А.В. Выбор методов и средств онтологического анализа стандартов информационной безопасности // VI Всероссийская межвузовская конференция молодых ученых. – СПб: СПбГУ ИТМО. – 2009. – Вып. 6. – С. 29–33.

УДК 004.056.53

АНАЛИТИЧЕСКИЙ ОБЗОР ПРОГРАММНЫХ КОМПОНЕНТОВ ИСПОЛЬЗУЮЩИХ В СВОЕЙ ОСНОВЕ НОРМАТИВНО-МЕТОДИЧЕСКУЮ ДОКУМЕНТАЦИЮ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.В. Васильева, С.С. Беляев

Научный руководитель – к.т.н., доцент Г.П. Жигулин

Краткое вступление, актуальность темы. В связи с созданием центров обработки данных и переводом информационных ресурсов в цифровую форму, произошли изменения в области информационной безопасности, связанные с переходом от инженерного подхода к вопросам управления доступом к информационным ресурсам. В результате таких изменений увеличилась заинтересованность специалистов и появилась необходимость глубокого анализа в этом направлении.

Цель работы. Аналитический обзор программных компонентов использующихся для обеспечения безопасности на основе нормативно-методической документации в области информационной безопасности и рассмотрение программного решения реализующего централизованный мониторинг событий безопасности.

Описание ситуации в предметной области. В настоящее время существует множество стандартов, таких как Стандарты в области компьютерной безопасности «Оранжевая книга», Международные стандарты управления информационной безопасностью ISO 27000, Общие критерии оценки безопасности информационных технологий ISO 15408, Стандарты Банка России в области информационной безопасности СТО БР ИББС, Международные стандарты безопасности информационных технологий ISO 13335, BaselineProtectionManualBSMIT, ControlObjectivesforInformationandrelatedTechnologyCOBIT. Их можно разделить на два направления: технические стандарты и стандарты аудита безопасности.

В Банке России и в коммерческих банках используется комплекс Стандартов Банка России, который включает в себя:

- методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях Банковской Системы Российской Федерации;
- методику оценки рисков нарушения информационной безопасности;
- общие положения;
- методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0;

- требования по обеспечению безопасности персональных данных в информационных системах персональных данных организации Банковской Системы Российской Федерации;
- методику оценки соответствия информационной безопасности организации Банковской Системы Российской Федерации требованиям СТО БР ИББС-1.0-20xx;
- руководство по самооценке соответствия информационной безопасности организаций Банковской Системы Российской Федерации требованиям СТО БР ИББС-1.0;
- отраслевую частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций Банковской Системы Российской Федерации;
- аудит информационной безопасности.

Именно эти стандарты положены в основу создания автоматизированной системы СОИБ (система обеспечения информационной безопасности), важнейшими элементами которой являются программные продукты IBM, такие как TivoliIdentityManager (TIM), TivoliComplianceInsightManager (TCIM), TivoliSecurityOperationsManager (TSOM), TivoliAccessManagerforEnterprisesSingleSign-On (TAM).

Основные результаты. Особо хочется отметить программный компонент TCIM, так как при помощи него происходит аудит действий пользователей и контроль соответствия нормативным требованиям. TCIM позволяет осуществлять мониторинг рабочих операций пользователей в соответствии с политикой определенной нормативными документами, также осуществляет преобразование значительных объемов информации о событиях информационной безопасности, отсортированных по правилам написанной политики, по разработанной компанией IBM уникальной технологии W7 (Who, didWhat, When, Where, Wherefrom, Whereto, onWhat).

Вывод. Результатом проведенной работы является аналитическая справка по существующим программным решениям, в основе которых реализованы Стандарты в области информационной безопасности. Также рассмотрен программный компонент IBMTCIM реализующий централизованный мониторинг событий безопасности.

УДК 004.056.5

ВЫБОР СРЕДСТВ ДЛЯ СОЗДАНИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА КАФЕДРЫ ВУЗА

А.С. Виволанцев

Научный руководитель – к.т.н., доцент А.А. Малинин

Цель работы. Выбрать средство для создания единого информационного пространства кафедры вуза.

Обзор внедрений единого информационного пространства в вузы.

Анализ существующих средств для создания единого информационного пространства вуза:

1. чистые языки программирования (C#, Java...);
2. платформы (DocsVision, 1С...).

Достоинства и недостатки средств создания единого информационного пространства вуза.

Предлагаемое средство разработки: Технологическая платформа 1С.

Преимущества предлагаемого средства разработки:

- количество внедрений;

- простота разработки;
- возможность работы под толстым, тонким и Web-клиентом;
- стоимость разработки и внедрения.

УДК 004.3

АНАЛИЗ ОСОБЕННОСТЕЙ ПОСТРОЕНИЯ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ РАЗНОГО РАЗМЕРА

М.Д. Газарян

Научный руководитель – к.т.н., доцент К.Н. Заикин

Системы контроля и управления доступом (СКУД) являются одним из наиболее быстро развивающихся сегментов рынка безопасности в России. Следует отметить, что для рынка СКУД характерно наличие систем различного технического уровня и функциональных возможностей, которые существенно различаются как по сложности, так и по стоимости и ориентированы на разные потребительские группы.

Необходимо для каждого потребителя определить наиболее подходящую архитектуру СКУД учитывая характер и размеры объекта.

В работе проанализированы особенности построения и предложена методика разработки наиболее подходящей архитектуры СКУД для определенного объекта.

Традиционными потребителями малых систем являются небольшие офисы, предприятия розничной торговли и т.п. Сегодня среди них появился новый потребитель – учебные заведения, для которого характерно использование СКУД в двух основных режимах.

Во-первых, это идентификация личности, а во-вторых, контроль и ограничение прохода.

В обоих режимах для прохода используются прох-карты, которыми снабжаются все сотрудники и слушатели учебного заведения. На таких объектах СКУД используется наиболее часто без интеграции с другими системами безопасности, и основной контроль осуществляется на одном (главном) входе. Если интеграция осуществляется, то, как правило, с системами теленаблюдения.

Другими особенностями, характерными для малых систем, являются:

- установка оборудования контроля доступа на двери всех помещений служебной зоны;
- установка на двери, отделяющие клиентскую зону от служебной, считывателей двойной технологии для повышения уровня безопасности.

Одной из тенденций, характерных для традиционных потребителей средних СКУД (офисные здания крупных компаний, бизнес-центры, предприятия оптовой торговли, супермаркеты и т.п.), является тесная интеграция СКУД с системой охранной сигнализации (ОС).

Функционирование СКУД и ОС тесно взаимосвязано, и на некоторых объектах устанавливается оборудование данного назначения от одного производителя, обладающее полной аппаратной совместимостью.

Извещатели ОС в помещениях, оборудованных средствами контроля доступа, подключаются в этом случае следующим образом:

- к самим контроллерам СКУД, оснащенным резистивными входами;
- к дополнительным входам ОС на интерфейсных модулях СКУД;
- к входам панелей охранной сигнализации, подключаемым к единому центральному контроллеру СКУД и ОС.

На рынке традиционных потребителей больших СКУД (крупные корпорации, имеющие отделения в одном или нескольких городах, мощные производственные компании, авиа- и транспортные компании с распределенной сетью офисов продажи билетов и обслуживания

пассажиров и т.п.) также можно выделить ряд тенденций.

Одной из них является построение на базе СКУД интегрированных систем безопасности, объединяющих в единый комплекс подсистемы, позволяющие решать различные задачи в сфере технических средств обеспечения безопасности.

Центральной частью таких интегрированных систем является программное ядро, обеспечивающее логическое объединение и управление всеми подсистемами:

- ведение единого протокола событий всех подсистем;
- обработка любых событий всех подсистем;
- программирование реакций на события через язык сценариев;
- задание сложных алгоритмов взаимодействия подсистем.

В работе проведен анализ особенностей построения СКУД, в результате чего были определены критерии выбора архитектуры СКУД для объектов различного характера и масштаба.

УДК 004.75

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

А.Б. Данилов

Научный руководитель – к.т.н., доцент Н.С. Кармановский

В качестве одного из наиболее перспективных способов оптимизации ИТ-инфраструктуры сейчас все чаще рассматриваются облачные вычисления (CloudComputing). При наличии очевидных достоинств, основным сдерживающим фактором при реализации концепции облачных вычислений является вопрос о надежности защиты данных вычислений. **Целью работы** является анализ основных проблем обеспечения безопасности облачных вычислений.

На данный момент традиционные средства защиты не способны обеспечить должный уровень безопасности в облаке, так как появляются специфические для данной концепции угрозы информационной безопасности.

Выделим следующие категории угроз информационной безопасности для данной технологии.

Общие (классические) угрозы информационной безопасности. Архитектура облачных вычислений основана на web-технологиях, и для нее также актуальны угрозы, связанные с уязвимостями сетевых протоколов, серверов приложений и операционных систем (ОС).

Несанкционированный доступ (НСД) к учетным записям или сервисам клиентов. Во время подключения пользователя к облачной среде между ним и облаком (возможно, еще и виртуальным сервером приложений) устанавливаются «доверительные отношения» посредством аутентификации пользователя и организации защищенного соединения с использованием криптографических средств. Такие доверительные отношения и могут стать целью злоумышленника – это атаки на парольную защиту, на механизмы авторизации, подмена содержимого (ContentSpoofing), межсайтовое выполнение сценариев (Cross-siteScripting, XSS) и т.д. Основная опасность НСД сегодня исходит прежде всего от самого облака, поскольку методы и техники защиты на уровне виртуальной среды еще недостаточно развиты.

Использование небезопасных программных интерфейсов (API), которые иногда предоставляют конечным пользователям для реализации различных услуг облака.

Утечка данных. Поскольку доступ к облаку осуществляется исключительно по сети, необходимо обеспечивать сохранность и конфиденциальность хранимых данных (включая резервные копии), в том числе в процессе их передачи по сети.

Утрата данных. При возникновении инцидента уничтожения виртуальных машин в облаке пользователь может потерять данные навсегда. При выходе из строя аппаратного средства, на котором функционирует несколько виртуальных машин, ущерб от события увеличивается в несколько раз. И хотя технологии резервирования сегодня весьма развиты, конкретная их реализация в облаке является тем узким местом, адекватную реализацию которого нужно доказывать.

Угрозы, связанные с применением виртуальной среды. В виртуализованной системе появляются новые элементы, которые могут быть потенциальным объектом атаки.

Для обеспечения информационной безопасности приходится осваивать новые методы и технологии защиты, учета инцидентов, разрабатывать новые стандарты информационной безопасности. Есть и сложности юридического характера. В частности, становится непросто разграничить, кто и за что отвечает, поскольку облачные вычисления инфраструктурно существенно отличаются от привычной модели и могут динамически изменяться. Необходимо отметить, что существует и психологический аспект данной проблемы. ИТ-аутсорсинг пока что не получил в России такого развития как на Западе, и многие руководители компаний скептически воспринимают саму идею передачи ИТ-инфраструктуры на обслуживание стороннему специалисту.

Как показывает практика, применение облачных вычислений способно даже значительно повысить уровень безопасности данных. Одна из причин – это постоянная забота о высоком уровне безопасности со стороны компаний, предоставляющих доступ к сервисам cloudcomputing. Зная об опасениях своих клиентов, они вынуждены вкладывать существенные средства в создание и поддержку надежной системы защиты. Некоторые провайдеры ИТ-услуг в сфере CloudComputing делают явный упор в своей маркетинговой компании именно на гарантию высокого уровня безопасности.

Таким образом, на сегодняшний день сдерживание внедрения облачных вычислений связано с тем, что не проработаны юридические аспекты по данному вопросу, а также отсутствуют надежные системы защиты в облаке.

УДК 004.7

ТИПИЗАЦИЯ АЛГОРИТМОВ РАЗВЕРТЫВАНИЯ ЛОКАЛЬНЫХ СЕТЕЙ

Н.А. Дородников, Ю.Г. Филиппова, А.В. Евлахова, Е.А. Златина

Научный руководитель – к.т.н., доцент А.А. Малинин

На сегодняшний день компьютеризация достигла распространенности в бизнес-сфере, близкой к 100 процентам. Это, в свою очередь, заставило очень и очень многих руководителей организации переучиваться и принимать решения с поправкой на электронный документооборот и более быстрый обмен информацией.

Вместе с тем, выросло и количество проблем, связанных с безопасностью. В данном случае подразумевается и опасность потери/кражи данных, и несанкционированного доступа к данным. Для коммерческих структур это особенно важно, ибо их доход напрямую зависит от конкуренции, а компьютерная сеть может все чаще и чаще быть стать фактором влияния.

Немаловажно бывает также учитывать и возможные проблемы, исходящие не извне, а изнутри, вследствие административных решений по расширению организации. Ведь, казалось бы, это благо, однако особенности конкретной реализации локальной сети могут не позволить безболезненно произвести расширение, будь-то качественным или количественным. Это может сказаться на скорости работы, на отказоустойчивости, на сложностях администрирования. К тому же, очень часто на начальных этапах построения сети исходят из финансовых возможностей организации. Оснастить сеть масштабируемыми и надежными устройствами способна далеко не каждая начинающая компания.

В противовес же этому, нужно учесть, что оснатив сеть изначально профессиональным и дорогим оборудованием, легко столкнуться с проблемой избыточности и несоответствия возможностей оборудования и квалификации обслуживающего персонала. Также, неграмотные решения, подготовленные в начальные этапы работы сети, могут в силу привычки сотрудников переключаться и в более поздние ее реализации, увлекая за собой набор так называемых «костылей» и сомнительных, неоптимальных и небезопасных особенностей реализации, и когда-то временное решение станет постоянным.

Следует также помнить о такой опасной вещи, как человеческий фактор. Ошибка может найтись сразу, а может быть незаметной, и ждать своего часа годами, обрушив шквал неприятностей в самый неподходящий момент. Можно долго подбирать и мотивировать специалистов, но от ошибок, увы, никто не застрахован.

Как же решать все эти проблемы? Решение есть, это автоматизация процесса развертывания сети. Конечно, можно отдать локальную сеть на «аутсорс» специализированной организации, но, во-первых, это – посторонние люди, а значит – очередной фактор риска утечки информации. А во-вторых, опять же, человеческий фактор.

Автоматизация же даст возможность оптимизировать используемые алгоритмы, создавая их непосредственно под нужды протекающих в сети бизнес-процессов. На этапе проектирования это не только поможет снизить риск ошибок, но и выведет на качественно новый уровень безопасность обмена информацией, надежность и масштабируемость сети. Позволит также сэкономить на обслуживании, предусмотреть все узкие места в системе.

Удивительно, но факт: сегодня на рынке достаточно много мониторинговых сервисов и сервисов по настройке того или иного сетевого функционала, но нет ни одного сервиса, автоматизирующего сам процесс создания сети поэтапно. Да и те, что местами покрывают некоторый функционал планирования сети – используют конструкторы, полные технических терминов, а потому – направленные непосредственно на использование профессиональными администраторами, которые для отдельно взятой сети могут все настроить и сами.

Важно также занять наиважнейшую нишу между профессиональными администраторами и профессиональными управленцами, чтобы спроектировать сеть под нужды организации мог бы человек без специального для этого образования. И более того – спроектировать хорошо.

Именно поэтому **целью работы** мы поставили изучение и типизацию существующих алгоритмов развертывания локальных сетей и их автоматизацию, а именно – создание промежуточного между управленцами и администраторами интерфейса, готового взять на себя обязанности планирования, моделирования и генерации конфигураций локальной сети под нужды организации. Работа довольно объемная, включает в себя этапы планирования сети по текущим нуждам с учетом возможных качественно-количественных увеличений, разграничения доступа и территориальных расположений в случае нескольких офисов, затраты на монтажные работы, предложения по узлам связи и обработки информации (по целям потребителя), конфигурации узлов связи и конечных станций, генерацию настроек готовых серверных решений и сервисов для них, моделирование системы безопасности путем соответствующей настройки межсетевых экранов, групп доступа и допуска, систем шифрования данных.

По ходу работы были произведены изучения современных технологий и их особенностей, составлены алгоритмы моделирования различного функционала, выявлялись зависимости конфигураций от различных входящих параметров сетей, изучалась база особенностей и исключений. Прорабатывались возможности будущего расширения функционала путем внедрения облачных вариантов сетей (персональных, публичные облака принципиально рассматриваться не будут).

На данный момент система находится в стадии разработки и описания внутренней логики и конфигураторов. Параллельно разрабатывается web-контейнер (cms) для данной системы.

ЗАЩИТА ИНТЕРНЕТ БРАУЗЕРА ОТ СЕТЕВЫХ АТАК ДИСКРЕЦИОННЫМ МЕТОДОМ РАЗГРАНИЧЕНИЯ ДОСТУПА

Е.А. Дудников

Научный руководитель – д.т.н., профессор А.Ю. Щеглов

Цель работы – защита интернет браузера от сетевых атак.

Исследование известных методов защиты от сетевых атак: эвристический анализ, эмуляция кода, анализ поведения, Sandboxing (Песочница) – ограничение привилегий выполнения, виртуализация рабочего окружения, классические и экспертные HIPS (Host-based Intrusion Prevention System, англ. система предотвращения вторжений), защита браузера от фишинга и malware.

Недостатки известных методов защиты информации: использование эвристических анализаторов и поведенческих блокираторов, обновления баз, использование как сигнатурного, так и эвристического анализов требует временных затрат и существенных процессорных мощностей, ложные срабатывания систем защиты, малый процент обнаружения новых атак, суть известных методов защиты от сетевых атак сводится к попытке предотвращения самой атаки.

Предлагаемый метод защиты: дискреционный метод разграничения доступом.

Реализация защиты – любой создаваемый файл помечается, ему сопоставляется учетная информация создавшего файл субъекта доступа (имя учетной записи и процесса – полнопутьное имя исполняемого файла процесса). При обращении к любому файлу (в том числе, и системой), анализируется, был ли создан этот файл в процессе эксплуатации системы (размечен ли он). Далее в соответствии с заданием правил на чтение, запись, удаление, переименование и исполнение устанавливаются разграничения доступа для субъектов.

Решаемые задачи защиты от: кражи информации, нарушения работоспособности системы, дезинформации, установки вредоносного программного обеспечения.

Апробация метода на примере КСЗИ «Панцирь+». Реализованы три варианта дискреционного метода:

1. базовая настройка – разрешает чтение, запись, переименование, удаление файлов, но запрещает их исполнение;
2. изоляция работы браузера и разграничения между пользователями – данная настройка изолирует работу интернет браузера, изолирует его работу между профилями пользователей. Следовательно, становятся, запрещены любые обращения к файлам, созданным браузером под тем или иным профилем;
3. расширенная настройка – разрешение на доступ к тому, что создает браузер, процессам, необходимым для работы того или иного профиля.

