Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Московский государственный технический университет им. Н. Э. Баумана»
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Калужский филиал МГТУ имени Н. Э. Баумана»

НАУКОЕМКИЕ ТЕХНОЛОГИИ В ПРИБОРО - И МАШИНОСТРОЕНИИ И РАЗВИТИЕ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ВУЗЕ

Материалы
Всероссийской научно-технической конференции

Том 3

ИЗДАТЕЛЬСТВО МГТУ им. Н. Э. Баумана
Калуга 2015

УДК 378:001.891
ББК 74.58:72
Н34

Н34 **Наукоемкие** технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе: материалы Всероссийской научно-технической конференции, 24–26 ноября 2015 г. Т. 3. – Калуга: Издательство МГТУ им. Н. Э. Баумана, 2015. – 280 с.

В сборнике материалов Всероссийской научно-технической конференции представлены результаты научных исследований, выполненных учеными в течение ряда лет. Систематизированы материалы различных научных школ. Результатами научных исследований являются новые методы, вносящие вклад в развитие теории, а также прикладные задачи, воплощенные в конструкции и материалы.

УДК 378:001.891
ББК 74.58:72

СЕКЦИЯ 10.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Е.М.Аксютина, Ю.С. Белов

BIG DATA В БИОИНФОРМАТИКЕ: ТИПЫ ДАННЫХ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Введение. Объём данных, получаемый при проведении современных исследований в биоинформатике, быстро увеличивается. Источники больших данных больше не ограничиваются экспериментами с физическими частицами или журналированием и построением индексов поисковых систем. С оцифровыванием всех процессов и доступностью устройств с большой пропускной способностью по низкой цене, объём данных увеличился везде, включая исследования в биоинформатике. Например, размер одной последовательности генома человека составляет практически 200 гигабайт [1]. Тенденция увеличения объёмов данных поддерживается снижением стоимости компьютеров и увеличением пропускной способности развивающихся технологий больших данных. Биологи больше не используют обычные лаборатории для открытия новых биомаркеров заболеваний, вместо этого они опираются на огромные и непрерывно растущие геномные данные, предоставленные различными исследовательскими группами. Технологии для получения биоданных становятся более дешёвыми и более эффективными, как, например, программа автоматического упорядочивания геномов, давшая рассвет новой эре больших данных в биоинформатике.

Проблемы больших данных в биоинформатике отличаются от других хорошо известных проблем, связанных с большими данными. Различия, главным образом, заключаются в двух аспектах. Во-первых, данные в биоинформатике неоднородны по своей природе. Кроме того, данные в биоинформатике производятся множеством бесконтрольных организаций и, как следствие, одни и те же типы данных представляются в разных формах.

Типы данных в биоинформатике. Прежде всего, существует пять типов данных, используемых в исследованиях по биоинформатике:

— данные, описывающие гены[2]
— ДНК, РНК и данные белковых последовательностей[3]
— данные о взаимодействии протеин-протеин (protein-protein interaction PPI)[4]
— данные pathway анализа[5]
— генная онтология[6]

Другие типы данных, такие как сеть заболеваний человека и объединённая сеть генов заболеваний так же используются и очень важны для множества направлений исследований, включая диагностику заболеваний (Рис.1) [7].

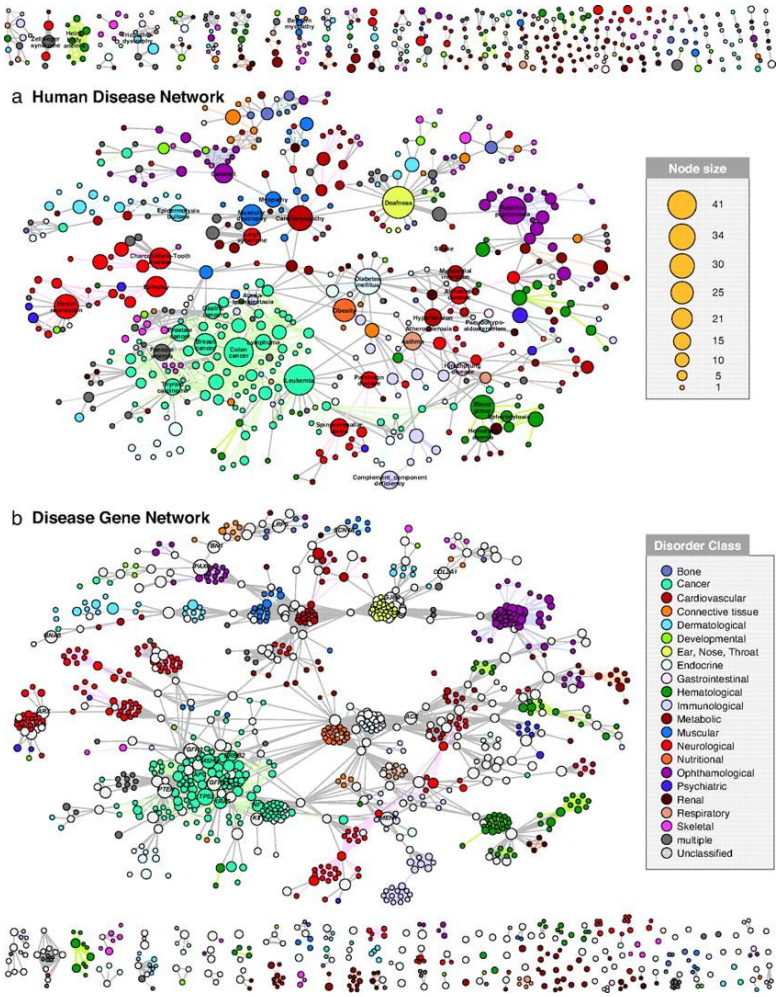


Рис.1. Графы сетей заболеваний человека и генов заболеваний

Данные, описывающие гены. При анализе аннотаций генов, уровни описания тысяч генов исследуются в различных условиях, таких как отдельные этапы развития методов лечения или на разных стадиях заболевания. Запись генных выражений производится с помощью микрочипов. Биологическим микрочипом называют микромножество или матрицу с нанесенными молекулами белков, нуклеиновых кислот, биомакромолекул или биоструктур для одновременного проведения большого числа анализов в одном образце [8]. Анализ генных выражений может идентифицировать гены, пострадавшие от потогенов или вирусов, сравнивая значения выражений из инфицированных и не инфицированных клеток. Результаты анализа могут использоваться для выявления боимаркеров для диагностирования и профилактики заболеваний.