Преимущества предлагаемого метода: данный метод практически не влияет на загрузку вычислительных ресурсов, процедура анализа никак не связана с типом файла, в том числе с типом его расширения, не используются обновления баз, осуществлен контроль субъекта, осуществляющего доступ к ресурсам субъекта создателя, а именно контроль чтения, записи, исполнения, переименования, исполнения файлов, при маркировке файлов указывается имя учетной записи и полнопутьное имя процесса, что исключает маскировку под легитимный файл, исключаются ложные срабатывания.

МЕТОДЫ КОНТРОЛЯ ПАЯНЫХ СОЕДИНЕНИЙ ЭЛЕМЕНТНОЙ БАЗЫ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Е.И. Ефимов, Р.Я. Лабковская

Научный руководитель – д.т.н., профессор В.Л. Ткалич

Переход от монтажа радиоэлектронных компонентов в отверстия к поверхностному монтажу в конце 80-х годов открыл новые возможности в области электронной техники. Поверхностный монтаж обладает рядом преимуществ, таких как высокая степень миниатюризации, возможность практически полной автоматизации процесса установки компонентов на печатную плату, повышение технологичности и, как следствие, снижение стоимости конечного изделия. В то же время данная технология предъявляет более строгие требования к контролю качества паяных соединений. На данный момент существует несколько способов контроля качества пайки поверхностно монтируемых компонентов: визуальный контроль, электрический контроль, автоматическая оптическая инспекция и рентгеновский контроль. В данной работе приводится сравнение этих методов и области их применения.

Визуальный контроль – самый простой и самый старый метод контроля пайки. Визуальный контроль применяют при проверке качества пайки выводных соединений и проверки качества пилотных образцов изделий при промышленном производстве. Электрический контроль, осуществляющийся либо с помощью «летающих щупов», либо с помощью специальной оснастки (так называемое «ложе гвоздей»), применяется для финального тестирования уже готовых изделий.

В настоящее время подавляющий объем работ по контролю качества пайки поверхностно монтируемых компонентов осуществляется с помощью установок автоматической оптической инспекции (АОИ). С помощью установки АОИ можно контролировать количество паяльной пасты в месте соединения, тип компонента, его ориентацию, позиционирование и маркировку. Контроль осуществляется путем сравнения с «золотой платой», за которую берется, например, пилотный образец полностью проверенный с помощью визуального контроля. Контроль с помощью АОИ – очень быстрый и технологичный, системы АОИ могут включаться прямо в производственную линию для практически полной автоматизации процесса монтажа компонентов.

Главным недостатком АОИ является невозможность контроля качества пайки компонентов, имеющих выводы под корпусом: такие как, например, микросхемы с массивом шариковых выводов (BGA) или микросхемы с термальными контактными площадками под корпусом (QFN). Единственным методом полного контроля качества пайки таких микросхем является рентгеновский контроль.

С помощью рентгеновского контроля можно диагностировать такие дефекты, как, например, пустоты, отсутствие паяного соединения (рис. 1), замыкания (рис. 2), смещение компонента и другие. Возможность фиксировать изображения исследуемого образца с помощью рентгеновской камеры предоставляет возможность анализировать сбой на каком этапе монтажа вызвал тот или иной дефект. На рис. 1 отсутствие 2-х паек у QFN-микросхемы (для данного образца паяльная паста наносилась с помощью трафарета, применялась конвекционная пайка) может свидетельствовать о том, что при нанесении паяльной пасты через трафарет апертуры трафарета оказались засорены и паста не попала на плату. На рис. 2 замыкания у BGA-микросхемы (паста наносилась каплеструйным способом, микросхема паялась методом парофазной пайки) могут говорить как о том, что либо было нанесено излишнее количество пасты, и нужно изменить настройки количества пасты наносимое принтером, либо о перегреве микросхемы в печи. Поскольку парофазная технология пайки исключает перегрев компонента выше заданной температуры, то в данном случае дефект

вызван неправильными настройками принтера.

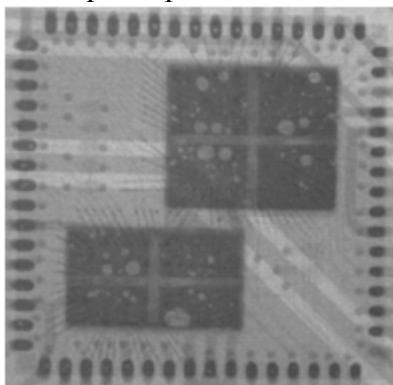


Рис. 1. Рентгеновская фотография QFN-микросхемы с отсутствием пайки 2-х контактных площадок

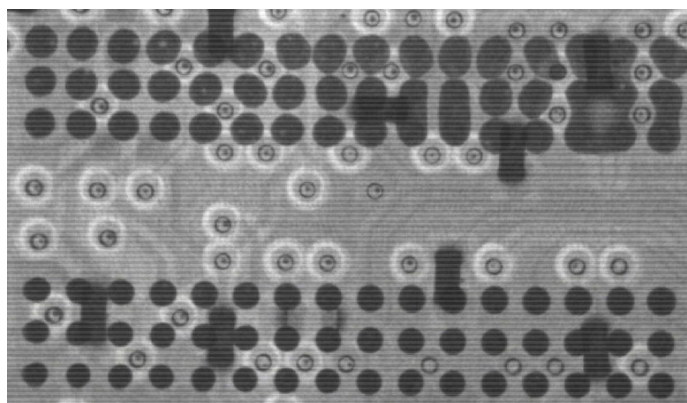


Рис. 2. Рентгеновская фотография BGA-микросхемы с замыканием контактов

Такие дефекты как пустоты были впервые обнаружены только с помощью рентгеновских установок. Согласно стандарту IPC, пустоты должны составлять не более 25% площади поверхности пайки. Таким образом, пустоты на образце на рис. 1 дефектами не являются.

При всех своих достоинствах рентген-контроль обладает и рядом недостатков: дороговизна оборудования, медленность проверки, полная зависимость качества контроля от оператора, практически полное отсутствие возможности автоматизации и интеграции в производственную линию.

Таким образом, при производстве вычислительной техники в промышленных масштабах рентгеновский контроль должен использоваться только для проверки пилотных и промежуточных образцов, поскольку подавляющее большинство дефектов можно устранить еще на этапах проектирования и технологической подготовки производства.

УДК 004.588, 004.6, 004.9

РАЗРАБОТКА ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ LINKEDLEARNING

М.Л. Зеленина

Научный руководитель – к.т.н., доцент Д.И. Муромцев

Технологии онлайн-образования (distantlearning, e-learning) на настоящий момент уже имеют уверенную позицию в мировой системе образования. Абсолютное большинство университетов мира выкладывают свои информационные, в т.ч. образовательные, ресурсы в Интернет для открытого доступа, зачастую для дистанционного ознакомления

представляются не только отдельные материалы (учебные пособия), но и полные курсы или циклы курсов. Данная тенденция имеет очевидные преимущества не только для ППС и студентов, но и служит инструментом для популяризации вуза на мировой арене. Примером последнего тезиса может являться опыт Стенфордского университета: популярность канала youtube «Stanforduniversity» (<http://www.youtube.com/user/StanfordUniversity>), который имеет 181,5 тыс. подписчиков, общее количество просмотров видео – 51 313 902 раз, обеспечивает дополнительное повышение репутации вуза среди мотивированной аудитории.

С развитием ряда факторов, таких как совершенствование технологий, растущая глобализация мирового научного сообщества, увеличивающаяся роль междисциплинарных областей науки, происходит активный рост спроса на сервисы онлайн-образования и происходит качественное развитие таких сервисов и в отношении представляемых ресурсов, и в отношении развитии инфраструктуры сервиса. Явной тенденцией последнего времени (2010–2013 гг.) является активное развитие так называемых МООС-ресурсов (a massive open online course, открытый онлайн-курс широкого доступа) – бесплатных ресурсов, предоставляющих подборку онлайн-курсов одного или различных направлений, открытых для большого количества пользователей сети Интернет. Известные примеры МООС-проектов – Coursera, основанный в 2012 г. профессорами Стенфордского университета Эндрю Энджи и Дафной Келлер, сотрудничающий с 33-мя ведущими университетами мира, на настоящий момент (январь 2013 г.) имеющий 1,9 млн. пользователей; Udacity, основанный в 2012 г. профессором Стэнфордского университета Себастьяном Труном, Дэвидом Ставенсом и Майком Сокольски и проч.

В настоящее время ведутся исследования и разработки по внедрению семантических технологий в образовательные онлайн-ресурсы и по переводу представленных данных в формат linkeddata. Часть таких программ имеет федеральную поддержку, например, проект ConnectED, который представляет собой национальный хаб, в рамках которого разрабатывается инструментарий для внедрения LinkedLearning, поддерживаются демо-проекты, производится техническая поддержка инициатив, производится управление сотрудничеством организаций в сфере linkedlearning, разрабатываются политики активного внедрения концепции linkedlearning. Часть проектов представляют собой инициативу вузов, например, LinkedUniversities – объединение европейских университетов, заинтересованных в представлении своих открытых данных в формате linkeddata. Идея этого проекта заключается в объединении информации из разных источников (организаций) в единое информационное пространство: WebofData (<http://linkeddatatbook.com/editions/1.0/>), планируется привлечение к выкладыванию в открытый доступ с помощью технологий RDF, SPARQLи т.п. материалов (курсов, публикаций, образовательных материалов) значительного большего количества университетов и обеспечение сотрудничества между ними. Разделение полномочий и обмен опытом между университетами-участниками проекта должно стать залогом успешного достижения глобальной цели: создания сети образовательных ресурсов (Webofuniversitydata).

В работе подробно рассматривается технология linkedlearning, раскрываются основные понятия, описываются этапы превращения информации в формат linkeddata.

СИСТЕМА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ ПРЕДПРИЯТИЯ МАЛОГО БИЗНЕСА

Е.А. Златина, Н.А. Дородников, А.В. Евлахова, Ю.Г. Филиппова

Научный руководитель – к.т.н., доцент А.А. Малинин

При решении производственных задач нередко возникает необходимость получения и обработки информации за пределами организации. Как следствие, возрастает число компаний, которые предоставляют сотрудникам возможность взаимодействия с существующей корпоративной информационной системой предприятия и обработки конфиденциальных данных при помощи личных мобильных устройств сотрудников, что влечет за собой повышение продуктивности, оперативности доступа к информации, улучшение мотивации, расположения сотрудников. В то же время, использование мобильных устройств создает ряд проблем, связанных с обеспечением защиты конфиденциальной информации.

Решаемые проблемы

- обеспечение защиты корпоративных данных при их передаче и обработке с помощью личных мобильных устройств сотрудников предприятия;
- отсутствие для указанной выше проблемы комплексного решения, обеспечивающего выполнения требования законодательных и нормативно-правовых актов РФ.

Цель работы – разработка проекта системы защиты конфиденциальной информации для мобильных устройств предприятия малого бизнеса.

Базовые положения исследования. Мобильные устройства обладают более широким рядом уязвимостей по сравнению с персональными компьютерами и ноутбуками.

При разработке и внедрении системы защиты для мобильных устройств возникает конфликт между интересами пользователей личных мобильных устройств и требованиями сотрудников отдела (службы) информационной безопасности предприятия в части настроек мобильных устройств, контролируемого сетевого доступа и возможности установки программных средств.

При создании системы защиты следует учитывать следующие особенности:

- использование криптографических средств в ряде случаев строго регламентируется законами и нормативно-правовыми документами;
- на текущий момент в мобильных устройствах наиболее широко используются зарубежные алгоритмы шифрования;
- стоимость создания системы защиты может быть велика в масштабах предприятия малого бизнеса.

В ходе работы необходимо сформировать требования к разрабатываемой системе защиты, в числе которых:

- соблюдение требований законодательства (выбор алгоритма шифрования, использование сертифицированных средств защиты);
- необходимость как контроля мобильного устройства при доступе к корпоративным ресурсам, так и защиты самого устройства;
- использование встроенных механизмов и централизованного средства защиты и управления;
- применение антивирусного средства на незащищенных платформах;
- применение организационных мер.

Промежуточные результаты. Выявлены уязвимости и угрозы, специфичные для мобильных устройств (высокая вероятность кражи или утраты устройства, использование съемных носителей информации, возможность установки несанкционированных приложений и настроек пользователем и др.).

Выявлены наиболее популярные мобильные платформы (iOS, Android). Различные платформы мобильных устройств обладают различным уровнем обеспечения безопасности в зависимости от встроенных механизмов защиты: операционная система iOS наиболее защищена, практически не подвержена воздействию вредоносного кода.

Осуществлен сравнительный анализ существующих программно-технических решений фирм-производителей программного обеспечения средств для защиты мобильных устройств: «Saferphone» (сертифицирован в системе «Газпромсерт», осуществляет поддержку только платформы Symbian), «Mobileiron», «McAfee EMM», а также криптошлюзов.

Установлено, что отсутствуют комплексные универсальные решения для защиты корпоративных мобильных устройств, сочетающие криптозащиту и централизованную защиту от несанкционированного доступа.

Проведен анализ требований нормативных документов при организации защиты конфиденциальной информации. Установлено, что при защите информации, составляющей коммерческую тайну, собственник информации вправе сам определять требования по защите информации. Выявлено, что возможно использование несертифицированных средств криптографической защиты информации, однако использование указанных средств защиты влечет за собой существенные ограничения на деятельность предприятия: невозможность обработки персональных данных, информационного взаимодействия с рядом государственных и исполнительных органов и другие.

Установлено, что передача корпоративной информации, включающей персональные данные, при помощи мобильных устройств возможна только для платформ «Apple iOS» (сертифицированное решение «ViPNetClientiOS» и сертифицированный криптошлюз «ViPNetCoordinator») и «Windows Mobile» (сертифицированный криптошлюз «Stonesoft SSL» и криптопровайдер «КриптоПро CSP 3.6»).

Результаты работы:

- разработана модель угроз и модель нарушителя на основе анализа уязвимостей;
- целесообразно на текущий момент ограничивать организационно-техническими мерами обработку и передачу персональных данных;
- оптимально использование криптошлюза «StonegateSSL» в качестве сертифицированного решения и дальнейшей доработки системы защиты;
- для мобильных устройств с операционной системой, отличной от «iOS», требуется антивирусное средство;
- система построена в соответствии с нормативно-правовыми актами РФ, структурирована на подсистемы, с использованием программно-технических решений и применением организационных мер.

МНОГОАГЕНТНЫЕ СИСТЕМЫ ПРИНЯТИЯ ТЕХНИЧЕСКИХ РЕШЕНИЙ

А.И. Иванов

Научный руководитель – к.т.н., доцент И.Б. Бондаренко

При проектировании сложных систем разработчики сталкиваются с различными проблемами, которые необходимо решить оптимальным путем. Так, например, при проектировании печатных плат, что, несомненно, является сложным процессом, разработчику необходимо, имея электрическую функциональную схему:

- выбрать элементную базу для платы (является многокритериальной задачей и зависит от стоимости, производителя, надежности, геометрических размеров, электрических параметров и др.);
- разработать электрическую принципиальную схему;
- оптимальным образом расположить компоненты на плате (учитывая равномерное распределение тепла);
- выполнить трассировку проводников (для многослойных печатных плат является весьма сложным процессом).

Автоматизация задачи проектирования печатных плат, безусловно, является чрезвычайно сложной проблемой, затраты на решение которой, непременно, будут оправданы. Для решения технически трудных задач предлагается использовать системы, состоящие из множества взаимодействующих агентов, каждый из которых владеет лишь частичным представлением о глобальной проблеме и способен решить лишь некоторую часть общей задачи. Поэтому для решения сложной задачи необходимо создать некоторое множество агентов, распределить между ними задачи и организовать их эффективное взаимодействие, что позволит построить между ними единую многоагентную систему.

Цель работы состоит в аналитическом обзоре обучаемых агентов, применяющихся для принятия решений, правил распределения задач между агентами и методов взаимодействия агентов в многоагентных системах, решающих сложную задачу.

По характеристике обучаемости агентов разделяют на два вида: когнитивные и реактивные. Когнитивные агенты, благодаря их сложности, наличию знаний и способностей к рассуждениям о своем поведении и внешней среде, могут быть более автономными, чем реактивные, и представляют собой интерес на индивидуальном уровне. Но сложность когнитивных агентов, в свою очередь, представляет основную проблему реализации их эффективного взаимодействия. Поэтому в составе многоагентных систем, состоящих только из когнитивных агентов, как правило, присутствует не более 7 единиц. В свою очередь, простота реализации взаимодействия между реактивными агентами позволяет им решать сложные задачи на коллективном уровне.

Для организации процесса распределения задачи в многоагентных системах создается либо система распределенного решения проблемы, либо децентрализованный искусственный интеллект. В распределенных системах объектом исследования является общая сложная проблема, для решения которой формируется группа агентов, строится общая концептуальная модель и вводятся глобальные критерии достижения цели. В полностью децентрализованных системах объектом исследования является деятельность автономного агента в динамическом многоагентном мире (в т.ч. координация действий других агентов).

Для успешного достижения поставленной цели, агентам необходимо взаимодействовать друг с другом (перераспределять задачи, помогать, мешать и т.д.). Взаимодействия между агентами характеризуются:

- направленностью (конкурентные и кооперативные, однонаправленные и двунаправленные);
- избирательностью;

- интенсивностью;
- динамичностью.

Все многообразие взаимодействия необходимо анализировать на различных уровнях. Необходимо отличать макроситуацию (взаимодействие всех агентов многоагентной системы) от микроситуаций (локальные взаимодействия). При таком подходе можно ранжировать по значимости различные виды взаимодействий и точно определить их место в многоагентной системе.

В работе произведен аналитический обзор многоагентных систем. Приведена классификация агентов, разобраны варианты взаимодействия между ними, а также рассмотрены варианты распределенного решения задач в многоагентных системах.

УДК 004.4

ПРИМЕНЕНИЕ ТРЕХМЕРНОГО МОДЕЛИРОВАНИЯ ПРИ РАЗРАБОТКЕ ЭЛЕКТРОННЫХ УСТРОЙСТВ В СИСТЕМЕ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ALTIUMDESIGNER

К.В. Козицын

Научный руководитель – д.т.н., профессор В.Л. Ткалич

Применение современных систем автоматизированного проектирования при разработке электронных устройств позволяет значительно снизить время и стоимость разработки, сократить количество ревизий устройства до начала производства и в целом повысить качество получаемого продукта. Одной из таких САПР в данный момент является AltiumDesigner-мощный программный продукт, создателями которого являются авторы небезызвестного PCAD. Одной из интереснейших возможностей, предлагаемых данной САПР является возможность интеграции в процесс разработки печатной платы трехмерных моделей.

Целью работы является выработка наиболее оптимальной методики и алгоритма работы в AltiumDesigner с применением трехмерного моделирования.

Ранее процесс взаимодействия «механических» и «электронных» САПР представлял собой сложный многоэтапный процесс. Средства AltiumDesigner позволяют быстро и просто импортировать трехмерные модели в среду разработки. Взаимосвязь с «механическими» САПР осуществляется через формат STEP, являющийся мировым стандартом для обмена информацией о геометрии объекта. Для создания моделей можно использовать современные САПР, направленные на работу с трехмерными моделями (SolidWorks, Компас 3Д и т.д.). После импорта, модель элемента можно устанавливать на печатную плату, использовать для создания библиотеки компонентов и т.д. Для сохранения связи между САПР и моделью, рекомендуется использовать специальную директорию для хранения используемых моделей, определяемую в настройках AltiumDesigner; в таком случае изменения в модели элемента сразу отобразятся в проекте.

Возможности AltiumDesigner позволяют производить так же обратный процесс-экспорт STEP файлов. Имея в своем распоряжении файлы печатных плат с установленными компонентами мы можем произвести компоновку устройства и внести необходимые коррективы, исправить ошибки в разработке.

Для оптимизации процесса разработки сформулируем методику работы в AltiumDesigner с применением трехмерных моделей. Последовательность действий выглядит следующим образом:

1. создание собственной библиотеки элементов с применением трехмерных моделей;
2. разработка компоновки устройства в «механической» САПР;
3. импорт файлов STEP с габаритами печатных плат в AltiumDesigner;

4. трассировка печатных плат;
5. экспорт файлов печатных платы в формате STEP;
6. общая сборка устройства в «механической» САПР.

Применение данного алгоритма позволяет максимально детализировать процесс разработки устройства, при этом количество выполняемых действий сводится к минимуму. Замыкание «обратной связи» через последнее действие алгоритма позволяет провести проверку компоновки устройства и исключить нежелательные ошибки.

УДК 004.891

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ПРОЕКТИРОВАНИЯ ОПТИЧЕСКИХ СИСТЕМ

М.А. Колчин

Научный руководитель – к.т.н., доцент Д.И. Муромцев

Краткое вступление, постановка вопроса. Проектирование оптических систем представляет собой последовательный процесс, включающий этапы анализа технического задания, структурного синтеза, параметрического синтеза и ряда других. Существующие на данный момент системы автоматизированного проектирования позволяют эффективно решать задачу параметрического синтеза, в ходе которого рассчитываются точные параметры оптической системы. Но для того, чтобы этап расчета параметров оптической системы оказался успешным, необходимо указать начальную оптическую схему, или «стартовую точку» для проектирования. До сих пор эту задачу решает оптик-проектировщик исходя из своего опыта. В то же время, уже несколько десятилетий для подобно класса задач успешно применяются экспертные системы [1] (ЭС). В НИУ ИТМО накоплен большой опыт по формализации этапа структурного синтеза оптической схемы, начиная от работ М.М. Русинова [2], развитых в трудах И.Л. Лившиц [3]. Это позволяет говорить о возможности создания экспертной системы и для оптического проектирования.

Цель работы. Разработка интеллектуальной системы проектирования оптических систем.

Базовые положения исследования. Экспертная система – это автоматизированная система, способная имитировать способность эксперта принимать решения в проблемах из определенной предметной области.

База знаний (БЗ) – хранилище формализованных правил для решения задачи в предметной области.

Язык представления знаний (ЯПЗ) – формальный язык для записи правил БЗ.

Машина вывода (МВ) – это программа способная производить вывод на правилах, содержащихся в базе знаний экспертной системы. Различают прямой вывод – от исходных фактов к цели, и обратный – вывод фактов от заданной цели.

Промежуточные результаты. В ходе работы был проведен обзор существующих платформ по разработке экспертных систем и выбрана платформа Drools, как наиболее гибкое и мощное решение. Обзор был представлен в докладе [4].

Далее на основе выбранной платформы был разработан прототип системы. Система имеет клиент-серверную архитектуру и как любая экспертная система имеет 4 основных компонента: интерфейса пользователя, машину вывода, базу знаний и редактор БЗ.

Интерфейс пользователя представлен на рисунок.

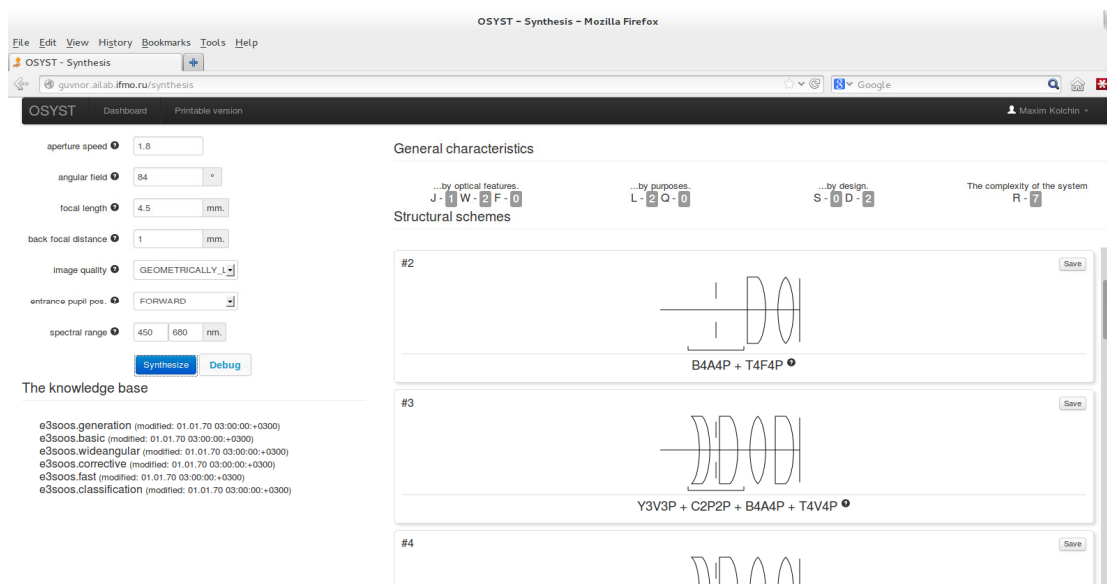


Рисунок. Интерфейс ввода технических требований к ОС

Основной результат, практические результаты. В результате работы был разработан прототип интеллектуальной системы проектирования оптических систем. Прототип системы описан в [5].

Литература

1. Гаврилова Т.А., Муромцев Д.И. Интеллектуальные технологии в менеджменте. – СПб: Изд. ВШМ СПбГУ, 2008. – 488 с.
2. Русинов М.М. Техническая оптика. – Л.: Машиностроение (Ленинградское отделение), 1979. – 448 с.
3. Лившиц И.Л., Сальников А.В., UnchungCho. Исследование возможности решения задачи структурного синтеза объективов методом экспертных оценок // Сборник трудов международной конференции «Прикладная оптика-2004». – СПб: СПбГУ ИТМО. – 2004. – С. 140–144.
4. Колчин М.А., Починок И.Н. Программный инструментарий для структурного синтеза оптических систем. Выбор платформы разработки экспертной системы // Сборник тезисов докладов I Всероссийского конгресса молодых ученых. – СПб: НИУИТМО. – 2012. – Вып. 1. – С. 178–179.
5. Mouromtsev D., Kolchin M. Using Drools rule-platform for the optical CAD web-application development // The 11th FRUCT Conference. – 2012. – P. 100–106.

УДК 004.056.53

МЕТОДЫ ОБРАБОТКИ ГИПЕРСПЕКТРАЛЬНОЙ ИНФОРМАЦИИ

А.Ю. Кузнецов

Научный руководитель – д.т.н., профессор Ю.А. Гатчин

На сегодняшний день существует шесть различных методов обнаружения скрытых объектов защиты информации. Особое внимание следует уделить оптическому методу как одному из наиболее перспективных путей развития методологии обнаружения скрытых объектов защиты информации. К оптическому методу обнаружения скрытых объектов относится дистанционное зондирование. Дистанционное зондирование представляет собой процесс измерения характеристик интересующих пользователя объектов с помощью

чувствительных датчиков, не находящихся в непосредственном контакте с предметом исследования. В настоящее время подобные датчики устанавливаются, как правило, на борту авиационных и космических носителей. Как показывает международный опыт последних десятилетий, наибольшей эффективностью при дистанционном зондировании обладают бортовые видеоспектрометры (imaging spectrometers), основанные на поэлементной регистрации спектров и структуры рассматриваемых удаленных объектов. Они открывают широкие возможности зондирования Земли и околоземного пространства, преодолевая самые изощренные естественные и искусственные маскировки исследуемых объектов. Основным достоинством данного метода является то, что он позволяет наблюдать поверхность Земли в любое время суток, независимо от состояния атмосферы. Видеоспектрометры отличаются от аналогичных классических приборов тем, что помимо обычной спектральной информации – измерения КСЯ – позволяют получать высококачественные панорамные изображения исследуемого объекта во многих различных спектральных интервалах. При этом видеоспектрометры, в отличие от аналогов, не интегрируют КСЯ по всей поверхности объекта, а обеспечивают поэлементную регистрацию КСЯ.

Постановка проблемы. Разработки в области видеоспектрометрии ведутся по всему миру. За последние два десятилетия за рубежом создано несколько десятков видеоспектрометров (гиперспектрометров) авиационного и космического базирования. В России реализованы лишь единичные разработки. К отечественным приборам можно отнести следующие видеоспектрометры: «Фрегат» (разработка НИУ ИТМО), НПО «Лептон», «Сокол-ГЦП». Существует определенная иллюзия, что можно использовать готовое программное обеспечение, поставляемое зарубежными фирмами: получаемые информационные продукты приспособлены исключительно к их же системам дистанционного зондирования. В начале 2000-х годов в России начались разработки программного обеспечения, предназначенного для обработки гиперспектральной информации. В связи с этим необходимо провести анализ и выявить основные тенденции развития методов обработки информации в видеоспектрометрах (гиперспектральной аппаратуре).

Цель работы. Проведение анализа и выявление основных тенденций развития методологии обработки гиперспектральной информации в системах дистанционного зондирования земной поверхности.

Промежуточные результаты. Рассмотрим основные Российские разработки в области обработки гиперспектральной информации.

1. Вычислительная система обработки данных гиперспектрального аэрокосмического зондирования (разработка Московского государственного университета им. М.В. Ломоносова, Московского физико-технического института, Института вычислительной математики РАН, Тверского государственного университета). Основная идея данной разработки заключается в использовании Байесовского формализма нахождения максимума апостериорной вероятности классификации объектов, что соответствует нахождению минимума функции энергии для вероятностного распределения Гиббса относительно случайных переменных, описывающих влияние соседних пикселей для заданного класса объектов.
2. Программно-аппаратный комплекс классификации объектов земной поверхности на основе средств искусственного интеллекта (разработка Рязанского государственного радиотехнического университета и ГНПРКЦ «ЦСКБ-Прогресс» (г. Самара)). Основной идеей данного проекта является использование искусственных нейронных сетей (ВР-сети, SOFM), нечеткой логики 1-го и 2-го типа, генетических алгоритмов и интегральных средств оценки.

3. Программный комплекс GS-VKA (разработка Военно-космической академии им. А.Ф. Можайского). Данное программное обеспечение разрабатывалось для выявления очагов возникновения лесных пожаров и определения уровня загрязненности почв. К основным особенностям данной разработки относятся:

- кластеризация методом Isodata, реклассификация методом спектральной угловой корреляции;
- обнаружение полигонов загрязнения по критерию корреляции;
- исключение ложных объектов по морфометрическим признакам;
- классификация идентифицированных полигонов по степени загрязнения с использованием индекса IS.

Результаты. В результате проведенного анализа следует выявить следующие тенденции развития методов обработки гиперспектральной информации:

1. применение методов искусственного интеллекта в построении алгоритмов идентификации конкретных объектов съемки;
2. разработка и накопление баз данных гиперспектральной информации;
3. совершенствование программного обеспечения в сторону увеличения быстродействия систем обработки гиперспектральной информации;
4. исправление программными методами оптических аберраций.

УДК 681.3

ПРИМЕНЕНИЕ МЕТОДИКИ 3D-МОДЕЛИРОВАНИЯ ПЕЧАТНОЙ ПЛАТЫ В ALTIUMDESIGNER

О.В. Кузнецова

Научный руководитель – к.т.н., доцент Е.Б. Романова

Трехмерные модели (3D-модели) играют большую роль при анализе свойств проектируемого изделия и принятии проектных решений. Они используются практически на всех этапах жизненного цикла изделия и позволяют более полно и наглядно описывать изделие. В докладе рассмотрены основные случаи применения методов 3D-моделирования печатной платы (под печатной платой понимается плата с установленными на ней электронными компонентами) использующиеся в системе AltiumDesigner, а также разработаны рекомендации по использованию методики 3D-моделирования.

Ранее в системе AltiumDesigner была разработана методика формирования 3D-модели печатной платы. Методика основана на следующих методах: методе формирования 3D-модели посредством экструзии средствами системы AltiumDesigner и методе добавления к посадочному месту готовых 3D-моделей корпусов в формате STEP, который осуществлялся в библиотеках посадочных мест электронных компонентов.

В ходе работы детально рассмотрены основные случаи использования соответствующих методов 3D-моделирования, а также перечислены основные команды, используемые при 3D-моделировании электронных компонентов платы. В большинстве случаев используются команды: ShapecreatedfromboundingrectangleonTopOverlay (создание формы по границам прямоугольника в слое TopOverlay); PolygonalShapecreatedfromprimitivesonTopOverlay (создание многоугольной формы из примитивов в слое TopOverlay); «ShapecreatedfromboundingrectangleonAllLayers» (создание прямоугольной формы из примитивов во всех слоях).

В результате проделанной работы были сформированы рекомендации по применению методов 3D-моделирования составляющих базис разработанной методики в системе AltiumDesigner, а также в других САПР печатных плат. Разработаны рекомендации по

применению основных команд используемых для 3D-моделирования корпусов различных электронных компонентов в системе AltiumDesigner.

УДК 621.01

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ГЕРКОНОВЫХ ИЗМЕРИТЕЛЕЙ УРОВНЯ ЖИДКОСТИ В ДАТЧИКАХ СИСТЕМ УПРАВЛЕНИЯ

Р.Я. Лабковская, А.Л. Лысов, О.И. Пирожникова

Научный руководитель – д.т.н., профессор В.Л. Ткалич

В датчиках уровня жидкости поплавкового типа в качестве коммутирующего элемента используются герконы. При достижении жидкостью уровня размещения датчика, поплавков со встроенным магнитом поднимается вместе с уровнем жидкости и замыкает или размыкает контакты геркона.

В настоящее время выпускается широкий ассортимент герконовых датчиков уровня жидкости горизонтального и вертикального исполнения, изготавливаемых из различных материалов и предназначенных для работы в различных средах, в том числе и агрессивных, в диапазоне рабочих температур от +20 до +120°C.

Области применения датчиков уровня жидкости очень разнообразны:

- резервуары для хранения воды;
- водонапорные станции и башни;
- поливочные сооружения;
- бассейны;
- топливно-раздаточные станции и хранилища;
- очистные сооружения;
- паровые системы отопления.

Промышленные датчики уровня бывают четырех типов: радарные, поплавковые, врезные, погружные.

Поплавковые датчики уровня одни из самых недорогих и, вместе с тем, надежных устройств для измерения уровня жидкостей. При правильном выборе, поплавковые датчики уровня могут использоваться для контроля уровня самых разных сред, в том числе химически агрессивных жидкостей. Высокие или низкие температуры, наличие пены, пузырьков или, например работающей мешалки так же перестает быть проблемой при правильном выборе.

Устройство поплавковых датчиков уровня. По конструкции поплавковые датчики уровня могут быть разделены на несколько видов.

Самым простым является датчик с поплавком, передвигающимся по вертикальному штоку. Внутри поплавок, как правило, находится постоянный магнит, а в штоке, представляющем из себя полую трубку, находятся герконы. Плавающая на поверхности жидкости поплавок, передвигается по штоку датчика вслед за изменением уровня и, проходя мимо герконов, внутри штока замыкает, или наоборот размыкает их, сигнализируя о достижении определенного уровня. Внутри штока могут располагаться сразу несколько герконов и, соответственно, один такой датчик может сигнализировать сразу о нескольких значениях уровня жидкости, например минимальном и максимальном.

Поплавковый датчик уровня такой конструкции может так же измерять непрерывный уровень жидкости и выдавать сигнал в виде сопротивления, пропорционального уровню жидкости, либо в виде стандартного токового сигнала 4–20 мА. Для этого герконы внутри штока соединены параллельно с резисторами. Поплавок, передвигаясь вслед за изменением уровня жидкости, замыкает разные герконы, вызывая изменение общего сопротивления

датчика уровня. Такие датчики уровня обычно устанавливаются сверху емкости, и их длина может достигать трех метров.

Отдельной областью применения для поплавковых датчиков уровня можно назвать контроль уровня жидкости в транспортных средствах. Прежде всего, это задачи по контролю за объемом топлива в тяжелой технике: грузовиках, экскаваторах, тепловозах. Здесь датчики уровня работают в условиях сильной вибрации и волнения на поверхности жидкости. Для устранения влияния этих факторов поплавок датчик помещают в специальную демпферную трубу, диаметром чуть большую, чем диаметр поплавка.

Если установка датчика сверху емкости невозможна, то поплавок датчик уровня можно вмонтировать в стенку емкости. В этом случае поплавок с магнитом крепится на шарнире, а герконовый выключатель обычно в корпусе датчика. Такие датчики срабатывают, когда жидкость достигает поплавка и предназначены для сигнализации предельного уровня. Датчики могут работать при температурах до 200°C в химически агрессивных средах.

Если в жидкости высокая концентрация твердых включений, существует вероятность замерзания или создания липкого слоя на оборудовании, то для контроля уровня в этом случае можно использовать поплавок датчик уровня на гибком кабеле. Датчик уровня такого типа представляет собой пластиковый цилиндр или сферу, внутри которой находится механический или герконовый переключатель и металлический шарик. Такой датчик уровня крепится за кабель на нужной глубине, и когда уровень жидкости достигает поплавка, то он переворачивается, и металлический шарик внутри него активирует геркон или механический переключатель. Примером таких датчиков уровня можно назвать серию поплавковых датчиков уровня жидкости LFL.

В настоящее время герконы применяются в автомобильных сигнализациях, в качестве контактных пар тумблеров и кнопок, в качестве датчиков положения и скорости в системах промышленной автоматики и во всевозможных счетчиках.

Литература

1. Ткалич В.Л., Лабковская Р.Я. Библиотека конечных элементов в приложении к упругим чувствительным элементам пластин и мембран датчиков систем управления // Научно-аналитический журнал «Научная перспектива». – 2010. – № 3–4. – С. 86–89.
2. Карабанов С.М., Майзельс Р.М., Шоффа В.Н. Магнитоуправляемые контакты (герконы) и изделия на их основе. Справочное руководство. – М.: Интеллект, 2011. – 432 с.