Последовательности ДНК, РНК и пептидов. В анализе ДНК, РНК или пептидов, последовательности обрабатываются с помощью различных аналитических методов, для понимания их характеристик, функций, структуры и эволюции. Последовательность ДНК используется для изучения геномов и фенотипов и определения потенциальных лекарств, идентификации микровидов, представленных в пробах окружающей среды. Хотя РНК последовательности в основном используются как альтернатива

микрочипов, они так же могут применяться для других целей, таких как определение мутаций, определение посттранскрипционных механизмов, обнаружения вирусов. Анализ последовательностей эффективнее, чем анализ микрочипов, так как данные последовательностей содержат более широкую информацию. Однако для обработки большого количества последовательностей, требуются более сложные аналитические инструменты и компьютерные структуры.

Взаимодействие протеин-протеин (protein-protein interaction PPI). Информация о белковых взаимодействиях очень важна для понимания большинства сложных молекулярных механизмов функционирования живых систем. Формирование и анализ PPI сетей могут дать правильное понимание о функциях белка. Аномальные PPI являются причиной многих заболеваний, таких как болезнь Альцгеймера или рак. PPI изучаются в различных областях: биоинформатике, биохимии, молекулярной динамике, и таким образом, приводят к большим объёмам разнородных данных о взаимодействии белков. Идентификация подобных белков представляет большой интерес, так как они могут рассматриваться как потенциальные мишени для создания новых типов лекарств, действующих через регуляцию PPI.

Данные pathway анализа. Pathway анализ полезен для понимания молекулярной основы заболеваний. Кроме того, pathway анализ идентифицирует гены и протеины, связанные с причинами возникновения заболеваний, помогает внедрить различную биологическую информацию и назначить функции генам.

Работа всех генов может быть классифицирована таким образом, что гены могут рассматриваться не сами по себе, а в контексте биологических процессов, за которые они отвечают, так гены можно разделить на ансамбли — внутриклеточные сигнальные пути.

Каждый сигнальный путь имеет сигнал на входе и действие, которое он запускает, на выходе. Например, на входе может быть связывание клетки с фактором роста или гормоном, а на выходе появляется изменение, например, в работе большого количества генов. Гены можно разложить на сигнальные пути, анализируя работу которых, можно гораздо более точно представить, что именно происходит в клетке, чем при анализе конкретных, индивидуальных, единичных генов.

Генная онтология. «Генная онтология» (англ. Gene Ontology или GO) — биоинформатический проект, посвященный созданию унифицированной терминологии для аннотации генов и генных продуктов всех биологических видов.

Базы данных генной онтологии содержат динамические структурированные и видонезависимые генные онтологии для связанных биологических процессов, клеточных компонентов, молекулярных функций. Генные онтологические базы данных используют управляемые словари, чтобы облегчить поиск на различных уровнях. Большое количество инструментов используют генные онтологические базы данных для исследований в области биоинформатики. Геномные онтологические базы данных широко используются для таких целей, как создание онтологий для анатомии, обработка данных аналитических результатов и разработки

временных графиков для моделирования организмов, человеческих заболеваний и среды для выращивания растений.

Выводы. Рассмотренные типы данных подтверждают тенденцию широкого применения больших данных в биоинформатике. Важность этих данных имеет первостепенное значение, так как они непосредственно связаны с событиями реальной жизни, такими как изменение окружающей среды, кибератаками, эпидемиями, а так же из-за того, что они генерируются и передаются в реальном времени. Как следствие, эти данные активно используются для принятия решений и интеллектуального управления.

Для эффективного использования больших данных необходимо решать проблемы их хранения, улучшать технологии анализа, создавать новые конфигурации компьютерных систем для эффективной обработки и проверки данных.

ЛИТЕРАТУРА

[1] R. J. Robison, «How big is the human genome?» URL: https://medium.com/precision-medicine/how-big-is-the-human-genome-90caa3409b0#.wev7gxi4z (дата обращения: 24.10.2015)

[2] Alvis Brazma, Jaak Vilo. Gene expression data analysis. *FEBS Letters*, 2000, vol. 480, no. 1, pp. 17-24. URL: http://www.febsletters.org/article/S0014-5793(00)01772-5/abstract (дата обращения: 24.10.2015)

[3] I.a. The DNA, RNA and Proteins. URL: http://www.bioinformatics.org/tutorial/1-1.html (дата обращения: 24.10.2015)

[4] Overview of Protein-Protein Interaction Analysis. URL: https://www.thermofisher.com/ru/ru/home/life-science/protein-biology/protein-iology-learning-center/protein-biology-resource-library/pierce-protein-methods/overview-protein-protein-interaction-analysis.html (дата обращения: 24.10.2015)

[5] Khatri P, Sirota M, Butte AJ (2012) Ten Years of Pathway Analysis: Current Approaches and Outstanding Challenges. *PLoS Comput Biol* 8(2): e1002375, doi:10.1371/journal.pcbi.1002375. URL: http://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1002375 (дата обращения: 24.10.2015)

[6] Plessis L, Skunca N, Dessimoz C «The what, where, how and why of gene ontology — a primer for bioinformaticians». *Brief Bioinform*, 2011, vol. 12, no. 6, 723–35

[7] Kwang-Il Goh, Michael E. Cusick, David Valle, Barton Childs, Marc Vidal, and Albert-La´ szlo´ Baraba´ si, «The human disease network». *PNAS*, 2007, vol. 104, no. 21, 8685–8690, doi:10.1073/pnas.0701361104

[8] Словарь нанотехнологических и связанных с нанотехнологиями терминов.URL: http://thesaurus.rusnano.com/wiki/article601?sphrase_id=31142 (дата обращения: 24.10.2015)

Аксютина Екатерина Михайловна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: aks.kate93@gmail.com

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

А.А. Карышев, А.А. Багдошвили

АВТОМАТИЗИРОВАННОЕ ПРОЕКТИРОВАНИЕ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ, ПРОБЛЕМЫ ПРОЕКТИРОВАНИЯ И ИЗГОТОВЛЕНИЯ ПРЕСС-ФОРМ, ИСПОЛЬЗУЕМЫХ ДЛЯ ЛИТЬЯ ПЛАСТМАССОВЫХ ИЗДЕЛИЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В современном производстве используется множество технологий при изготовлении различных изделий. Широкое распространение получили так называемые традиционные технологии (штамповка, обработка материалов резанием, прокатка, ковка и др.), кроме того, имеют место и новые технологии (высокоскоростное фрезерование, лазерная и плазменная резка, литье пластмасс в горячеканальные формы и др.)[1].

При рассмотрении *неавтоматизированной* подготовки производства, технологические процессы (ТП) проектируются в форме технологической документации. В свою очередь, использование *автоматизированных систем технологической подготовки производства* (АСТПП) предполагает создание общего описания технологических процессов в соответствующей базе данных (БД), а так же основной технической документации. В свою очередь, хранящиеся в БД ТП являются первоисточником информации для решения поставленных задач автоматизированного управления технологической подготовкой производства (АУТПП). Причем, разработка ТП осуществляется благодаря специальным системам автоматизированного проектирования ТП (САПР ТП). В условиях отсутствия автоматизации, проявляется низкая производительность ТПП. Особенно это относится к сложной оснастке, образующей форму и инструменту.

Пресс-форма — сложное устройство для получения изделий различной конфигурации из металлов, пластмасс, резины и других материалов под действием давления, создаваемого на литьевых машинах. Как правило, сложность и стоимость оснастки, сроки разработки и изготовления пресс-формы зависят от детали, которую необходимо произвести [2].

Рассмотрим, общие проблемы изготовления и проектирования пресс-форм, используемых для литья пластмассовых изделий. В приборостроении, к ним в первую очередь, относятся сборочные единицы многих приборов (корпусы и т.д.), а так же другие элементы (кнопки, переключатели и т.д.).

Сложность и стоимость пресс-формы зависят от большого числа факторов. В свою очередь, конструктор пресс-формы всячески пытается снизить ее стоимость уже, непосредственно, на этапе проектирования пресс-формы. Этот процесс происходит по нескольким направлениям:

— Необходимо принять решения, которые обеспечат технологичность изготовленной продукции.
— Необходимо принять решения, которые упростят конструкцию самой пресс-формы.

При разработке ТП изготовления пресс-формы в первую очередь принимаются решения, учитывающие наличие или отсутствие на предприятии технологического оборудования.

Основные проблемы проектирования пресс-форм в приборостроении могут состоять в следующем:

— Решение поставленных задач, связанных с обеспечением технологичности конструкции начинается на поздних этапах проектирования изделия, что, в свою очередь, приводит к большим изменениям в конструкторской документации (КД).
— Коммуникации, передача и обмен данными между сотрудниками и службами ТПП производится в основном на бумажных носителях, что, в свою очередь, приводит к серьезному замедлению всех процессов ТПП.
— Во многих случаях, процесс проектирования носит ручной характер, а применяемые инструменты автоматизации используются для решения лишь определенных задач, отсутствует полная комплексная АСТПП.
— В некоторых случаях, нет возможности эффективного взаимодействия с другими предприятиями.
— Возникают существенные ошибки при проектировании, что приводит к значительным временным и финансовым затратам на проведение соответствующих мер [3].

В результате затягиваются сроки запуска новых изделий в производство, неоправданно увеличиваются затраты, качество изделий заметно уступает конкурентам.

Таким образом, в следствии данных проблем, могут серьезно увеличиться как затраты, так и необходимое время для комплексного запуска новых изделий в целом, причем качество, изготавливаемых изделий может быть гораздо ниже, нежели у конкурентов.

С масштабным распространением персональных ЭВМ и их повсеместным внедрением стало возможным:

— обеспечение каждого сотрудника персональным автоматизированным рабочим местом;
— осуществление электронного обмена данными;
— организация единых БД;
— решение задач, требующих огромных вычислительных ресурсов;
— внедрение системы управления данными о продукции – *Product Data Management (PDM)*;
— внедрение системы управления жизненным циклом продукции – *Product Lifecycle Management (PLM)*;
— внедрение системы планирования ресурсов предприятия – *Enterprise Resource Planning (ERP)*;
— внедрение системы управления проектами – *Project Management (PM)*[4] и др.

К видам информации, используемой в АСТПП можно отнести:

— данные о деталях и сборочных единицах изделия;
— основная информация о ТП изготовления изделия;
— нормативно-справочная информация;
— планово-учетная информация.