МОДЕЛИ ПОГРЕШНОСТЕЙ ЧУВСТВИТЕЛЬНЫХ ЭЛЕМЕНТОВ НАВИГАЦИОННОЙ СИСТЕМЫ

А.Л. Лысов, Р.Я. Лабковская

Научный руководитель – д.т.н., профессор В.Л. Ткалич

Модель погрешностей канала построителя вертикали. Линеаризованная модель погрешностей канала ПВ в выработке параметров ориентации и навигационных параметров может быть представлена в следующем виде [1]:

$$\begin{aligned}\dot{\beta} &= -\omega_H \cdot \gamma - \frac{\Delta V_N}{R_3} - \delta\omega_E, \\ \dot{\gamma} &= \omega_H \cdot \beta + \frac{\Delta V_E}{R_3} - \delta\omega_N, \\ \Delta \dot{V}_E &= -n_H \cdot \gamma + \delta a_E - \Delta a_{BE}, \\ \Delta \dot{V}_N &= n_H \cdot \beta + \delta a_N - \Delta a_{BN},\end{aligned}\tag{1}$$

где β , γ – погрешности построения вертикали при моделировании горизонтной СК с географической ориентацией осей (географического сопровождающего трехгранника) ENH (рисунок).

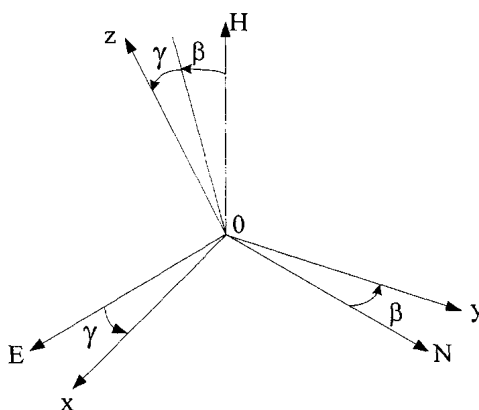


Рисунок. Погрешности ПВ при моделировании горизонтной СК с географической ориентацией осей ENH

ΔV_E , ΔV_N – погрешности в выработке составляющих вектора линейной скорости; $\delta\omega_E$, $\delta\omega_N$ – проекции нескомпенсированных дрейфов ВОГ и так называемых «вычислительных» дрейфов на оси горизонтной СК

$$\begin{bmatrix} \delta\omega_E \\ \delta\omega_N \\ \delta\omega_H \end{bmatrix} = C_h^b \begin{bmatrix} \Delta\omega_{xb} \\ \Delta\omega_{yb} \\ 0 \end{bmatrix},$$

где δa_E , δa_N – проекции инструментальных погрешностей акселерометров на оси горизонтной СК; Δa_{BE} , Δa_{BN} – погрешности компенсации «вредных» ускорений по соответствующим осям, взятые со знаком «-», выражения для которых в приближенном виде будут:

$$\begin{aligned}\Delta a_{BE} &= \Delta V_N (2\Omega + \dot{\lambda}) \sin\varphi, \\ \Delta a_{BN} &= -\Delta V_E (2\Omega + \dot{\lambda}) \sin\varphi,\end{aligned}\tag{2}$$

ω_E , ω_N , ω_H – составляющие вектора угловой скорости вращения горизонтной СК; n_E , n_N , n_H – проекции кажущегося ускорения на оси горизонтной СК.

Как видно из уравнений (1), для описания модели погрешностей канала построения необходимо описание погрешностей чувствительных элементов.

Модель погрешностей волоконно-оптических гироскопов. Модель дрейфов ВОГ может быть представлена в виде суммы трех составляющих:

1. погрешности калибровки начального смещения «нуля» и его нестабильности в пуске, которую будем считать практически постоянной на достаточно длительном интервале времени;
2. погрешности масштабного коэффициента, которая определяет составляющую, пропорциональную измеряемой величине;
3. «шумовой» составляющей, характеризующей флуктуационные погрешности гироскопов.

Таким образом, модель погрешностей имеет вид:

$$\begin{aligned}\Delta\omega_{xb} &= \Delta\bar{\omega}_{xb} + \Delta\tilde{\omega}_{xb} + \Delta\omega_{xb}^{\Phi} \\ \Delta\omega_{yb} &= \Delta\bar{\omega}_{yb} + \Delta\tilde{\omega}_{yb} + \Delta\omega_{yb}^{\Phi},\end{aligned}\tag{3}$$

где $\Delta\bar{\omega}_{xb}$, $\Delta\bar{\omega}_{yb}$ – погрешности калибровки начального смещения «нуля» ВОГ от пуска к пуску с интенсивностями Q_{gx} , Q_{gy} ; $\Delta\tilde{\omega}_{xb}$, $\Delta\tilde{\omega}_{yb}$ – составляющие, характеризующие погрешности масштабных коэффициентов; $\Delta\omega_{xb}^{\Phi}$, $\Delta\omega_{yb}^{\Phi}$ – белозумные составляющие погрешностей гироскопов с интенсивностями Q_{gb}^{Φ} , Q_{gb}^{Φ} .

Погрешности смещения «нуля» ВОГ $\Delta\bar{\omega}_{xb}$, $\Delta\bar{\omega}_{yb}$ и изменения систематических составляющих погрешностей масштабных коэффициентов ΔM_{gx} , ΔM_{gy} , ΔM_{gz} ВОГ от запуска к запуску аппроксимируем соответствующими винеровскими процессами:

$$\Delta\dot{\tilde{\omega}}_{xb} = \sqrt{Q_{gx}} \cdot \xi_1,\tag{4}$$

$$\Delta\dot{\tilde{\omega}}_{yb} = \sqrt{Q_{gy}} \cdot \xi_2,$$

$$\Delta\dot{M}_{gx} = \sqrt{Q_{Mgx}} \cdot \xi_3,\tag{5}$$

$$\Delta\dot{M}_{gy} = \sqrt{Q_{Mgy}} \cdot \xi_4,$$

где ξ_i – центрированные независимые между собой гауссовские белые шумы единичной интенсивности, $i=1,4$; Q_{Mgx} , Q_{Mgy} – интенсивности погрешностей масштабных коэффициентов.

Запишем выражения для составляющих $\Delta\tilde{\omega}_{xb}$, $\Delta\tilde{\omega}_{yb}$, которые пропорциональны погрешности масштабного коэффициента в следующем виде:

$$\Delta\tilde{\omega}_{xb} = \omega_{xb} \Delta M_{gx},$$

$$\Delta\tilde{\omega}_{yb} = \omega_{yb} \Delta M_{gy},$$

где ω_{xb} , ω_{yb} – составляющие вектора угловой скорости вращения связанной с ИБ СК $x_b y_b z_b$ относительно горизонтного трехгранника (ЕНН).

Модель погрешностей акселерометров. В модели погрешностей акселерометров можно выделить следующие составляющие:

- погрешность калибровки начального смещения «нуля» и его нестабильность в пуске, которую будем считать практически постоянной на достаточно длительном интервале времени;
- шумовую составляющую, характеризующую флуктуационные погрешности датчиков:

$$\Delta a_{xb} = \Delta\bar{a}_{xb} + \Delta a_{xb}^{\Phi},\tag{6}$$

$$\Delta a_{yb} = \Delta\bar{a}_{yb} + \Delta a_{yb}^{\Phi},$$

где $\Delta\bar{a}_{xb}$, $\Delta\bar{a}_{yb}$ – погрешности калибровки начальных смещений «нуля» акселерометров с

интенсивностями Q_{Ax} , Q_{Ay} ; $\Delta a_{xb}^\Phi, \Delta a_{yb}^\Phi$ – белозумные составляющие погрешности акселерометров.

Составляющие погрешности смещения «нуля» линейных акселерометров $\Delta \bar{a}_{xb}, \Delta \bar{a}_{yb}$ аппроксимируем винеровскими процессами:

$$\begin{aligned} \Delta \dot{\bar{a}}_{xb} &= \sqrt{Q_{Ax}} \cdot \xi_5, \\ \Delta \dot{\bar{a}}_{yb} &= \sqrt{Q_{Ay}} \cdot \xi_6, \end{aligned} \quad (7)$$

где ξ_i – центрированные независимые между собой гауссовские белые шумы единичной интенсивности, $i=5,6$.

Выводы. Описана модель погрешностей канала ПВ в составе ИНС, включающая модели погрешностей чувствительных элементов. Также представлены необходимые выражения для определения матрицы динамики системы F .

УДК 621.01

СИСТЕМА ТЕРМОСТАТИРОВАНИЯ МАЯТНИКОВОГО ПОПЛАВКОВОГО АКСЕЛЕРОМЕТРА

А.Л. Лысов, Р.Я. Лабковская, О.И. Пирожникова
Научный руководитель – д.т.н., профессор В.Л. Ткалич

Для поддержания постоянной температуры жидкости, а также поплавкового гиросузда в маятниковых акселерометрах предусмотрено автоматическое термостатирование. Время, требующееся на приведение прибора в рабочее состояние, определяется периодом, необходимым для достижения рабочего стабильного температурного режима. Этот отрезок времени достигает значительной величины, и время готовности поплавковых интегрирующих гироскопов пока остается достаточно большим, что сильно снижает тактико-технические данные прибора и объекта. Поэтому при разработке конструкции поплавкового маятникового акселерометра следует обращать серьезное внимание на его параметры, характеризующие его как объект регулирования температуры. Колебания температуры в приборе изменяют вязкость μ и плотность ρ жидкости.

Изменение плотности ρ жидкости приводит к изменению плавучести поплавка, вследствие чего изменяется нагрузка на опоры прибора. Кроме того изменение плотности жидкости может привести к изменению балансировки поплавка, если центр давления вытесненного объема жидкости не совпадает с осью вращения поплавкового гиросузда.

Изменение коэффициента динамической вязкости μ вызывает изменение выходной характеристики прибора. Покажем это на приближенном уравнении движения поплавкового маятникового акселерометра

$$J_x \ddot{\beta} + B \dot{\beta} = H \omega_{y1},$$

где B – коэффициент демпфирования, который определяется размерами зазора и жидкостью.

Или, вводя обозначения постоянной времени и чувствительности, получим

$$T \ddot{\beta} + \dot{\beta} = h \omega_{y1}. \quad (1)$$

Постоянная времени поплавковых маятниковых акселерометров обычно находится в пределах $T=0,002-0,005$ сек, а чувствительность h (или постоянная интегрирования прибора) равна

$$h = \frac{H}{B} = \frac{981H\delta}{2\pi\mu r^3 l_n}. \quad (2)$$

Пренебрегая значением T , из уравнения (1) найдем

$$\beta - \beta_0 = \frac{H}{B} \int_0^t \omega y_1 dt.$$

Для того чтобы результат интегрирования был точным, кинетический момент H и удельный коэффициент демпфирования B должны быть постоянными. Но B является функцией коэффициента μ , величина которого сильно меняется от температуры. Рабочая температура прибора, которая поддерживается системой термостатирования, выбирается несколько выше возможной температуры окружающей среды, чтобы был некоторый перепад между температурой корпуса прибора и средой для обеспечения процесса регулирования.

Так как приборы должны нормально работать при изменении температуры окружающей среды от -60 до $+50^\circ\text{C}$, а температура среды в корпусе системы, в которой используется поплавковый маятниковый акселерометр, может быть выше 50°C за счет выделения тепла различными электрическими устройствами системы, рабочую температуру прибора обычно выбирают в диапазоне $70-85^\circ\text{C}$. В этом диапазоне температур коэффициент динамической вязкости μ меняется незначительно при колебаниях температуры. Благодаря этому чувствительность h прибора практически остается постоянной величиной.

Система автоматического термостатирования прибора состоит из термодатчика – чувствительного элемента температуры, усилителя и обмотки обогрева термостата, выполняющего роль исполнительного органа системы автоматического регулирования.

Обмотку термодатчика наматывают на цилиндрическую поверхность специального стакана и помещают в корпусе прибора как можно ближе к рабочему зазору поплавкового прибора так, чтобы температура обмотки термодатчика соответствовала температуре рабочей жидкости прибора. Для исключения трансформации ложных сигналов от посторонних магнитных полей переменного тока и уничтожения магнитного поля самого термодатчика его обмотка наматывается бифилярно.

Сопротивление термодатчика Γ_T изменяется от температуры по формуле

$$\Gamma_T = \Gamma_{T0}(1 + \varepsilon\Delta t), \quad (3)$$

где ε – температурный коэффициент сопротивления материала провода; Γ_{T0} – сопротивление обмотки термодатчика при рабочей температуре жидкости; Δt – отклонение температуры термодатчика от регулируемой величины.

Питание моста обычно осуществляется напряжением переменного тока.

Если температура обмотки термодатчика соответствует рабочей температуре жидкости, мост сбалансирован. С изменением температуры изменяется сопротивление Γ_T обмотки термодатчика и в диагонали моста появляется напряжение, которое поступает на вход фазочувствительного усилителя.

Реле, которым управляет фазочувствительный усилитель, играет роль усилителя мощности. Обмотка обогрева термостата подключается и отключается от напряжения питания через контакты реле. Укладывают обмотку обогрева на цилиндрической поверхности корпуса прибора и наматывают бифилярно так, чтобы она не создавала магнитного поля.

При установке двух реле термостат делают из двух обмоток: обмотки разогрева и обмотки подогрева. Менее чувствительное реле управляет обмоткой разогрева, а более чувствительное реле-обмоткой подогрева. Такая схема позволяет сократить время готовности прибора.

В целях уменьшения тепловой инерции между обмоткой обогрева и термодатчиком обе обмотки располагают в непосредственной близости на цилиндрической поверхности корпуса прибора. Однако в этом случае система термостатирования обеспечивает только поддержание температуры обмотки термодатчика и температуры цилиндрической поверхности корпуса

прибора. Температура жидкости в рабочем зазоре при колебаниях окружающей температуры может значительно отличаться от рабочей вследствие изменения теплоотдачи прибора через его торцовые поверхности.

На точность рабочей температуры жидкости значительное влияние оказывают внутренние источники тепла (гиромотор, датчики угла и момента) прибора, а также колебания частоты и напряжения питания фазочувствительного усилителя и термочувствительного моста. Еще с более низкой точностью поддерживается температура вдоль выходной оси прибора.

Для компенсации расширения жидкости при работе системы термостатирования в конструкции поплавковых приборов предусматривается сильфон. Размеры сильфона и его ход рассчитываются из условия компенсации объемного расширения жидкости поплавковой камеры от температуры хранения до рабочей температуры.

При разогреве прибора или его охлаждении подпятники прибора воспринимают значительные усилия из-за проявления «поршневого эффекта». Проявление «поршневого эффекта» связано с тем обстоятельством, что, например, при разогреве прибора приращение объема жидкости, расположенной в торцовой камере поплавковой камеры с противоположной стороны сильфона, должно компенсироваться перетеканием жидкости к сильфону через узкую кольцевую щель между поплавком и корпусом прибора.

Для перетекания жидкости через узкую кольцевую щель на торцовых поверхностях поплавок должен возникнуть значительный перепад давления. Для уменьшения перепада давлений и снижения осевых усилий «поршневого эффекта» в конструкции прибора предусматривают проходные каналы. Поперечное сечение проходных каналов и количество их определяется из допустимого усилия на подпятник и интенсивности разогрева прибора.

УДК 004.82, 65.012.123

ОБЗОР ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ ДЛЯ ПОСТРОЕНИЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ В ОБРАЗОВАНИИ

Г.Л. Маркина

Научный руководитель – д.т.н., профессор С.К. Стафеев

Управление сложным объектом (системой, процессом) можно рассматривать как последовательность процедур поиска (выбора) и принятия решений на всех этапах жизненного цикла объекта управления. При управлении системами поддержки принятия решений в сложных ситуациях проблема выбора лучших решений является одной из наиболее важных. Выбор и принятие решений происходят в условиях многокритериальности выбора, неполноты исходной информации. С развитием современных информационных технологий все большее внимание уделяется созданию и использованию интеллектуальных систем поддержки принятия решений.

Постановка проблемы. Разработка методов, средств и технологий построения систем поддержки принятия решений (СППР) составляет предмет исследования многих направлений науки. Разработанные теории позволили и позволяют эффективно решать многие практические задачи, как обработки информации, так и управления. Однако всегда существовал и существует значительный класс реальных задач, для которых применение классических методов либо невозможно, либо затруднено. Это связано с естественным разрывом между положениями, на которых базируются те или иные математические методы и свойствами информации о реальных объектах реальной задачи.

Цель работы. Проведение аналитического обзора интеллектуальных методов для построения систем поддержки принятия решений.

Основной результат. Проведен аналитический обзор литературы, который показал, что в настоящее время интеллектуальные системы поддержки принятия решений в области образования применяются крайне редко. В основном используются такие системы в медицине, бизнесе, промышленности. Также рассмотрены различные методы построения систем интеллектуального анализа данных, приведены примеры таких СППР.

Группа BISC в университете Беркли, Калифорния, под руководством Л. Задэ успешно реализует дедуктивный подход – Нечеткую Логику [1]. Группа красноярских ученых использовала индуктивный нейросетевой подход для решения широкого круга задач в различных областях человеческой деятельности [2]. Группа нейросетевых исследований (NeuralNetworksResearchGroup) в Университете Остина, штат Техас, под руководством Мииккулайнена (RISTOMiikkulainen) [3] в рамках индуктивного подхода синтезирует нейросетевые и эволюционные алгоритмы, как и группа украинских ученых, разработавших метод группового учета аргументов, предложенных А.Г. Ивахненко [4].

Сотрудниками ЮФУ [5] для разработки интеллектуальных систем поддержки принятия решений был предложен метод отыскания наилучшего решения при многих критериях и наличии нескольких экспертов одновременно (с возможностью учета важности каждого из экспертов). Сотрудниками Волгоградского государственного технического университета для решения задачи обеспечения поддержки лица, принимающего решение о реализации конкретных антипаводковых мер, была сформулирована концепция интеллектуальной системы поддержки принятия решений для задачи управления водохозяйственной системой реки Эльба [6]. В Оренбургском государственном университете для создания ИСППР было предложено использовать относительную независимость отдельных модулей, содержание и назначение которых, равно как и моменты связывающие их между собой (интерфейсы) описаны параллельно.