Все это должно быть организовано в виде единой структурированной информационной модели, которая, в свою очередь, должна быть доступна для дальнейшего взаимодействия. Таким образом, должна быть организована *интегральная информационная система ТПП (рис. 1).*

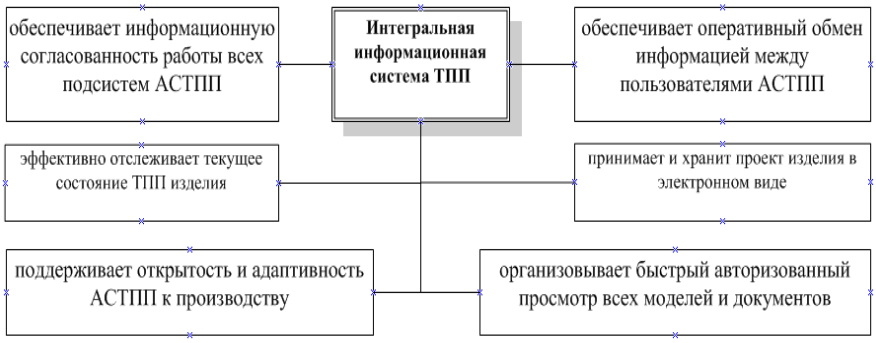


Рис. 1. Интегральная информационная система технологической подготовки производства

Следовательно, данные требования к интегральной информационной системе могут быть предоставлены только в том случае, если все процессы технологического и конструкторского проектирования в ТПП – автоматизированы. В информационную систему вся проектная информация поступает автоматически и становится доступной, в соответствии с имеющимися правами доступа, пользователям АСТПП [5].

Процесс создания АСТПП не может быть отделен от схожих мероприятий, связанных с техническим перевооружением производства. Процесс компьютеризации напрямую зависит от технологий и оборудования на предприятии.

Рассмотрим основной способ интегральной системы компьютеризации – создание *компьютерной базы знаний (КБЗ)* или *компьютерной модели*. В первую очередь, КБЗ – это средство формализации и накопления знаний о процессах проектирования и производства технологической оснастки в условиях развивающихся информационных технологий [6]. В общем случае, КБЗ представляется, как взаимосвязанная совокупность *символьной* и *графической информации* (рис. 2).

Рис. 2. Иерархическая структура компьютерной базы знаний

КБЗ содержит словарь понятий, факты (данные) о предметной области и правила, использующие эти данные как основу для принятия решений, она открыта для пополнения, что, несомненно, поощряет разработчиков к накапливанию и максимальному использованию проектного опыта той или иной организации.

В результате работы были рассмотрены, ключевые особенности автоматизированных систем технологической подготовки производства, возможные проблемы проектирования и изготовления пресс-форм, связанные, в том числе и с отсутствием соответствующей *интегральной информационной системы технологической подготовки производства*.

Исследована иерархическая структура базы знаний, представлена возможная схема переноса имеющейся информации о предприятии в бумажном формате в соответствующую компьютерную модель данных.

Список литературы

[1]. Валетов В.А., Мурашко В.А. Основы технологии приборостроения. – СПб, СПбГУ ИТМО, 2006, 180с.

[2]. Пресс-форма. URL: https://ru.wikipedia.org/wiki/Пресс-форма/ (дата обращения 14.10.2015).

[3]. Тюрина Л.А. Анализ и обработка информации для управления конструкторско-технологической подготовкой производства сложных промышленных изделий. Автореф. дис. канд. технич. наук. Пенза, 2005, 181 с.

[4]. Ширяев Н. PLM/PDM/ERP: реалии и перспективы. *САПР и графика*. *Сер. Машиностроение*, 2007, № 12, с. 16–20.

[5]. Яблочников Е.И. Автоматизация технологической подготовкипроизводства в приборостроении. СПб, СПбГИТМО (ТУ), 2002, 92 с.

[6]. Бирбраер Р., Бельцов В., инженерно-консалтинговая компания «Солвер». Автоматизация технологических процессов в условиях мелкосерийного многономенклатурного производства. *Умное производство*, 2015, вып. 31. URL: http://www.umpro.ru/index.php?page_id=17&art_id_1 =548&group_id_4=125 (дата обращения 15.10.2015).

Карышев Андрей Анатольевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ak9105252055@yandex.ru

Багдошвили Андрей Александрович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: ak9105252055@yandex.ru

К.Н. Солдатов, А.Е. Потапов

АДАПТАЦИЯ ВХОДНЫХ ТАБЛИЧНЫХ ДАННЫХ В ИС НА ПРИМЕРЕ ПЛАТЕЖНОЙ СИСТЕМЫ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Большинство людей в своей жизни пользуются услугами различных организаций (например, предоставляющих коммунальные услуги, мобильную связь, доступ в интернет и т.д.). Оплата этих услуг проводится по счетам и квитанциям, при этом поставщики услуг делегируют права приема денежных средств от населения третьим компаниям (агентам), имеющим разветвленную кассовую сеть и использующих специализированное ПО. Многие поставщики заботятся о минимизации ошибок, допускаемых кассирами при приеме платежа, предоставляя информацию о своей базе абонентов. Базы абонентов, как правило, содержат большой объем данных, касающийся платежных реквизитов.

Информацию о клиентах агент получает от организаций, предоставляющих услуги, в виде файлов данных, имеющих структуру, описанную в договоре. Как правило, эти входные файлы представляют собой табличные данные, хранящиеся как наборы строк, разделенные на столбцы. Каждая строка содержит информацию об одном клиенте, а столбцы делят ее на отдельные реквизиты. Выделяется два основных типа: DBF и CSV. DBF – формат хранения данных в виде электронной таблицы. В случае CSV для формирования столбцов используются символы-разделители, такие как запятая и тому подобные символы. Информация о клиентах для агента формируется с учетом внутренней организации хранения данных, используемой поставщиком услуг. Поэтому файлы могут иметь различные кодировки и структуры [1].

Для своевременной обработки огромного объема поступающей информации используются автоматизированные информационные системы, каждая имеет свою структуру в зависимости от деятельности и внутреннего устройства организации. Это означает, что структура БД платежной системы агента может не совпадать со всеми структурами автоматизированных систем, генерирующих файлы с клиентскими данными. В связи с этим возникает проблема сопоставление структуры поступающих данных и структуры хранения информации в БД системы.

Платежная система имеет собственную базу данных, в которой хранятся клиентские данные. При проведении платежей, клиентское приложение запрашивает информацию о клиентах из базы данных системы. Общая структура системы изображена на рисунке 1.

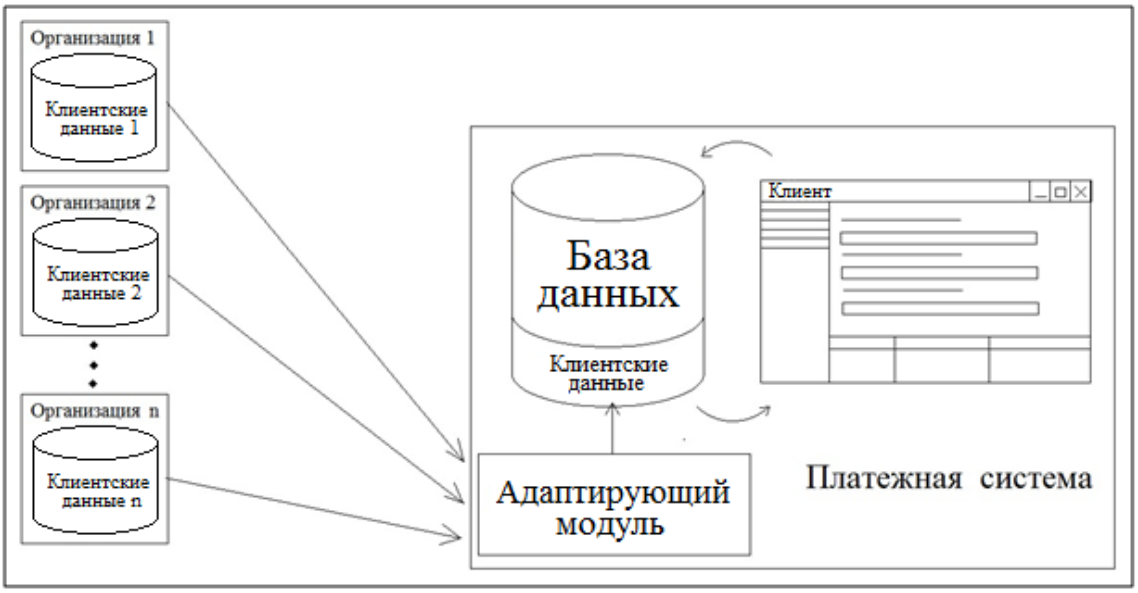


Рис. 1. Общая структура системы

Клиентские данные хранятся в двух таблицах: ClientDataRecord и ClientDataParameter. Первая из них содержит записи, каждая из которых относится к одному конкретному клиенту, а вторая - параметры всех клиентов. Таблицы имеют между собой связь «один ко многим», это означает, что одной записи в таблице ClientDataRecord может соответствовать несколько записей из таблицы ClientDataParameter (см. рисунок 2). Данный вид наиболее оптимален для хранения данных в реляционной базе данных [2].

Рис. 2. Структура данных БД системы

Для устойчивого функционирования необходимо, что бы система была способна корректно воспринимать поступающие в нее разнородные данные. Для этого можно использовать программу с гибкими настройками, адаптирующую входные данные всех типов к виду, пригодному для использования платежной системой.

Разработанный адаптирующий модуль удовлетворяет поставленным требованиям и позволяет хранить и использовать индивидуальные настройки для файлов каждой организации. В процессе разбора файла в

программе формируется двумерная таблица, после чего она разбивается на две таблицы, соответствующие структуре хранения данных в БД системы. В первой таблице хранятся записи, каждая из которых соответствует строке в исходной таблице и относится к одному клиенту. Вторая таблица хранит записи, в которые помещаются значения параметров клиентов, таким образом, несколько записей второй таблицы соответствуют одной записи первой таблицы (см. рисунок 2).

Так как все поступающие файлы имеют разнородную структуру, то их необходимо привести к виду, допускающему разбор данных в программе. Для этого используется механизм предварительной обработки. Он представляет собой приведение данных к виду, в котором они могут быть считаны и загружены в БД. В ходе проектирования программного модуля было получено два алгоритма форматирования.

В первом из них происходит предварительное форматирование, в результате чего генерируется файл формата *.txt, данные в котором имеют необходимый для считывания и загрузки вид. После чего программа считывает данные из полученного файла и загружает их в БД. Данный метод применяется в случаях, когда файл с данными имеет недопустимое расширение, иную кодировку или по каким-либо еще причинам не может быть корректно считан программой.

Во втором – форматируются уже считанные программой данные. Постобработчик вносит в сформированную таблицу данных необходимые изменения, к ним относится удаление пустых либо устаревших записей. После чего данные из форматированной таблицы загружаются в БД. Этот метод применяется, когда данные имеют необходимый формат, но часть данных являются неактуальными или не несут никакой информации. Поэтому такие данные нужно исключить при загрузке в БД.

Наиболее оптимальным является синтез двух этих алгоритмов. Можно выделить два типа форматирования: предобработка и постобработка. Первый генерирует форматированный файл и предоставляет его для считывания, второй форматирует уже считанные программой загрузки данные.

Для выполнения пред или пост обработки используются индивидуальные библиотеки форматирования, которые разрабатываются оператором для каждой услуги при первом анализе поступившего от организации файла. Разработанные библиотеки загружаются и хранятся в БД в виде массива байт. Их использование происходит по средствам рефлексии – механизма динамического использования сборок [3]. Разработанная программа-адаптер обладает собственной базой данных, в который хранится список услуг и все соответствующие им настройки, включая индивидуальные библиотеки для форматирования разбираемых данных.

Клиентская информация имеет значительный объем, поэтому количество записей, добавляемых в базу велико, в связи с этим появляется риск быстрого роста объема файла беклога. Это может привести к

проблемам, связанным с нехваткой места на жестком диске. Так же данный процесс накладывает значительную нагрузку на систему, что понижает ее производительность.