Литература

1. Zadeh L.A. From computing with numbers to computing with words – from manipulation of measurements to manipulation of perceptions // *IEEE Transactions on Circuits and Systems*. – 1999. – V. 45. – P. 105–119.
2. Горбань А.Н., Дунин-Барковский В.Л., Кирдин А.Н. Нейроинформатика. – Новосибирск: Наука. Сибирское предприятие РАН, 1998. – 296 с.
3. Using marked-based genetic encoding of neural networks to evolve finite – state behavior // *Proceedings of the First European Conference on Artificial life (EACAL 91)*. – Cambridge. MA^MIT Press. – 1992. – P. 255–262.
4. Ивахненко А.Г., Мюллер И.А. Самоорганизация прогнозирующих моделей. – Киев: Техника, 1985. – 224 с.
5. Глушань В.М., Карелин В.П., Кузьменко О.Л., Выбор лучшего управленческого решения при нечетких исходных данных и множественности критериев // *Известия вузов. Сев.-Кавказский регион, Технические науки*. – 2006. – Прил. №1. – С. 158–165.
6. Дворянкин А.М., Дворянкин М.Б., Кульцова М.Б., Жукова И.Г., Капыш А.С., Кульцова А.Е. Интеграция онтологии и рассуждений по прецедентам и правилам в системе управления водохозяйственной системой реки Эльба // *Открытое образование: приложение к журналу [по мат. междун. конференций, Ялта-Гурзуф 2008г.]*. – 2008. – Б/н. – С. 125–126.
7. Дворянкин А.М., Кульцова М.Б., Жукова И.Г., Кольцова А.Е., Капыш А.С. Разработка онтологической базы знаний для интеллектуальной системы поддержки принятия решений в сфере управления водохозяйственной системой // *Известия ВолгГТУ*. – 2008. – С. 95–99.

8. Ахмедьянова Г.Ф., Пищухин А.М. Интеллектуальная система поддержки принятия педагогических решений // Научный журнал «Фундаментальные исследования». – 2008. – № 5. – С. 48–51.
9. Нечаев В.В., Дарьин А.В. Интеллект – стратегический ресурс информационного общества // Проблемы информатизации. – 2001. – № 1. – С. 37–41.
10. Валькман Ю.Р., Валькман Р.Ю., Исмагилова Л.Р. Бизнес-интеллект и управление знаниями: понятия, технологии, интеллектуальность // Труды Международных НТК IEEE AIS. – М.: Физматлит, 2009.

УДК 004.056.5

МЕТОД ФОРМАЛЬНОГО ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ

Т.А. Маркина

Научный руководитель – д.т.н., профессор А.Ю. Щеглов

Известные методы проектирования системы защиты строятся на основе стандарта ГОСТ ИСО МЭК 15408-2002 «Общие критерии оценки безопасности информационных технологий» [1] и на основе его прототипа – международного стандарта «CommonCriteriaforInformationTechnologySecurityEvaluation» [2]. Эти стандарты обобщают подходы к построению системы защиты на основе учета качественного состава механизмов и средств защиты.

Постановка проблемы. Существующие критерии для проектирования системы защиты основываются на защите от конкретной атаки. Они не рассматривают атаку как взаимосвязанную последовательность реализаций угроз, и не учитывают тот фактор, что не эффективно строить защиту, основываясь на определенной угрозе.

Цель работы. Разработка метода формального проектирования системы защиты на основе представления атаки на направленном графе и его оптимизация с целью найти такую угрозу, нивелирование которой позволит минимизировать риск.

Базовые положения исследования. Под угрозой информационной безопасности АС понимается возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к искажению уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носители информации, средства взаимодействия с носителем или средства его управления.

Вероятность того, что угроза будет использована, определяется вероятностью осуществления атаки на эту угрозу.

Под атакой (attack, intrusion) на информационную систему понимается действия (в общем случае последовательность связанных между собой действий нарушителя), которые реализуют угрозы.

Промежуточные результаты. Предложен метод проектирования системы защиты, состоящий в следующем: с использованием теории рисков при проектировании рассматривается в качестве элемента не угроза, а атака, которая представляется последовательностью реализации угроз с заданной вероятностью. Метод предполагает оптимизацию направленного взвешенного графа (рисунок) с целью определения и нивелирования наиболее актуальных угроз, присутствие которых приводит к максимальному риску.

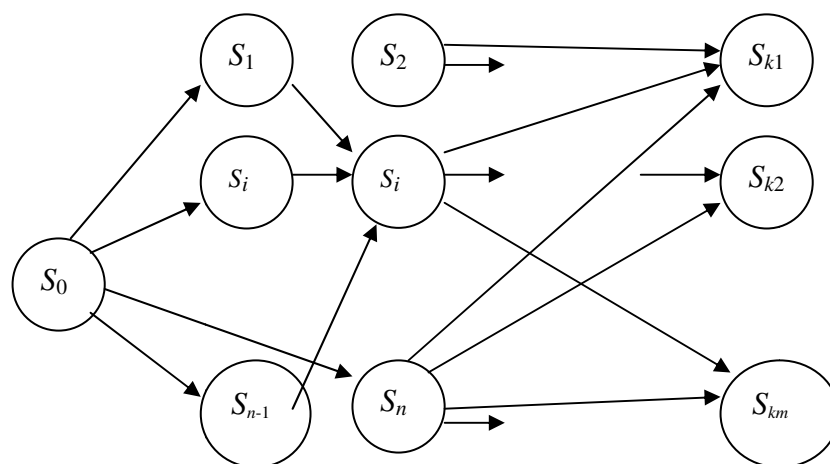


Рисунок. Представление атаки на направленном графе

$$R = \sum_{i=1}^k p_{S_0 \rightarrow S_k} * C_i$$

где S_0 – исходное безопасное состояния; безопасное состояние (Safestate) – это предопределенное начальное состояние системы; S_k , где k от 1 до m – конечное событие, характеризующее потерей от осуществления атаки (цели атак ИБ, в том числе, нарушение конфиденциальности, целостности и доступности); S_i , где i от 1 до n – вершины графа – состояние системы с условием реализации угрозы при осуществления атаки, она осуществляется слева направо; дуги между вершинами – переход из одного состояния ИС в другое с определенной вероятностью наличия угроз – p_i .

Под длиной пути понимаем вероятность перехода из состояния S_0 в состояние S_k .

В качестве основного критерия оптимизации при проектировании системы защиты на данном взвешенном направленном графе используется путь, который имеет наибольшую вероятность перехода из состояния S_0 в состояние S_k . Далее следует определить вершину, нивелирование которой по заданному критерию позволит исключить критичную совокупность ветвей. Исключение пути позволит минимизировать риск и уменьшить потери.

Специфичность метода заключается в том, что граф может изменяться, основываясь на актуальных угрозах информационной безопасности. Количество промежуточных состояний и переходов между состояниями может увеличиваться и уменьшаться.

Основные результаты. Разработан метод формального проектирования системы защиты. Определен основной критерий оптимизации, который позволяет минимизировать риск.

Литература

1. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Часть 1. Введение и общая модель. Часть 2. Функциональные требования безопасности. Часть 3. Требования доверия к безопасности. – Госстандарт России, Москва, 2002.
2. Common Criteria for Information Technology Security Evaluation. Version 2.2. Revision 256. Part 1: Introduction and general model. – January 2004.

**ЛАБОРАТОРНАЯ УСТАНОВКА ДЛЯ ИЗМЕРЕНИЯ ВЫСОКОЧАСТОТНЫХ
ВОЛЬТ-ЕМКОСТНЫХ ХАРАКТЕРИСТИК СТРУКТУР Si/SiO₂
НЕРАЗРУШАЮЩИМ МЕТОДОМ**

В.А. Нурмухамедов

Научный руководитель – ст. преподаватель К.О. Ткачев

Цель работы – разработать лабораторную установку для измерения высокочастотных вольт-емкостных характеристик структур Si/SiO₂ неразрушающим методом.

Анализ существующих методов измерения высокочастотных вольт-емкостных характеристик показал необходимость создания специализированных тестовых МОП-структур, что влияет на электрофизические параметры структур Si/SiO₂. Это, в свою очередь, не позволяет провести корректный анализ изменения электрофизических параметров Si/SiO₂ структур, в процессе производства на разных стадиях технологического цикла создания полупроводниковых приборов. Ввиду этого остро встает вопрос метрологического обеспечения в области неразрушающих методов измерения высокочастотных вольт-емкостных характеристик и появляется необходимость разработки лабораторной установки отвечающей поставленным требованиям.

Результатом работы явилась разработанная лабораторная установка для измерения высокочастотных вольт-емкостных характеристик структур Si/SiO₂, представляющая собой: прецизионный источник питания, программно управляемый высокоточный цифровой измерительный блок, построенный на базе приборов NationalInstruments, с подключенной к нему зондовой установкой, обеспечивающей контакт с верхним слоем SiO₂ при помощи плоского зонда.

В процессе разработки установки были испытаны различные конструкции и материалы изготовления верхних зондов. Впоследствии были получены, структурированы и проанализированы данные полученные с испытуемых зондов, что позволило судить о качестве проведенных измерений и выбрать конструкции зондов соответствующие поставленной задаче.

В процессе исследования конструкций зондов была получена плоская зона зонда, эквивалентная верхней обкладке МОП структуры, радиусом около 80 мкм. При этом значения емкости сформированного в процессе МОП-конденсатора составило приблизительно 1 пФ. Нижний омический контакт обеспечивается и контролируется посредством 4-х вольфрамовых зондов подключаемых к нижней части полупроводниковой пластины.

Конструкция установки предполагает легкую замену зондов и выбор конфигурации измерительного блока, для проведения измерений с различными требованиями к точности, а так же с различными требованиями к типу измеряемых электрофизических параметров структуры Si/SiO₂.

Разработанная установка позволяет измерять электрофизические характеристики исследуемых полупроводниковых пластин с выращенным на поверхности слоем SiO₂, с учетом паразитных эффектов и других, негативно сказывающихся на точности измерения факторах, без создания тестовых структур приводящих к изменению электрофизических свойств структур Si/SiO₂.

МЕТОДИКА ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ВИРТУАЛЬНОЙ СЕТИ В ОБЛАЧНЫХ СИСТЕМАХ

А.О. Очередыко

(Оренбургский государственный университет)

Научный руководитель – к.т.н., доцент Ю.А. Ушаков

(Оренбургский государственный университет)

Ключевой проблемой в децентрализованных моделях безопасности и распределенных инфраструктурах является исполнение политик безопасности, особенно, если бизнес-процессы охватывают несколько организаций. На текущий момент наиболее распространенным решением по обеспечению информационной безопасности является защита конечных точек. При этом, управление распределенными инфраструктурами становится небезопасным и затрудняется взаимодействие с внешними запросами. Для решения этих задач была предложена архитектура безопасности, которая переносит модель программного обеспечения как услуги (Saas, Software as a Service) в безопасную область, и тем самым реализуя безопасность как услуга (Seaas, Security as a Service).

SEaaS – модель обеспечения безопасности, реализуемая на удаленной системе, которая находится в собственности третьей стороны (одного или нескольких поставщиков услуги). Поставщик обеспечивает функции безопасности, основанные на разделяемых технологических услугах, которые потребляются в рамках модели «один ко многим» с оплатой по факту использования объема потребленных услуг.

Сеть как услуга (Naas, Network as a Service) – это модель облачного сервиса, дающая возможность пользователю использовать виртуальную сеть со всеми преимуществами реальной сети. С точки зрения защиты, ключевыми моментами являются конфигурирование, мониторинг сети и политика безопасности. Seaas идеально подходит для децентрализованного управления политикой безопасности, сформированной в соответствии с концепцией безопасности организации.

В рамках исследования были поставлены следующие задачи:

1. проведение сравнения методов и средств защиты виртуализированных сетей с традиционными методами и средствами защиты в КС;
2. проведение анализа сервисов/приложений, применяемых для защиты виртуализированных сетей.

По данным исследования, проведенным в 2012 г., рынок облачных услуг составил 4,5 млрд. рублей, и ожидается, что к 2016 г. он вырастет до 19 млрд. рублей. При этом затраты организации на ИТ снижаются на 20–60%.

Исследование направлено на выявление возможных угроз для виртуализированных сетей, разработку методов организации моделей безопасности в облачных системах. **Целью исследования** является построение единой безопасной сети, расположенной в облаке для децентрализованных организаций с разными политиками безопасности.

Наибольшая практическая значимость данного исследования будет представлена для распределенных инфраструктурах: систем электронного документооборота (СЭД) и систем управления взаимоотношениями с клиентами (CRM, Customer Relationship Management).

Анализ научно-информационных источников показал отсутствие эффективных решений по проблеме исследования.

СИСТЕМЫ ЗАЩИТЫ И СИГНАЛИЗАЦИИ НА ОСНОВЕ ГЕРКОНОВОЙ ЭЛЕМЕНТНОЙ БАЗЫ

О.И. Пирожникова, Р.Я. Лабковская

Научный руководитель – д.т.н., профессор В.Л. Ткалич

Термобиметаллические пружины могут быть получены путем сварки, пайки или совместной горячей прокатки двух пластин из металлов с разными температурными коэффициентами линейного расширения α_1 и α_2 получают так называемые термобиметаллические (ТБ) плоские пружины. Слой биметалла с $\alpha_1 > \alpha_2$ называют активным, а с $\alpha_1 < \alpha_2$ – инертным. При нагреве ($\Delta t > 0$) ТБ-пружина изгибается в сторону инертного слоя, а при охлаждении ($\Delta t < 0$) – в сторону активного.

Для создания высокой чувствительности материалы обоих слоев должны обладать не только резко отличными температурными коэффициентами линейного расширения, но и высокими упругими свойствами, обеспечивающими работу пружины в пределах закона Гука. Кроме того, металл должен хорошо свариваться или спаиваться, а также обладать высокой пластичностью для прокатки в ленты толщиной $\delta = 0,2\text{--}2,0$ мм. Если биметалл предназначен работать в условиях высоких температур, то его материал должен быть и термостойким. Этим требованиям в значительной мере удовлетворяют железоникелевые сплавы. Из них широкое применение получил термобиметалл ТБ-3 с инертным слоем из инвара Н36 (35–37% Ni, 65–63% Fe, $\alpha_2 = 10^{-6}$) и активным слоем из маломагнитной стали (26,5–28% Ni, 5,5–6,5% Mo, 68–65,5% Fe, $\alpha_1 = (18\text{--}20) \cdot 10^{-6}$).

ТБ-3 обладает высокой чувствительностью, стабильностью характеристики, большим электрическим удельным сопротивлением.

Кроме инвара для пассивного слоя применяют и платинит Н42, а для активного – хромоникелевую и никельмолибденовую стали.

Для расчета ТБ-пружин необходимо установить зависимость, связывающую деформацию пружины λ с изменением температуры Δt .

Изменение кривизны ТБ-пластины при нагреве Δt для пластин из нормального ТБ-металла выражается формулой

$$\Delta\chi = \frac{3}{2} (\alpha_1 - \alpha_2) \frac{\Delta t}{(h_1 + h_2)}.$$

При одновременном действии температуры Δt и внешней нагрузки M перемещение любой точки ТБ пружины можно найти с помощью интеграла Мора. Так как $\Delta\chi = \frac{M}{(EJ)}$, где M – изгибающий момент, то формулу можно записать следующим образом:

$$\lambda = \frac{3}{2} (\alpha_1 - \alpha_2) \frac{\Delta t}{(h_1 + h_2)} \int_0^l M_1 dz,$$

где M_1 – изгибающий момент от единичной нагрузки, приложенной в направлении искомого перемещения; l – длина пластины.

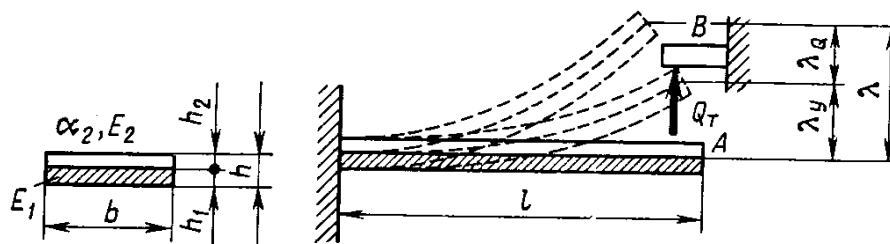


Рисунок. Консольная ТБ-пружина геркона

Один из контактов геркона может быть выполнен из плоской ТБ-пластины (рисунок). В противоположном торце стеклянного баллона геркона запаян плоский контакт, выполненный из ферромагнитного токопроводящего материала. При замыкании контактов обеспечивается замыкание аварийной сигнализационной цепи защиты от повешенной температуры.

На примере геркона определим, на каком расстоянии λ_y следует установить контактный сердечник (B) для того, чтобы при нагреве консольной ТБ-пружины (рисунок) на Δt осуществлялся контакт конца пружины A и контактный (B) с усилием Q_r . Размеры h , b , l и материал пружины (α_1 , α_2 , E_1 и E_2) заданы.

1. Свободное перемещение конца пружины A (при отсутствии КС)

$$\lambda = \frac{3}{2} (\alpha_1 - \alpha_2) \frac{\Delta t}{h} l^2.$$

2. Рассматривая действие неподвижного контакта как действие на пружину силы Q_T в точке A, вызывающем деформацию λ_Q , получаем

$$\lambda_Q = \frac{Q_T l^3}{(3E_{\text{пр}} J)},$$

где $E_{\text{пр}} = \frac{4E_1 E_2}{(\sqrt{E_1} + \sqrt{E_2})^2}$ – приведенный модуль упругости биметалла (E_1 – активного;

E_2 – инертную слоев); $J = \frac{b^2 h}{12}$ – момент инерции поперечного сечения пружины.

3. Искомое расстояние $\lambda_y = \lambda - \lambda_Q$.

Литература

1. Карабанов С.М., Майзельс Р.М., Шоффа В.Н. Магнитоуправляемые контакты (герконы) и изделия на их основе. Справочное руководство. – М.: Интеллект, 2011. – 432 с.
2. Ткалич В.Л., Лабковская Р.Я. Библиотека конечных элементов в приложении к упругим чувствительным элементам пластин и мембран датчиков систем управления // Научно-аналитический журнал «Научная перспектива». – 2010. – № 3–4. – С. 86–89.

УДК 621

ПЕРСПЕКТИВНЫЕ РАЗРАБОТКИ ДЛЯ БОРТОВЫХ УСТРОЙСТВ ИЗМЕРЯЮЩИХ УСКОРЕНИЯ

А.В. Плотников, С.О. Салтыков

Научный руководитель – д.т.н., профессор В.Л. Ткалич

В работе осуществлены патентные исследования устройств, предназначенных для измерения ускорений в навигации. Эти устройства предназначены для применения в качестве чувствительного элемента в системах стабилизации, наведения и навигации.

Исследование разделено на 5 подгрупп по целям совершенствования устройств.

1. Повышение быстродействия:

- повысить быстродействие устройства возможно за счет введения в цифровой канал схемы управления потоком входной информации;
- за счет усложнения схем аналогового и цифрового каналов приема-передачи сигналов.