В качестве решения данной проблемы в БД программы создаются промежуточные таблицы, в которые загружаются разобранные данные по мере их поступления. Эти таблицы дублируют таблицы из целевой базы, к которым обращается система для использования данных. Через определенный период весь объем накопленных данных в промежуточной БД перемещается в целевую базу. В результате за весь период загрузка данных в основную базу проходит однократно, что повысит производительность.

Перенос данных осуществлен по средствам простой инструкции insert, которая реализована в хранимой процедуре. Затем промежуточная БД очищается, после чего готова к загрузке новых данных.Данный процесс автоматизирован и выполняется в заданное время с определенным периодом. Наиболее подходящим периодом являются одни сутки. А время выполнения хранимой процедуры назначено в момент, когда система испытывает наименьшую нагрузку, то есть в ночное время, когда проводится минимальное количество операций [4].

В результате разработанный адаптирующий модуль позволяет автоматизировать разбор и загрузку поступающих в систему клиентских данных, что в итоге повышает общую производительность платежной системы.

Список литературы

[1]. Шигаров А.О. Технология извлечения табличной информации из электронных документов разных форматов. Дис. канд. тех. наук. Иркутск, 2010, 142 с.

[2]. Ицик Бен-Ган. Microsoft SQL Server 2012. Основы T-SQL. Москва, Эксмо, 2015, 400 с.

[3]. Рефлексия (C# и Visual Basic). URL: https://msdn.microsoft.com/ru-ru/library/ms173183.aspx (дата обращения 17.10.2015).

[4]. Создание и использование хранимых процедур. Региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе». Москва, 2014, том 2 с.195-203.

Солдатов Константин Николаевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: Smile35777@gmail.com

Потапов Андрей Евгеньевич - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: potapov-ae@mail.ru

А.А. Карышев, А.И. Веселин

АНАЛИЗ СИСТЕМ УПРАВЛЕНИЯ ПЕРСОНАЛЬНЫМ КОМПЬЮТЕРОМ ДЛЯ ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В современном мире существует идея инклюзии — полного включения людей с особенностями и ограниченными возможностями в жизнь общества. Главные материальные условия инклюзии — создание единой информационной среды, одинаково доступной людям с любыми видами ограничений.

В рамках данной идеи компьютер представляет собой доступный человеку с ограниченными возможностями инструмент для выполнения каких-то определенных задач, а также для восстановления или замены отдельных сенсорных функций. Например, программы экранного доступа, озвучивая текст, позволяют человеку с ограничениями по зрению читать. Однако для некоторых категорий людей (например, незрячие люди, с нарушениями двигательных функций, пожилые) возникает проблема управления персональным компьютером, что существенно затрудняет доступ к информации, и, соответственно, препятствует реализации идеи инклюзии.

Одним из решений обозначенной проблемы является использование программ экранного доступа (скринридеров) - программных средств для чтения текстовой информации и озвучивания действий пользователя с помощью синтезаторов речи. В операционную систему Windows встроен экранный диктор, отчасти выполняющий функции экранного доступа, однако его возможности ограничены озвучиванием активных элементов интерфейса и чтением текста в активных окнах. Кроме того, в экранном дикторе Windows отсутствует поддержка русского языка [1]. Поэтому на территории РФ используются программные продукты сторонних производителей JAWS и NVDA, позволяющие выполнять без зрительного контроля практически все задачи, с которыми сталкивается пользователь компьютера:

— просмотр веб-страниц в Internet Explorer и Mozilla Firefox;
— работа с документами в редакторах WordPad или Microsoft Word;
— создание электронных таблиц в Microsoft Excel;
— отправка и получение почты в Outlook Express;
— запуск приложений из командной строки;
— управление компьютером с помощью меню кнопки «Пуск», проводника Windows, панели управления и других стандартных средств операционной системы;
— работа с программой Skype[2].

Управление тем, что следует зачитывать, осуществляется в скринридерах с помощью «горячих клавиш» — программа может перечислять по очереди все элементы активного окна или озвучивать

только выбранное. Например, в настройках программы JAWS в категории «Информативность речи» задается степень детализации сообщений. Высший уровень информативности подходит начинающим пользователям — программа произносит все доступные сведения о каждом элементе, включая сообщения контекстной справки. На низшем уровне, предназначенном для опытных пользователей, озвучивается лишь самый необходимый минимум сведений.

В окнах браузеров и редакторов JAWS озвучивает текст в рабочей области окна. Для перемещения курсора по тексту используются клавиши со стрелками. Сочетания клавиш JAWS указывают, как следует читать текст. Для этих самых востребованных команд удобно пользоваться цифровым блоком в правой части клавиатуры.

Помимо программ экранного доступа существует несколько дополнительных приложений, таких как FSReader и HJPad, расширяющих функционал скринридеров. FSReader — модуль для программы экранного доступа JAWS, предназначенный для чтения электронных книг. HJPad — текстовый редактор, напоминающий WordPad. Его основное достоинство — встроенная проверка орфографии и адаптированность к работе на слух.

В программном продукте NVDA есть несколько функций, которые не были реализованы в других скринридерах. Например, это объектная навигация — объекты рабочего стола представляются как древовидная иерархическая структура по аналогии с пунктами во вложенных меню и папок в проводнике Windows. Пользователь с помощью клавиш или мыши может перемещаться по такому дереву, а NVDA озвучивает названия объектов, их свойства, положение в иерархии и позволяет выполнять с объектами различные действия.

Кроме того в NVDA реализована поддержка работы с мышью. При этом положение указателя мыши на экране контролируется с помощью звуков. При наведении мыши на объект он озвучивается. А для озвучивания индикаторов выполнения в прикладных программах использует тоновые сигналы — чем ближе полоса индикатора к 100%, тем выше тон сигнала.

В озвучивании текста в программах экранного доступа всегда участвуют два основных компонента:

— SAPI (Speech Application Programming Interface) — программные библиотеки, входящие в состав операционной системы Microsoft Windows. Они отвечают за взаимодействие самой ОС и различных приложений с программами синтеза, и распознавания речи. К настоящему времени актуальными являются две версии Speech API: SAPI 4 и SAPI 5.
— Голосовой движок — компонент, отвечающий непосредственно за синтез голоса. За основу берутся записи реального голоса живого диктора. Затем из них нарезаются отдельные звуки (фонемы), а уже из этих фрагментов программа в процессе чтения воспроизводит произносимые слова. Каждый голосовой движок привязан к определенному языку, и тексты, написанные на другом языке, воспроизводиться не будут.

Основной проблемой использования программ экранного доступа является их недостаточная совместимость с браузерами. Некоторые типы браузеров не поддерживают работу с программами экранного доступа. Наилучшим образом обеспечивается совместимость с браузером Internet Explorer.

Другой распространенной проблемой является неадаптированность контента сайтов для скринридеров. Например, если текст на сайте представлен в виде изображения, то программа не сможет его озвучить. Следует отметить, что наличие динамически подгружаемого контента, а также использование технологии Flash также отрицательно сказывается на работоспособности программ экранного доступа. Поэтому был разработан ряд требований для реализации сайтов, позволяющий избежать данных проблем[3].

Еще одним решением проблемы управления персональным компьютером для людей с ограниченными возможностями является использование средств голосового управления. Попытки создать средства распознавания живой речи предпринимаются давно, однако все существующие технологии далеки от совершенства. Во-первых, система распознавания речи создается строго под определенный язык и требует больших временных затрат. Большинство существующих на сегодня речевых программ — англоязычные. Во-вторых, требуется индивидуальная настройка на голос и особенности дикции: в процессе обучения человек раз за разом произносит в микрофон предлагаемые

слова и фразы, а программа постепенно накапливает сведения о том, как звучит то или иное слово в произношении конкретного человека. Однако голос меняется в зависимости от состояния, настроения — это сильно влияет на точность и правильность распознавания. Кроме того, многое зависит от качества микрофона и уровня сигнала. Распознаванию существенно мешают посторонние шумы, поэтому всегда рекомендуется использовать микрофонную гарнитуру.

В операционных системах Windows 7, Windows 8 и Windows 10 предусмотрен встроенный механизм распознавания речи. Он работает в тех случаях, когда в качестве языка системы выбран английский, французский, испанский, немецкий, японский или китайский языки. Язык системы — тот, на котором отображаются все диалоговые окна, меню, сообщения, названия программ, справка. Соответственно, распознаваться будут слова, произносимые на том же языке. Данная функция доступна только в английской версии Windows. Ссылки странице распознавания речи запускают мастера настройки и интерактивные руководства:

— Start Speech Recognition (Начать распознавание речи). Мастер начальной настройки — обязательный этап. Пока не выполнены все шаги этого мастера, программа распознавания речи не запустится;
— Set up microphone — настроить микрофон;
— Take Speech Tutorial (Обучение разговору с компьютером) — руководство, помогающее освоить на примерах основные приемы голосового управления и диктовки текста;

— Train your computer to better understand you (Научите компьютер лучше понимать вас) — адаптация системы к особенностям дикции и голосу;
— Open the Speech Reference Card (Открыть справочник по речевым командам).

Работа функции распознавания речи возможна в двух режимах: управления программами — произносимые команды запускают и закрывают программы, переключают активные окна, сохраняют и удаляют файлы и т. п.; и диктовка в программы, которые поддерживают ввод текста — например, в редакторы Microsoft Word или WordPad. В первом случае используется строго определенный набор команд — их перечень содержится в справочнике речевых команд. Например, для щелчка мыши на значке «Компьютер» используется команда «Click Computer». При диктовке текста произносимые слова вводятся в документ там, где сейчас находится курсор. При этом слова, которые присутствуют в словаре, распознаются и вводятся целиком. Если же слова в словаре нет, его нужно диктовать по буквам.

Над проблемой распознавания речи работает целый ряд компаний. Однако выпущенных и актуальных на сегодняшний день программ для персонального компьютера не так уж много. Самое известное приложение —ViaVoice, разработанное компанией IBM. Российские компании VoiceLock и White Computers основательно переработали данную программу и выпустили приложение «Горыныч». Голосовые команды, которые распознает приложение, позволяют выполнить практически любые действия на рабочем столе, в меню кнопки «Пуск» и в окнах приложений. Среди доступных команд имеются «Выделить», «Копировать», «Вставить», «Удалить» и т. д. Предусмотрены команды управления указателем мыши, например: «Мышь влево», «Мышь вправо», «Щелчок левой» и т.д. Программа «Горыныч» на сегодняшней день устарела, ее поддержка полностью прекратилась несколько лет назад, однако для русскоязычных пользователей она является альтернативой встроенным средствам Windows.

Голосовые технологии начинают активно использоваться в браузерах. В первую очередь, распознавание речи нацелено на поиск. На настольных компьютерах голосовой поиск и ввод реализован в браузерах Google Chrome и Opera. Данные функции реализованы с помощью расширений браузера (Extensions) и плагинов. Браузер Opera поддерживает только английский язык, поддержка других языков не предусмотрена. Ниже приведены некоторые расширения для браузера Google Chrome, реализующие функции распознавания речи:

— Голосовой ввод Oweb — по умолчанию после установки расширения голосовой ввод постоянно действует в текстовых полях на веб-страницах. Голосовой ввод Oweb поддерживает около 30 языков, в том числе русский. В русскоязычной версии Chrome это расширение использует русский язык по умолчанию. Данное расширение хорошо подходит для заполнения любых полей на веб-страницах — поиска, форм и т. д;

— Chrome Voice Control — расширение для голосового управления браузером. Команды позволяют переключаться между вкладками, прокручивать страницы, открывать ссылки и т. д. Кроме того, Chrome Voice Control умеет открывать многие популярные сайты, когда произносится соответствующий веб-адрес, осуществляет поиск на картах Google по названиям объектов. Присутствует и голосовой ввод в текстовые поля;
— Voice In — голосовой ввод текста при минимальном использовании ресурсов компьютера. Особенность этого расширения в том, что обработка и распознавание голоса полностью осуществляются на сервере в Интернете[4].