2. Повышение точности вычислений:

- повышение точности вычислений осуществляется за счет наличия дискретизаторов, которые приводят к запоминанию информации на время преобразования, что

исключает апертурную ошибку, связанную с изменением входной информации, а также за счет наличия накопителя цифровой информации;

- есть также и другие способы, такие как: работа устройства в автоколебательном режиме, а также за счет того, что измеряемое ускорение пропорционально цифровому коду и не зависит от динамических показателей;
- за счет введения двух параллельных каналов с датчиком угла и мостовой схемы и двух параллельных отрицательных обратных связей;
- за счет введения цифрового интегрирующего канала с выхода первого реверсивного двоичного счетчика на вход датчика момента;
- за счет усилительно-преобразующего тракта, охваченного как отрицательной обратной связью, так и пересекающимися положительными обратными связями, значения фазы равным нулю по несущей частоте и опережение по фазе по огибающей частоте

3. Повышение устойчивости системы:

- за счет введения обратных связей противоположных знаков ;
- за счет того что устройство содержит местную положительную обратную связь, в которую введено апериодическое звено, местную отрицательную обратную связь, в которую введен широкополосный фильтр второго порядка, и отрицательную интегрирующую обратную связь.

4. Увеличение полосы пропускания:

- за счет введения в обратную связь прецизионного релейного элемента, управляемого знаковым разрядом второго комбинационного двоичного сумматора;
- за счет введения двух параллельных каналов с датчиком угла и мостовой схемы и двух параллельных отрицательных обратных связей;
- за счет введения обратных связей противоположных знаков.

5. Повышение чувствительности прибора:

- за счет введения усилительно-преобразующего тракта, охваченного как отрицательной обратной связью, так и пересекающимися положительными обратными связями, значения фазы равным нулю по несущей частоте и опережение по фазе по огибающей частоте.

Из всех разработанных изделий, которые применяются в системах стабилизации, наведения и навигации, можно выбрать устройство для определения ускорений, описанное в патенте RU 2165625. Так как оно удовлетворяет основным требованиям, применяемым к изделиям данного вида. Введение в устройство обратных связей разных знаков обеспечивает устойчивость устройства и расширение полосы пропускания, отрицательная интегрирующая обратная связь повышает точность за счет астатизма первого порядка, а также за счет формирования в ней импульсной связи. Однако не мало важным фактором является и быстродействие, обеспечиваемое устройством описанным в патенте RU 2190857. Способ повышения быстродействия, за счет введения в цифровой канал приема-передачи сигналов схемы управления входным потоком, описанный в данном патенте, может также применяться в любом изделии данного вида, так как управление потоком происходит еще до его начальной обработки, а следовательно интеграция, например, изделия, описанного в патенте RU 2165625, и изделия описанного в патенте RU 2190857, даст нам существенный прирост производительности, без потери других параметров.

Литература

1. Патенты РФ с 2001 по 2011 гг.: RU 2163380; RU 2165625; RU 2171994; RU 2171995; RU 2189046; RU 2190226; RU 2190857; RU 2190858; RU 2226695; RU 2405160.

РАЗРАБОТКА МОДУЛЕЙ УПРАВЛЕНИЯ УМНЫМ ДОМОМ НА ОСНОВЕ КОНТРОЛЛЕРОВ ARDUINO

С.О. Попов, П.Д. Золов

Научный руководитель – д.т.н., профессор В.Г. Парфенов

В настоящее время цена контроллера Arduino позволяет покупать их широкому кругу разработчиков и начинающим командам. Контроллеры Arduino имеют достаточно дружелюбный интерфейс для начинающих программистов, а также базируются на промышленных контроллерах Atmel. Что позволяет применять их, например, в системах домашней автоматизации, которая требует управления различными нагрузками с использованием реле. Однако существуют ситуации, когда обычное реле не всегда применимо. Например, при перезагрузке контроллера от срабатывания сторожевого таймера или просто сбоя в питании, контроллер на время снимает управляющие сигналы с реле. Что приводит к выключению нагрузок и включению их через пару секунд. Такой перебой питания часто не приемлем для сложной техники или освещения. А также обычные реле все время тратят энергию, для поддержания себя во включенном состоянии, что не приемлемо в системах с ограниченными возможностями по питанию.

Основная **цель работы**, это решение проблемы переключения реле при выключении питания контроллера.

Было принято решение разработать дополнительный модуль к контроллеру Arduino, который бы решал указанные проблемы с помощью бистабильных реле. Бистабильные реле управляются импульсом и запоминают свое состояние после переключения, не тратя энергию в дальнейшем. В результате исследований было принято решение использовать реле производства компании finder, они имеют розетки на печатную плату, что позволяет без пайки быстро заменить реле на месте.

В результате была спроектирована и отправлена в производство шилда, получено несколько опытных образцов. Шилда обладает следующими особенностями:

Шилда предназначена для использования с контроллерами Arduino UNO или Arduino MEGA. На шилде установлены две finder розетки 95.15.2 для подключения реле серий 40.51, 40.52, 40.61. Могут быть использованы как обычные, так и бистабильные реле. Рекомендованное реле для использования на шилде: 40.52.6.005.0000.

Конструктивные особенности шилды: возможность питания реле от стороннего источника питания до 36 вольт; выбор источника питания определяется джампером; 4 кнопки для ручного управления реле; один общий джампер отключения команд с контроллера; по четыре винтовых разъема на каждую сторону реле из трех контактов. Что позволяет протянуть шину питания без использования скруток. Форма платы позволяет использовать дополнительные шилды, а также устанавливать данную шилду на Ethernet шилду. Установка двух данных шилд друг на друга не возможна в силу высоты реле.

Для работы с контроллером Arduino используются контакты 6,7,8,9.

В настоящее время шилда проходит финальное тестирование и готовится к выходу на свободный рынок.

Планируется увеличение количества реле на шилде, а также отказ от использования выводов контроллера, в пользу расширителя портов работающего на одной из шин контроллера, что позволит расширить список совместимых шилд.

СОЗДАНИЕ ВЕРХНЕУРОВНЕВОЙ АРХИТЕКТУРЫ ИНТЕРНЕТА ВЕЩЕЙ

С.О. Попов, Е.В. Черный

Научный руководитель – д.т.н., профессор В.Г. Парфенов

В настоящее время активно развиваются сервисы по созданию интернета вещей. Они позволяют переносить мониторинг и управление различными устройствами в облако устройств. Благодаря подключению всех устройств к облаку можно обеспечить их взаимодействие на принципиально новом уровне. Например, если раньше робот уборщик был системой в себе и работал по таймеру, не зная о существовании других систем вообще. То с применением интернета вещей можно сообщить роботу уборщику, что пользователь покинул помещение и можно начинать уборку. Также появляются дополнительные возможности по энергосбережению и учету ресурсов.

Основная **цель работы** определить верхнеуровневую архитектуру интернета вещей. Описать основные компоненты и проблемы системы.

В результате работы было решено строить систему максимально простой на стороне устройств. Каждое устройство содержит только две функции, это передача состояния и исполнение команды. В простейшем случае устройство не задумывается о значении команды и своего состояния. Например, команда включить свет ничем не ограничивается, считается, что она не может нанести ущерба. Но существуют сложные системы, например стиральные машины, они уже обладают некой собственной волей с целью обеспечения безопасности. Например, нельзя запустить барабан машины при не заблокированной дверце машины. При этом исполнительное устройство должно отвергнуть команду сервера на запуск двигателя барабана.

Принятое построение устройств подразумевает постоянное соединение с сервером и защиту от сбоев связи. Применение общих центральных серверов, в отличие от локальных домашних, позволяет производить обновление функционала устройств, обеспечить гибкость системы, статистику использования и низкую стоимость системы.

В независимости от расположения серверов существует две основные проблемы по организации работы. Это подключение любой новой техники от чайника, до систем жизнеобеспечения и отслеживания состояния пожилых людей. Такую гибкость могут обеспечить технологии семантического интернета, в том числе RDF хранилища данных. Однако они не решают второй проблемы по хранению потоковых данных. Поточные данные могут генерироваться ежесекундно. Поэтому отдельная база данных должна хранить набор часто схожих значений, а также отслеживать возможность удаления устаревшей статистики из истории потока.

Отдельные проблемы связаны с безопасностью и обеспечением невозможности перехвата управления или определения набора устройств в доме. Также существуют проблемы с безопасностью и разграничением прав доступа в общих RDF базах данных.

В настоящее время создаются пробные реализации вышеописанной системы на основе разработанных под нее исполнительных и передающих данные устройств. Дальнейшие исследования направлены на практическую реализацию и отработку архитектуры системы в реальных условиях, а также решение проблем хранения, обеспечения доступа и безопасности данных и команд.

ЭЛЕКТРОДНЫЕ СИСТЕМЫ ЭЛЕКТРОХИМИЧЕСКИХ КОАГУЛЯТОРОВ В УСТРОЙСТВАХ ПОЛУЧЕНИЯ ПИТЬЕВОЙ ВОДЫ

С.О. Салтыков, А.В. Плотников

Научный руководитель – к.т.н., доцент А.В. Панков

Аналитический обзор существующих разработок устройств обработки питьевой воды по методу электрохимической коагуляции выявил серьезные недостатки в конструкциях электродных систем. В обзоре рассмотрены устройства «Аквалон», «БСЛ-Мед» и «Водолей». Во всех этих устройствах электродные системы не обеспечивают одинаковый режим обработки всей массы обрабатываемой воды, что не позволяет достичь ее эффективного обеззараживания.

Конструкция электродных систем для обеспечения механической жесткости требует значительной толщины растворимых электродов, что обуславливает необходимость периодической зачистки их поверхностей для эффективного использования массы растворимого материала электродов.

Конструкция сменных электродов не позволяет обеспечить надежный контакт их с внешней электрической цепью, что определяет невысокую надежность системы.

Для устранения перечисленных недостатков была проведена разработка электродного блока кассетного типа, что позволило, практически полностью освободиться от недостатков разработанных ранее конструкций.

В новой конструкции весь объем обрабатываемой воды подвергается одинаковому электрическому воздействию, что гарантирует эффективное обеззараживание воды. Растворимые электроды соединены в общую электрическую цепь последовательно, при этом контакт их в этой цепи осуществляется по всей поверхности электродов через водные промежутки.

В конструкции кассеты с растворимыми электродами обеспечены условия необходимой жесткости электродов при малой толщине, которая позволяет практически полностью израсходовать материал электродов без механической очистки их поверхности.

Быстросъемная кассета позволяет легко заменять свободно лежащие в ней растворимые электроды и не требует квалифицированного персонала для обслуживания.

Разработанная конструкция защищена патентом.

РАЗРАБОТКА МЕТОДОВ ПОИСКА ШАБЛОНОВ ВЗАИМОДЕЙСТВИЯ ВСТРОЕННЫХ СИСТЕМ

Е.А. Святушенко

Научный руководитель – аспирант С.О. Попов

В рамках проекта [1] разрабатывается централизованная, расширяемая система для накопления данных и контроля над объектами. Одним из наиболее важных аспектов данного проекта является уменьшение стоимости и увеличение производительности встраиваемых вычислительных машин, широкое внедрение встроенных систем управления в быт человека.

Разработка методов выявления закономерностей и построения на их основе шаблонов поведения и взаимодействия встроенных систем поможет обеспечить такие положительные особенности разрабатываемой системы, как [2]:

- оптимальное распределение ресурсов между системами, энергоэффективность;
- возможность автоматически обучать систему, чтобы она могла самостоятельно принимать

- решения в зависимости от набора факторов окружающей среды;
- возможность применения системы для осуществления помощи одиноко проживающим пожилым людям;
 - значительное повышение комфорта пользователя системой.

Целью работы является найти способ анализировать поведение встроенных систем в зависимости от различных параметров окружающей среды, и на основе проведенного анализа выстраивать необходимое их взаимодействие автоматически при попадании системы в сходные условия. Таким образом, будут найдены шаблоны поведения встроенных систем, которые можно было бы использовать либо как рекомендации пользователю (создание профилей, режимов работ в системе), либо для автоматического обучения системы.

В результате работы было решено использовать генетический алгоритм [3] для поиска наиболее выгодных шаблонов поведения встроенных систем. Генетический алгоритм применяется к уже существующему минимальному набору шаблонов, построенных в помощью элементарного анализа данных. Полученные шаблоны являются популяцией генетического алгоритма, а функция приспособленности (fitnessfunction) вычисляется на сохраненных последовательностях текущих событий и отражает, насколько часто встречается предложенный шаблон поведения в рассматриваемой последовательности. Таким образом, она отражает степень пригодности того или иного шаблона в данных условиях.

Так же было отмечено, что управлением встроенными системами занимается человек, который по природе своей непостоянен и чьи потребности и привычки со временем могут меняться в связи с внешними факторами, не доступными системе для анализа. По этой причине так же необходимо найти периодичность, с которой стоит запускать в системе поиск шаблонов поведения.

Были определены дальнейшие направления исследования:

- изучить существующие методы анализа данных, моделирования сложных систем и машинного обучения;
- найти примеры взаимодействия систем для последующего моделирования;
- создать виртуальную модель совокупности изученных встроенных систем и их взаимодействия;
- на созданной виртуальной модели разработать методы поиска закономерностей в поведении встроенных систем;
- изменить поведение виртуальной модели и проверить разработанные методы;
- определить период поиска новых шаблонов в связи с изменчивостью пользователя.

Таким образом, в работе был выбран метод построения шаблонов, взаимодействия встроенных систем, определены пути его проверки и дальнейшее направление исследований.

Литература

1. Парфенов В.Г., Муромцев Д.И., Елизаров Р.А., Попов С.О. Сбор, передача, хранение и распространение данных с различных приборов учета // Проект научно-технического исследования НИУ ИТМО. – 2012.
2. Prof. dr. ir. F. Gielen, Jelle Nelis, Pieter-Jan Maenhaut. Self-Learning Smart Home Control. University of Ghent – Department of Engineering. Project as part of the course Software Architecture. – 2011–2012.
3. Егоров К., Чураков М. Генетические алгоритмы [Электронный ресурс]. – Режим доступа: <http://logic.pdmi.ras.ru/~yura/internet/03ia-seminar-note.doc>, свобод.

ИНТЕГРАЦИЯ РЕЛЯЦИОННЫХ БАЗ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ RDF\OWL**И.А. Семерханов, Г.В. Варгин****Научный руководитель – к.т.н., доцент Д.И. Муромцев**

Проблема интероперабельности сложных компьютерных систем известна уже давно. Она обуславливается тем, что компьютерные системы в большинстве случаев являются распределенным, т.е. физически удаленны друг от друга. Помимо этого, различные информационные системы строятся на различных технологиях, с применением разных типов баз данных. Кроме того, чаще всего информационные системы проектируются для работы независимо от других систем. Все эти факторы препятствуют построению единого унифицированного хранилища данных.

Один из методов решения проблемы интеграции различных баз данных заключается в использовании метаданных описанных в формате RDF\OWL для обеспечения семантической интероперабельности. ResourceDescriptionFramework (RDF) была разработана для решения задач, связанных с описанием семантики. Основополагающим для RDF является понятие модели данных. Это есть набор фактов и семантических связей между ними. RDF представляет собой абстрактную модель, обеспечивающую способ разбиения знаний на дискретные части. Утверждение, высказываемое о ресурсе, имеет вид «субъект-предикат-объект» и называется триплетом. Множество RDF-утверждений образует ориентированный граф, в котором вершинами являются субъекты и объекты, а ребра помечены предикатами. OWL в свою очередь, является языком описания, позволяющим описывать классы и отношения между ними, присущие веб-документам и приложениям. Онтологии на базе OWL гораздо мощнее и гибче, нежели схемы баз данных. В основном схемы баз данных лишь определяют те виды информации, которые могут быть связаны с объектами (или кортежами), принадлежащими какому-либо классу (или таблице). В OWL-онтологиях классы могут предназначаться для аналогичных целей, однако они также могут содержать условия по распознаванию, поэтому явная типизация в OWL необязательна.

Извлекая структуру реляционных баз данных и трансформируя ее в формат RDF и OWL можно получить средство для построения связей между объектами баз данных, вне зависимости от их типа. Глобальная онтология, созданная из нескольких метописаний структур разных баз данных, позволяет описать всевозможные связи между объектами баз. Такая структура дает возможность извлекать информацию сразу из нескольких источников данных, при помощи языка запросов к данным, представленным по модели RDF, SPARQL.

Для извлечения структуры базы данных можно использовать библиотеку D2RQ, которая при помощи jdbc адаптера для выбранного типа базы данных, будет генерировать из схемы RDF файл в формате Turtle с описанием базы. D2RQ использует свой собственный язык описания для мапинга схем в RDF словари и OWL онтологии. Основными объектами в мапинг файле являются d2rq:ClassMap и d2rq:PropertyBridge. d2rq:ClassMap соответствует таблице, а d2rq:PropertyBridge полю в таблице, в реляционной базе данных.

Объединив несколько таких файлов из разных систем в один, можно получить общий мапинг файл для интеграции баз данных. Применяв XSLT преобразования на такой файл, можно привести его к формату OWL. Полученную онтологию легко редактировать при помощи различных инструментов для работы с онтологиями, например SWOOP. При редактировании, объекты в разных базах привязывают друг к другу, помимо этого им прописываются свойства из онтологий общего пользования, таких как DublinCore, FOAF.

Библиотека D2RQ на основе созданной онтологии способна преобразовывать запросы на языке SPARQL в запросы на языке SQL, направляя их в нужную систему и хранилище данных. Таким образом можно получить механизм для доступа к данным, хранящимся в базах данных различного типа, при помощи языка SPARQL.

Данный метод подразумевает большое количество ручных действий со стороны эксперта по онтологиям, что не всегда возможно в реальных условиях. В связи с этим в данный момент в НИУ ИТМО идет работа по созданию автоматизированных средств для реализации выше изложенного метода.

УДК 004

УНИВЕРСАЛЬНЫЙ МЕТОД ОЦЕНКИ РИСКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.Н. Созинова

Научный руководитель – к.т.н., доцент Г.П. Жигулин

Деятельность любой современной компании или организации невозможно представить без использования информации и информационных технологий. Информация стала одним из важнейших активов, находящихся в распоряжении компаний. Все это порождает новый, принципиально отличающийся от привычных финансовых, юридических и других – класс рисков нарушения информационной безопасности.

Процесс оценки рисков – это инструмент, с помощью которого можно определить цели управления ИБ, оценить основные критические факторы, негативно влияющие на ключевые бизнес-процессы компании, и выработать осознанные, эффективные и обоснованные решения для их контроля или минимизации. На данный момент тема комплексной оценки рисков в области информационной безопасности очень актуальна.

На сегодняшний день существует немалое количество методик оценки рисков нарушения информационной безопасности. Это, к примеру, OCTAVE, CRAMM, RiskWatch, ГРИФ, отраслевая методика Банка России РС БР ИББС 2.2. Но при детальном анализе данных методик можно выделить ряд недостатков, которые, являются существенными. Например: некоторые методики устарели, являются узконаправленными, не производят комплексную оценку и в применении очень сложные. На основании данного анализа и учитывая недостатки методик, можно создать «свой» метод оценки рисков нарушения информационной безопасности.

Цель работы – создать универсальный метод оценки рисков в области информационной безопасности, учитывая изменения в законодательстве и в самой области ИБ и ИТ. А так же сделать метод комплексным и удобным в применении для различных сфер деятельности.

Основные этапы оценки рисков:

Этап 1: определение характеристик организации или системы;

Этап 2: определение входных (ключевых) параметров;

Этап 3: составление модели нарушителя;

Этап 4: определение уязвимостей;

Этап 5: составление модели угроз;

Этап 6: анализ применяемых мер безопасности;

Этап 7: расчет уровня защищенности активов;

Этап 8: расчет вероятности возникновения угрозы;

Этап 9: анализ и расчет реализуемости угрозы;

Этап 10: определение ущерба;

Этап 11: определение актуальности угрозы;

Этап 12: оценка риска;

Этап 13: разработка рекомендаций;

Этап 14: документирование результатов и составление отчета.

Грамотный анализ и учет существующих угроз и уязвимостей информационной

системы и выполненный на этой основе анализ рисков закладывают основу для выбора политики безопасности при минимальных затратах.

Достоинства созданной методики: сочетание количественной и качественной оценки; учитываются организационные и административные факторы информационной и физической безопасности; данная методика является универсальной и подходит для больших, и мелких организаций как государственного, так и коммерческого сектора; позволяет давать конкретные рекомендации; простота методики, позволяет самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе и эффективность существующей системы защиты информации; может использоваться на всех стадиях проведения аудита информационной безопасности; учитывает соотношения ущерба и риска; выявляет недостатки существующей политики безопасности

Полученный метод оценки рисков в области информационной безопасности является универсальным и может найти широкое практическое применение:

- в образовании при подготовке и повышении квалификации специалистов в области ИБ;
- в организациях в качестве основной, дополнительной или промежуточной оценки рисков;
- на основе данного метода можно создать экспертную систему.

УДК 336.1.07

МОДЕЛЬ УГРОЗ ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКОГО ОБЪЕКТА НА ПРИМЕРЕ КРЕДИТНО-ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Е.А. Сорокина

Научный руководитель – к.т.н., доцент Г.П. Жигулин

Краткое вступление, постановка проблемы. Финансово-кредитная организация – неотъемлемый элемент экономической системы страны, обеспечение безопасности которой носит приоритетный характер. Один из аспектов безопасности – обеспечение технической безопасности организации.

Цель работы – анализ существующей ситуации в области обеспечения технической безопасности финансово-кредитной организации, построение и описания схем взаимодействия организации и специализированных контрагентов, обеспечивающих техническую безопасность, построение модели злоумышленника, рассмотрение возможных уязвимостей в технической защите, построение модели угроз технической безопасности.

Описание ситуации в предметной области. В процессе осуществления своей деятельности в кредитных организациях протекают определенные информационные процессы, осуществление которых позволяет говорить о финансово-кредитных учреждениях как о полноценных информационных системах. Целью злоумышленника также являются физические носители данных (важный источник информации о внутренней и внешней деятельности учреждения), находящиеся в архивах/хранилищах и других помещениях организации.

Основной результат, практические результаты. В ходе работы были построены: схема взаимодействия кредитной организации и частного охранного предприятия, модель злоумышленника, модель проникновения злоумышленника в здание организации-цели для получения доступа к данным, располагающимся на физических носителях, рассмотрены различные варианты развития события, затрагивающие как преднамеренное, заранее подготовленное и спланированное действие, совершенное злоумышленником для осуществления проникновения, плохо подготовленное заранее, но с некоторой вероятностью

успешное проникновение из-за трудно учитываемых внешних факторов, способное нанести ощутимый вред организации-цели, так и проникновение, которое может стать возможным по вине непосредственно самой кредитной организации, выступающей в качестве заказчика работ/услуг.

Вывод. В результате проведенной работы касательно построения моделей и рассмотрения возможных уязвимостей в технической защите финансово-кредитной организации в целом были намечены дальнейшие проблемы для исследования данной тематики ввиду характерной для нынешнего времени возрастающей доступности технологий и, как следствие, снижения стоимости осуществления атак на информационные ресурсы, в том числе и кредитных организаций, а также возрастающей стоимости обеспечения безопасности. Важность данного направления исследований заключается в предотвращении вреда, который злоумышленник может нанести безопасности финансовой системы в лице достаточно крупной кредитной организации и/или нескольких средних, что, в свою очередь, может оказаться вполне ощутимым для всей экономики страны.

УДК 681.5.011

ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ ПРИНЯТИЯ РЕШЕНИЙ В САПР РАЗЛИЧНЫХ НАПРАВЛЕНИЙ

Е.Ю. Трофимова

Научный руководитель – к.т.н., доцент И.Б. Бондаренко

Автоматизация проектирования осуществляется системами автоматизированного проектирования (САПР). Принято выделять в САПР машиностроительных отраслей промышленности системы функционального, конструкторского и технологического проектирования [1].

Очевидно, что на все сто процентов автоматизировать процесс проектирования невозможно, а это значит, что последнее слово всегда остается за человеком. Он принимает основные проектные решения и несет за них полную ответственность. Поэтому проектировщику должен быть обеспечен полный доступ к промежуточным результатам инженерных вычислений. Их оценка способствует принятию эффективных решений, помогает находить ошибки в исходных данных, проверять достоверность полученных результатов. При этом необходимо учитывать требования наглядности, легкости восприятия, компактности представления информации, удобства и простоты ее корректировки.

К сожалению, те, кто больше всего нуждается в этой ценной информации, как правило, не могут ее получить. Для вычислений и их документирования проектировщику зачастую приходится использовать разнородный набор программных средств. Соответственно техническая информация, рассредоточена и ни о какой согласованности в данных, говорить не приходится. В лучшем случае разработчики пытаются объединить модули с помощью промежуточных файлов и специальных средств синхронизации. Но даже когда появляется некое подобие единой среды проектирования, такие комплексы обычно имеют «вход» для ввода информации и «выход» для отображения результатов, а механизм работы малопонятен и к тому же скрыт в компьютерном коде или ячейках различных таблиц.

Таким образом, современные САПР должны быть основаны на следующих принципах:

- ориентация на инженерно-технические работы с учетом отечественных методик;
- работа с единой моделью объекта;
- работа в трехмерном пространстве;
- интерактивность технологии проектирования;
- расчеты в реальном времени;

- интуитивно понятный интерфейс;
- комплексность представления информации;
- тотальный контроль качества.

Это позволит создать эффективную и высоко интуитивную инженерную среду, которая предоставит проектировщику возможность быстро осуществлять анализ исходных данных, выбирать методику проектирования, производить требуемые инженерные вычисления, обосновывать принятые допущения, а также обмениваться этой информацией.

Работа с единой моделью объекта подразумевает, что любое редактирование с помощью любого инструмента прямо влияет на состояние модели и мгновенно обновляет все представления информации. Поэтому в любой момент можно быть уверенным в согласованности данных во всех подсистемах [2].

Использование компьютеров для генерации программных средств носит название CASE-технологии (Computer-Aided Software/System Engineering). В широком смысле CASE-технология представляет собой совокупность методологий анализа, проектирования, разработки и сопровождения сложных систем программного обеспечения (ПО), поддержанную комплексом взаимосвязанных средств автоматизации.

Большинство CASE-средств основано на парадигме методология/метод/нотация/средство. Эти инструменты поддерживают работу пользователей при создании и редактировании проекта в интерактивном режиме, они способствуют организации проекта в виде иерархии уровней абстракции, осуществляют генерацию ПО и используются при его тестировании [3].

Основной целью создания интеллектуальных САПР является простота и удобство представления знаний для структурного и параметрического синтеза [4].

Инженерные вычисления используются для прогнозирования поведения конструкции еще на стадии разработки, их результаты часто задают критические параметры и размеры промышленной модели. Вычисления являются ядром технической информации. Разнообразие представления этих данных позволяет «на лету» выполнять качественный и глубокий инженерный анализ. Значительно упрощается выпуск документации, существенно сокращается число ошибок проектирования, а 3D-модель обеспечивает возможность убедиться, что разработанный проект адекватно отражает принятые проектные решения.

Все это существенно повышает уровень проверки, сертификации, публикации и совместной работы на всех этапах разработки [2]. Таким образом, простота освоения интерактивных инструментов современных САПР, надежность методов, скорость работы их алгоритмов позволяют в кратчайшие сроки создавать очень сложные и насыщенные проекты.

Литература

1. Норенков И.П. Основы автоматизированного проектирования. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – 336 с.
2. Карпов М., Воробьев С. Организация инженерных вычислений в среде проектирования ModelStudio CS // САПР и графика. – 2010. – № 12. – С. 36–42.
3. Евгеньев Г. САПР XXI века: персональному компьютеру персональное программное обеспечение // САПР и графика. – 2000. – № 2.
4. Евгеньев Г., Кузьмин Б., Лебедев С., Тагиев Д. САПР XXI века: интеллектуальная автоматизация проектирования технологических процессов // САПР и графика. – 2000. – №4.

РАЗРАБОТКА ТРЕБОВАНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

Ю.Г. Филиппова, Н.А. Дородников, А.В. Евлахова, Е.А. Златина
Научный руководитель – к.т.н., доцент А.А. Малинин

С приходом информационных технологий в здравоохранение стала актуальна проблема защиты медицинской информации и персональных данных (ПДн) пациентов. Распространение Интернета расширило круг субъектов, имеющих допуск к личной информации медицинского характера, и создало условия для возможности злоупотребление полученными сведениями.

В России был принят ряд законодательных актов защиты ПДн пациента, ограничивающий ее использование и доступ к медицинской информации. основополагающими законами в этой сфере являются Федеральные от 27.07.2006 № 152-ФЗ «О персональных данных» и от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», которые предъявляют жесткие требования к порядку получения, хранению и защите, использованию, и уничтожению информации, содержащей личные данные о пациентах, и предусматривают ответственность за нарушение этих требований.

Главные проблемы, ограничивающие ведение истории болезни пациента в электронном виде, – это сложность разграничения доступа к информации, обеспечения неизменяемости записей, легитимность записей (кто, что и когда записал) и защищенность от утечек информации.

В работе проведен анализ требований для обеспечения безопасности ПДн, предъявляемых нормативными документами к МИС.

Целью работы является выявление требований безопасности ПДн для разработки защищенной автоматизированной МИС. Выявить, какие задачи предстоит решить при разработке МИС для удовлетворения требований российских нормативных документов.

Многие вопросы разработки и эксплуатации МИС уже отражены в приведенных выше документах (№ 152-ФЗ «О персональных данных» и ГОСТ Р 52636) и соответствующих национальных и отраслевых стандартах – Национальный стандарт «Электронная история болезни», регламентирующих работу МИС, также существует Федеральный закон №323 «Об основах охраны здоровья граждан в Российской Федерации» (статья 13 «Соблюдение врачебной тайны»), в которых указаны дополнительные требования к сохранности медицинский данных.

Существуют предложенные иностранными коллегами варианты решения задачи защиты данных в подобных системах, которые можно применить в российских реалиях с некоторыми доработками. Архитектура системы играет важную роль в ее развитии, и коллеги предложили подход к повышению безопасности системы клиент-серверной архитектуры для ее развития. После применения этого подхода, удовлетворение требований безопасности в архитектуре можно проверить программным обеспечением и достаточно быстро получить отчет.

Практические результаты. При функционировании МИС информационная безопасность данных обеспечивается специальными программными средствами – подсистемой информационной безопасности.

Основная функциональность:

- организация санкционированного доступа к данным;
- мониторинг «опасных» событий;

- управление свойствами пользователя МИС;
- ведение журналов безопасности.

Требования к медицинским информационным системам:

- полнота данных;
- возможность доступа со стороны пациента и медицинского персонала;
- неизменяемость записей для защиты от фальсификации;
- логирование доступа к записям;
- возможность удаленного доступа;
- предоставление данных для отчетов;
- доступность для проведения экспертизы.

Существующие нормативные документы влияют на разрабатываемую систему уже на этапе проектирования: сущности в системе должны коррелироваться с терминами, используемыми в законе и ГОСТе (персональная медицинская запись и т.п.).

УДК 621:004.896

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ПРОЦЕССОВ РЕЗАНИЯ

Алтунин К.А.

(Тамбовский государственный технический университет)

Научный руководитель – д.т.н. доцент М.В. Соколов

(Тамбовский государственный технический университет)

В настоящее время сокращение сроков проектирования и подбор оптимальных параметров процесса резания – это важнейшие требования, предъявляемые к разработке технологического процесса. Применение современной система автоматизированного проектирования (САПР) позволяет удовлетворить их лишь частично, так как в большинстве случаев технолог самостоятельно применяет решение о выборе тех или иных режимов резания, руководствуясь собственным опытом. Наличие САПР, предлагающей пользователю выбрать из списка возможных параметров процесса резания оптимальные при заданных условиях, позволило бы существенно повысить эффективность технологического процесса.

Такая САПР позволила бы технолог рассмотреть все доступные наборы параметров конкретного процесса резания, смоделировать этот процесс и, исходя из каких-либо конкретных ограничений, обусловленных данным производством, или из целей, которые должны быть достигнуты при осуществлении данного технологического процесса, выбрать его оптимальный в данных условиях вариант.

Таким образом, возникает потребность в разработке концепции создания САПР для оптимизации процесса резания, описать последовательность работы ее блоков и создать алгоритмы работы этих блоков.

В начале работы был выполнен обзор и анализ современного состояния методов математического моделирования и оптимизации процессов резания. Выявлены особенности построения математических моделей описания силовых и тепловых явлений при резании материалов. Обоснованы методы моделирования процессов резания с применением метода конечных элементов и определена применимость программных продуктов, реализующих данный метод. Рассмотрены подходы к оптимизации процессов резания, определены целевая функция и ограничения на ее значения. Результатом данного исследования стало создание следующего алгоритма оптимизации лезвийной обработки материалов.

1. Для обрабатываемой заготовки (известны размеры заготовки и конструкционный материал) назначаются материал и геометрические параметры режущего инструмента, а также режимы резания (глубина резания t , подача s и скорость резания v).

2. Рассчитываются параметры математической модели процесса резания, такие как: составляющие силы резания, длина контакта стружки с передней поверхностью режущего инструмента, температуры в зоне резания, а также тепловые потоки в системе заготовка – режущий инструмент – стружка.
3. Создается твердотельная модель режущего инструмента в одной из программ твердотельного моделирования. Используя, встроенные в программы твердотельного моделирования, CAE-модули, исследуется напряженно-деформированное состояние режущего инструмента. В результате проведения такого анализа могут быть получены распределения напряжений по телу инструмента и перемещения режущих кромок инструмента. По этим показателям делается вывод о допустимости принятых режимов резания в зависимости, например, от требуемых показателей к качеству изготавливаемой детали или жесткости системы станок-приспособление-инструмент-деталь (СПИД).
4. Исследуется динамика процесса резания на основе анализа передаточных функций, частотных характеристик (АФЧХ, АЧХ и т.д.), характеристических уравнений системы СПИД и производится оценка устойчивости процесса по различным критериям устойчивости (критерии Раусса, Гурвица, Найквиста, Михайлова) в зависимости от конкретного процесса резания.
5. Проводится выбор диапазона варьирования конструктивных и режимных параметров процесса резания.
6. Осуществляется постановка и решение задачи оптимизации конструктивных и режимных параметров процесса резания.

На основе данного алгоритма были созданы следующие блоки САПР для оптимизации процесса резания:

- блок задания исходных параметров, включающий в себя базу данных параметров процесса резания (таких как геометрические параметры режущего инструмента, теплофизические и физико-механические свойства обрабатываемого материала) и приложение, отвечающее за получение начальных данных, и переработку полученной информации;
- блок расчета параметров математической модели резания. Математическая модель процесса резания построена по блочному принципу. Она включает в себя блоки определения силовых и тепловых нагрузок, возникающих во время резания;
- блок анализа результатов моделирования нагрузок, действующих на режущий инструмент, осуществленного в программах твердотельного моделирования. Данный модуль исследует напряженно деформированное состояние режущего инструмента;
- блок исследования динамики процесса резания;
- блок расчета оптимальных параметров процесса резания.

Система построена на примере токарной обработки основных металлов и сплавов, используемых в промышленности.

УДК 004.822

АРХИТЕКТУРА СЕМАНТИЧЕСКОГО ФРЕЙМВОРКА ДЛЯ ПРИЛОЖЕНИЙ В СФЕРЕ ЭЛЕКТРОННОГО ТУРИЗМА

Д.А. Замула

Научный руководитель – к.т.н., доцент Д.И. Муромцев

Сегодняшний этап развития туризма позволяет охарактеризовать его одним из самых прибыльных видов бизнеса. Его доля в мировой торговле услугами составляет более 30%. Ежегодный рост инвестиций в индустрию туризма составляет около 35%. Туризм использует до 7% мирового капитала. С ростом индустрии, отмечается рост продаж туристических

предложений через интернет. Уже на сегодняшний день, более 30% всех B2C транзакций в этой области проводятся через интернет. С увеличением масштабов индустрии, появляется требование обновления существующей инфраструктуры электронного туризма, для возможности реализации более интеллектуальных сервисов и обеспечения более широких возможностей, для пользователей в данной области.

На сегодняшний день, отсутствуют инструменты, покрывающие все требования конечных пользователей в едином информационном окружении. Существующие сервисы направлены на решение узкоспециализированных задач туризма (планирование маршрута, бронирование отелей, покупка билетов). Отсутствует возможность производить планирование поездки на основании предпочтений пользователя, выраженных в оценках уже проведенных путешествий.

Реализация систем электронного туризма следующего поколения позволит решать бизнес задачи не только туристов, но и компаний, работающих в данной отрасли. Например, появление более интеллектуальных средств агрегации билетов, позволит оптимизировать расходы туроператоров в данной области.

Конечная цель создания новых инструментов в сфере электронного туризма – освобождение пользователей от рутинных задач планирования путешествий, заключенных в необходимости ручного подбора услуг сторонних сервисов (продажа билетов, аренда жилья) по неким критериям, обеспечении согласованности данных услуг по времени, а также поиска потенциально полезной информации, связанной с путешествием.

Основные требования к фреймворку:

- возможность связывать данные из разных источников;
- производить логические выводы на основании существующих данных;
- реализовывать концепцию модульного приложения, упрощая разработку и подключение дополнительного функционала к уже существующей системе;
- предоставить возможность разработки различных клиентов (Web, мобильные приложения).

Для реализации описанного функционала предлагается использовать модель и технологии семантической сети. Данный подход позволяет реализовать функциональность связывания туристических данных. Важной составляющей является возможность произведения логических выводов на основе существующих данных.

Архитектура разрабатываемого фреймворка основывается на модели SOA (Service-oriented architecture), дополненной в соответствии со спецификой предметной области. Каждый компонент системы является независимым модулем, предоставляющим интерфейсы, для интеграции с другими компонентами посредством технологии веб-сервисов. Компоненты приложения могут быть физически распределены на различных вычислительных средах, что позволяет более гибко распределять нагрузку на систему в целом, а также способствует надежности системы.

С учетом использования семантической сети, данный подход трансформируется в SSOA (Semanticservice-oriented architecture). Таким образом, появляется возможность реализации сторонних агентов, работающих с определенным компонентом системы, и не затрагивающих всю систему в целом. При данном подходе упрощается интеграция с внешними системами за счет существования сервисов, покрывающих весь функционал представленного приложения.

Для многочисленных внутренних сервисов приложения необходимо использование большого количества внешних данных. При отсутствии у провайдера данных поддержки семантических данных существует возможность реализации дополнительного сервиса, который необходим для трансляции специфичного представления в семантическое.

Используемая архитектура не налагает ограничений на инфраструктурный уровень. В качестве вычислительных ресурсов может использоваться как единственный сервер, так и кластер (и его реализации, основанные на семантике – SemanticGrid).

В качестве реализации веб-сервисов предполагается использовать технологии WSDL-S,

и строить всю реализацию на протоколе SOAP. Данный протокол обеспечивает на зависимость от протоколов прикладного уровня, а также строго определяет существующие интерфейсы на программном уровне. В качестве фреймворков для поддержки данной функциональности могут быть использованы ApacheAxis, Metro, SpringWS. Для поддержки семантической составляющей, используются технологии RDF (ResourceDescriptionFramework), OWL (WebOntologyLanguage) и SPARQL.

В качестве основных онтологий, предполагается использование стандартов ОТА (OpenTravelAlliance). Онтологии будут расширяться, с учетом определения отдельных сервис-провайдеров.

В работе был рассмотрен семантический фреймворк, как основа для реализации систем электронного туризма следующего поколения. Были определены требования к данному программному каркасу относительно решаемых бизнес задач. В качестве основы архитектуры, был выбран подход SSOA, и описаны возможные варианты использования. В качестве реализации был предложен общий набор технологий, решающий конкретное архитектурное требование. На текущий момент, SSOA находится в фазе изучения, из чего следует необходимость в дополнительных практических исследованиях преимуществ данной технологии.

УДК 621.396

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ ОЦЕНКИ ИНТЕНСИВНОСТЕЙ ОТКАЗОВ ЭРИ

О.А. Кузнецова

(ФГУП СПб ОКБ «Электроавтоматика»; Санкт-Петербургский государственный университет информационных технологий, механики и оптики)

Научный руководитель – д.т.н., профессор Ю.А. Гатчин

(Санкт-Петербургский государственный университет информационных технологий, механики и оптики)

Краткое вступление, постановка проблемы. С появлением на российском рынке программных комплексов оценки надежности зарубежной разработки российским пользователям стали доступны методы прогнозирования надежности зарубежных стандартов (помимо MIL-HDBK-217F). При попытке применения отдельных зарубежных стандартов для прогнозирования интенсивностей отказов ЭРИ одного и того же типа результаты порой удивляют своей колоссальной разницей.

Цель работы. Для определения причин отличий результатов расчетов необходимо выполнить сравнительный анализ математических моделей оценки интенсивностей отказов из материалов отечественного Справочника «Надежность ЭРИ», MIL-HDBK-217F, международного стандарта IEC TR 62380 «Reliabilitydatahandbook – Universalmodelforreliabilitypredictionofelectronicscomponents, PCBsandequipment», в моделях которого учтены современные достижения технологии радиоэлектронных компонентов, и французского руководства FIDES 2009.

Базовые положения исследования. В соответствии со справочником «Надежность ЭРИ», расчетная интенсивность отказов отечественного элемента в конкретных условиях эксплуатации определяется как произведение исходной (базовой) интенсивности отказов ЭРИ и коэффициентов, учитывающих изменения интенсивности отказов изделий в зависимости от различных конструктивно-технологических и эксплуатационных факторов. Модели справочника MIL-HDBK-217F в целом аналогичны моделям отечественного

справочника с отличием для микросхем лишь в том, что исходные, аналогичные базовым интенсивностям отказов отечественного справочника, интенсивности применяются отдельно для кристалла и корпуса. Общая модель прогнозирования интенсивности отказов электрорадиоизделия по FIDES 2009 содержит физическую составляющую интенсивности отказов изделия и коэффициент, учитывающий влияние качества и технического контроля производства ЭРИ и процессов разработки, производства и эксплуатации изделия более высокого уровня, куда входит элемент. При этом физическая составляющая интенсивности отказов определяется как среднегодовое значение и учитывает длительности и интенсивности отказов во время различных фаз работы изделия (хранение, применение и т.п.). Модель оценки интенсивности отказов компонентов, предложенная стандартом IEC TR 62380, учитывает все фазы жизни изделия (хранения, включения на земле, работы в полете), на основе типового года эксплуатации.

Промежуточные результаты. Из представленных моделей следует, что:

- интенсивность отказов, полученная по Справочнику «Надежность ЭРИ» и MIL-HDBK-217F, представляет собой интенсивность отказа изделия на один час налета, так как учет наработки авионики в эксплуатации ведется по журналам, регистрирующим налеты,
- интенсивность отказа, вычисляемая по FIDES 2009 и IEC TR 62380, является интенсивностью отказов на один календарный час. Следует отметить, что в интенсивности отказов стандарта IEC TR 62380 и FIDES 2009 учтены отказы, связанные с пайкой и монтажом, что не включено в отечественный справочник и MIL-HDBK-217F.

Основной результат. Выполненный анализ выявил существенные отличия в моделях оценки интенсивностей отказов электрорадиоизделий и в результатах расчета по этим моделям. Основной причиной разнящихся расчетных значений является тот факт, что по моделям стандарта IEC TR 62380 и FIDES 2009 полученные значения интенсивностей имеют размерность [1/ календарный час], что не соответствует предъявляемым отечественными стандартами требованиям по средней наработке (среднему налету) на отказ и повреждение.

УДК 65.011.56

АВТОМАТИЗАЦИЯ ОПЕРАТИВНОГО ПРОИЗВОДСТВЕННОГО ПЛАНИРОВАНИЯ С УЧЕТОМ ЗАДАЧИ СНАБЖЕНИЯ ПРОИЗВОДСТВА СЫРЬЕМ И МАТЕРИАЛАМИ

Ю.Г. Мехова

Научный руководитель – к.ф.-м.н, доцент Д.А. Зубок

В сложившихся рыночных условиях происходит индивидуализация производства. Все большую значимость приобретает система планирования производства, причем в последнее время наблюдается смещение фокуса планирования на цеховой уровень.

Целью работы является формирование механизма оперативного планирования производства с учетом задачи снабжения производства сырьем и материалами.

Основными целями оперативного планирования являются: распределение работ по единицам оборудования, формирование последовательности выполнения заказов, определение точного времени начала выполнения операций. Ввиду динамического характера производственной среды оперативный план пересматривается достаточно часто, возможна его корректировка несколько раз в течение смены.

Для автоматизации оперативного производственного планирования могут использоваться MES-системы. Следует отметить, что «идеальный» вариант автоматизации планирования подразумевает применение на производственном предприятии целого ряда систем: ERP, APS и MES. Каждый класс систем автоматизирует определенный уровень

планирования: ERP – объемный, APS – календарный, MES – оперативный. Каждый последующий уровень планирования детализирует предыдущий.

Вопросы интеграции MES-систем с системами более высокого уровня рассмотрены в стандарте ISA-95. Стандарт содержит в себе 9 моделей («интерфейсов» между системами): модель персонала (Personnelmodel), модель оборудования (Equipmentmodel), модель материалов (Materialmodel), модель сегментов процесса (Processsegmentmodel), модель производственных мощностей (Productioncapabilitymodel), модель возможностей сегмента процесса (Processsegmentcapabilitymodel), модель определения продукции (Productdefinitioninformationmodel), модель производительности (Productionperformancemodel), модель расписания производства (Productionschedulemodel).

Определим модели, описывающие входные данные для построения оперативного плана. Рассмотрим модель расписания производства, представленную в стандарте ISA-95 в виде диаграммы классов.

Анализ модели позволяет установить, что данная модель основывается на других самостоятельных моделях: модели персонала, модели оборудования и модели материалов. Таким образом, для построения оперативного расписания в MES-систему должно передаваться либо готовое расписание, требующее детализации, либо сведения о ресурсах и сегментах процессов. Очевидно, источником уточняемого расписания для MES-системы должна служить APS-система, если же интеграция осуществляется между ERP и MES, то целесообразно передавать сведения о ресурсах для того, чтобы MES-система самостоятельно строила расписание с учетом всех ограничений.

Рассмотрев возможные варианты входных данных, остановимся подробнее на модели материалов. Данная модель содержит в себе информацию о группировке материала, определение свойств и характеристик материала, его запасах и текущем состоянии. Таким образом, при составлении и корректировке оперативного расписания как ограничения учитываются только запасы материала и его состояние.

Однако для предприятий с позаказной системой планирования характерным является осуществление закупок под конкретный заказ. В этом случае при включении заказа в оперативный план, а так же в ходе дальнейшей корректировки производственного расписания важен срок поставки материала: операция не может быть перенесена на некоторую дату, если период между текущей датой (датой корректировки) и планируемой датой осуществления операции меньше срока поставки.

Введение подобного ограничения возможно путем добавления нового атрибута «Срок поставки» классу «Подпартия материала» («Materialsublot»).

УДК 658.512:621.316.925.44

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРИ РЕШЕНИИ ЗАДАЧ ПРОЕКТИРОВАНИЯ СЕЛЬСКОХОЗЯЙСТВЕННОЙ ТЕХНИКИ

К.В. Немтинов

(Тамбовский государственный технический университет)

Научный руководитель – д.т.н., профессор С.Я. Егоров

(Тамбовский государственный технический университет)

В настоящее время в России вопросам развития сельского хозяйства уделяется большое внимание. Для повышения эффективности аграрно-продовольственной системы принят ряд серьезных мер, разработаны общие предложения по отдельным элементам государственного регулирования в аграрно-промышленном комплексе, которые должны заметно оздоровить обстановку в отрасли. Большую роль при этом играет разработка и внедрение в производство новых типов сельхозтехники, использование качественных удобрений, совершенствование

условий хранения зерна и т.п. В настоящее время решение этих и других задач практически невозможно выполнить без использования современных информационных технологий.

Анализ литературных источников, связанных с технологией проектирования сельскохозяйственной техники (на примере проектирования посевных комплексов) показал, что в большей степени, в них основное внимание уделяется вопросам конструкторской разработки отдельных сельскохозяйственных комплексов, и меньшей степени – выбору наиболее подходящей структурной схемы комплекса для конкретных исходных данных: типа почвы, вида посевного материала, технологии посева, тягового класса трактора и критериев, заданных потребителем.

В связи с этим **целью работы** является разработка процедуры автоматизированного проектирования сельскохозяйственной техники на примере посевного комплекса для зерновых культур в зависимости от вышеперечисленных требований.

В целом задача автоматизированного проектирования посевного комплекса для множества конкретных исходных данных: типа почвы, вида посевного материала, технологии посева, тягового класса трактора и критериев, заданных потребителем предусматривает: разработку структурной схемы узлов и механизмов, выбор типовых элементов, их компоновку, а также конструкторскую разработку оригинальных узлов и механизмов.

При такой постановке ее решение невозможно получить в связи с высокой размерностью пространства переменных для посевного комплекса, сложностью построения математических моделей поддержки принятия решений, конструкторских особенностей отдельных элементов комплекса и т.д. Поэтому процедура синтеза посевного комплекса состоит из последовательного рассмотрения трех подзадач меньшей размерности, имеющих, кроме того, самостоятельное значение в процессе проектирования:

- формирование вариантов структурной схемы комплекса и выбора оптимального варианта с позиций множества критериев;
- формирование множества вариантов типовых элементов и оптимального выбора варианта, удовлетворяющего их потребительско-эксплуатационным показателям;
- конструкторская разработка оригинальных узлов и механизмов.

В случае отсутствия решения на следующем этапе проектирования комплекса лицо, принимающее решение, выбирает другой вариант решения задачи предыдущего этапа.

Задача выбора структурной схемы узлов посевного комплекса из множества вариантов на основании математических критериев оптимальности решается, как правило, редко вследствие сложности накладываемых на комплекс условий, а также большого множества критериев оценки. Наиболее прогрессивным методом решения этой задачи является применение экспертных систем.

Используя опыт, накопленный при проектировании посевных комплексов в виде базы данных и задавая цель – например, высокое качество высева зерновых культур и обеспечение 100%-ой их всхожести, при помощи механизма принятия решения можно найти совокупность узлов комплекса, обеспечивающих достижение этой цели. В базе собраны правила, эмпирические знания и общие данные, которыми обладают специалисты.

В настоящее время база содержит более 100 продукционных правил, с помощью которых может быть сформирована оптимальная структурная схема посевного комплекса для конкретных исходных данных.

В качестве примера рассмотрим следующие продукционные правила определения типа дозирующего узла и транспортирующего устройства: если (рама=«цельная» и тип бункера=«общий»), то дозирующее устройство=«катушечное, количество=1»; если (рама=«цельная» и тип бункера=«раздельный для четырех высевающих аппаратов»), то дозирующее устройство=«катушечное, количество=4»; если (рама=«цельная» и тип бункера=«общий» и дозирующее устройство=«катушечное, количество=1»), то транспортирующее устройство «элеваторное ковшое» и т.п.

Комбинируя несколько вариантов структурных схем конструкций узлов посевного

комплекса, обладающих разной эффективностью, формируют целостную конструкцию посевного комплекса. Поскольку размерность множества комбинаций не превышает 10^3 , учитывая быстрое действие современных персональных компьютеров, решение сводится к последовательному перебору всех возможных комбинаций схем.

Следующим этапом процедуры автоматизированного проектирования посевного комплекса для зерновых культур является выбор типовых узлов и механизмов, выпускаемых промышленностью и их предварительное распределение в общей конструкции посевного комплекса. Большинство элементов посевного комплекса имеет стандартизованный типоразмер (например, дисковые ножи, сошники, анкерные и чизельные сошники и т.д.). Зерновые бункера, прикапывающие устройства выпускаются заводами – изготовителями по индивидуальному заказу.

Вследствие значительного количества критериев оценки (более 10–15, например, ремонтпригодность, простота в обслуживании, высокий КПД и т.п.), которые могут быть использованы конструктором при выборе детали или узла, авторами предложена процедурная модель автоматизированного выбора детали или узла, характеризующихся наилучшими заданными потребительскими показателями для каждого конкретного случая.

Следующим этапом процедуры автоматизированного проектирования посевного комплекса для зерновых культур является конструкционная разработка оригинальных узлов и механизмов, окончательная компоновка всего посевного комплекса, а также создание конструкторской документации (чертежей, эскизов, расчетов и т.д.).

Апробация процедуры автоматизированного проектирования посевного комплекса осуществлена при проектировании комплекса для зерновых культур.

Среди достоинств разработанной конструкции посевного комплекса следует отметить: сокращение сроков посевных работ – нет разрыва между подготовкой и самим посевом; укладка семян на наиболее оптимальную глубину заделки семян, где формируется точка росы, сохранение исходных состояний капилляров, сохраняя природный подвод влаги из земли; применение современных высоконадежных подшипников и уменьшение вдвое их количества по сравнению с аналогами и др.

Предложенная в настоящей работе процедура автоматизированного проектирования посевных комплексов для зерновых культур с использованием теории построения экспертных систем позволяет в условиях большой размерности возможных вариантов выбрать оптимальный вариант совокупности узлов и механизмов комплекса для заданного ассортимента зерновых культур, климатических и почвенных условий и критериев, заданных потребителем, а также реализовать его конструкторское решение.

УДК 004.822

МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТ ДЛЯ ВИЗУАЛИЗАЦИИ НОМЕНКЛАТУРЫ ДЕЛ

В.С. Солодкова

Научный руководитель – к.т.н., доцент Г.П. Жигулин

На сегодняшний день, сложно себе представить нормальный документооборот в любой организации без ведения номенклатуры дел. Благодаря ведению номенклатуры систематизировать всевозможные документы в дела, вести общий учет дел и находить необходимые бумаги очень просто.

Существующие подходы для ведения и визуализации номенклатуры дел создают трудности по работе с номенклатурой дел на предприятиях с большим потоком документов и не всегда используют возможности современного аппаратного обеспечения – например, мониторов с высоким разрешением.

Модели интеллектуальных карт для визуализации номенклатуры дел помогут решить задачи информационной безопасности и сделать работу с номенклатурой дел более эффективной.

При разработке таких моделей были применены интеллектуальные карты и диаграмма вариантов использования. Интеллектуальные карты – это способ изображения процесса системного мышления с помощью схем. Они реализуются в виде древовидной схемы. Их можно создавать вручную, но процесс может быть поддержан специализированным программным обеспечением. Для работы с интеллектуальными картами была использована программа FreeMind, так как она имеет наименьшее количество недостатков. А также в ней можно добавлять атрибуты и защищенные узлы.

Для того чтобы более точно понять как должна работать система, используется описание функциональности системы через варианты использования (UseCase). При разработке алгоритмов системы визуализации номенклатуры дел с применением интеллектуальных карт пользователей нужно разделить на типы, и для каждого типа пользователя определить действия, которые они могут выполнять в системе. Так как дела имеют разные режимы секретности, то пользователей можно разделить на группы: пользователи, которые имеют допуск и которым разрешен доступ к конфиденциальной информации и пользователи, которые не могут работать с этой информацией. Также действия над делами разделяются на два типа: просмотр и редактирование. Редактированием могут заниматься только те пользователи, которые являются сотрудниками отдела делопроизводства. А просмотр могут совершать все пользователи системы.

При визуализации номенклатуры дел центральным объектом будет «номенклатура дел». Дальше в виде дерева от него будут отходить ветви – подразделения предприятия. Потом для простоты использования номенклатуры можно разделить на отделы. У каждого подразделения и отдела есть свой индекс. От подразделения или отделения отходят ветви с названием дела. Каждое дело отличается сроком хранения. Также дела отличаются грифом секретности. Для отображения индекса, срока хранения и грифа секретности дела применяются соответствующие атрибуты. Для обеспечения безопасности конфиденциальной информации можно защитить отдельную ветвь номенклатуры паролем. С помощью диаграммы вариантов использования получаем разграничение доступа. Пользователи, которые имеют допуск и которым разрешен доступ к конфиденциальной информации, могут выполнять действия над делами разных режимов. А пользователи, которые не имеют допуск или доступ к конфиденциальным документам могут выполнять действия только над делами без грифа «конфиденциально». Редактированием могут заниматься только те пользователи, которые являются сотрудниками отдела делопроизводства. В редактирование включается удаление, добавление и изменение дел. А просмотр могут совершать все пользователи системы.

Таким образом, были разработаны модели интеллектуальных карт для визуализации номенклатуры дел. Использование интеллектуальных карт повышает наглядность, уменьшает время поиска и доступа к делам, позволяет эффективно унифицировать данные в полном объеме и систематизировать номенклатуру. Это позволяет улучшить работу с номенклатурой дел на предприятиях с большим потоком документов.