Из всего вышеперечисленного можно сделать вывод о том, что программы экранного доступа и голосового управления позволяют людям с ограниченными возможностями в той или иной степени осуществлять управления персональным компьютером, работать с документами, просматривать сайты, почту, осуществлять голосовой ввод и поиск информации. Голосовые технологии управления стоит рассматривать только как дополнение к другим способам ввода информации и управления в связи с тем, что на сегодняшний день они далеки от совершенства.

Многие программы не имеют поддержки русского языка, что существенно сказывается на возможности выбора пользователем наиболее подходящего продукта для своих нужд и целей.

Список литературы

[1]. Сенкевич Г.Е.Компьютер для людей с ограниченными возможностями. БХВ — Петербург, 2014-320с.

[2]. Программа экранного доступа NVDA [Электронный ресурс] http:// http://nvda.ru/ (Дата обращения 22.10.2015)

[3]. Рекомендации по доступности страниц для людей с ограниченными возможностями [Электронный ресурс] http:// http://habrahabr.ru// (Дата обращения 02.10.2015)

[4]. Расширения для браузера Google Chrome [Электронный ресурс]. http:// https://www.google.ru/chrome/webstore/extensions.html (Дата обращения 18.10.2015)

Карышев Андрей Анатольевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ak9105252055@yandex.ru

Веселин Андрей Игоревич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: ak9105252055@yandex.ru

С.В.Сайкин, Н.А. Борсук

АНАЛИЗ СПОСОБОВ РЕШЕНИЯ ЗАДАЧИ СЕГМЕНТИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ВЕБ-СТРАНИЦЕ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Интернет развивается очень быстро. Из небольшой сети, соединяющей несколько университетов США, она выросла до действительно гигантских размеров. К 30 июня 2012 года число пользователей, регулярно использующих интернет, составило более чем около трех млрд человек, а количество веб-сайтов еще в 2014 году превысило 1 миллиард. [1]

Если с начала своего появления веб-страницы содержали в основном текст, то в настоящее время для привлечения посетителей необходима и дизайнерская составляющая. Человеку больше нравится видеть пестрые краски, чем черный текст на белом фоне. Поэтому разработчики все чаще для оформления сайта используют изображения. Использование сегментированных изображений (изображений-карт) позволяет постепенно, пошагово перемещаться по различным Интернет-ресурсам, в некоторых случаях детализируя требуемую информацию. Существует несколько способов разбиения изображения на части:

— Сегментировать целостное изображение на отдельные фрагменты.
— Разрезать изображение на фрагменты и объединить их воедино с помощью таблицы, при этом отдельные фрагменты будут служить ссылкой.
— Воспользоваться позиционированием элементов.

Использование карты-изображения позволит разбить единое изображение на сегменты различной формы, что очень удобно для создания, например, карты мира или карты регионов. Для использования карты-изображения используется специальный тег <map>, который служит контейнером для элементов <area>. У элемента <area> есть 4 атрибута:

— shape – определяет форму активной области (окружности – circle, прямоугольника – rect, полигона – poly).
— alt - добавляет альтернативный текст для каждой области.
— coords - задает координаты активной области.
— href - определяет адрес ссылки для области.

```
<img src="Picture.png" usemap="#Map">
<map name="Map">
<area shape="poly" coords="113,24,211,24,233,0,137,0" href="Page.html">
</map>
```

Соединение изображений с помощью таблицы хорошо подойдет для массива элементов, например, при создании небольшого Интернет-магазина, в котором представлено изображение товара и краткое его описание.

```
<table>
 <tr>
 <td><a href="page.html"><img src="Товар.png"></a><br>описание</td>
 </tr>
</table>
```

Позиционирование элементов удобно использовать для точного расположения элемента на странице. Оно устанавливается через стилевые свойства элементов. С помощью свойств *position*, *left*, *top*, *right* и *bottom* элементы можно накладывать один на другой, выводить в точке с определёнными координатами, фиксировать в указанном месте, определять положение одного элемента относительно другого и др. Подобно другим свойствам CSS, управление позиционированием доступно через скрипты. Таким образом, можно динамически изменять положение элементов без перезагрузки страницы, создавая анимацию и различные эффекты.

```
<div id="ID" style="position:absolute; left:100px; top:100px">
<a href="page.html"><img src="Picture.png"></a>
</div>
```

Из сказанного выше следует, что хоть и способов разбиения изображений немного, но они отлично справляются со своей задачей, обеспечивая навигацию по сайту с помощью изображений.

Список литературы

[1]. [Электронный ресурс] Интернет. URL: https://ru.wikipedia.org/wiki/Интернет (дата обращения 27.10.2015)

Сайкин Сергей Вячеславович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: saikinry@ya.ru

Борсук Наталья Александровна – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: borsuk.65@yandex.ru

А.Н. Воронцов, Ю.С.Белов

АРХИТЕКТУРА СИСТЕМЫ УПРАВЛЕНИЯ ПРОЕКТАМИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

При наличии большого количества однотипных задач, например, заполнение определенного вида анкет, решаемых вручную, целесообразным является разработка программного обеспечения, которое будет решать задачи подобного рода. Система сокращает время, затрачиваемое на решение задачи и обработку ее результатов, что положительным образом сказывается на производительности задействованных в трудовой деятельности сотрудников.

По поручению Министерства развития информационного общества Калужской области начата разработка Системы управления проектами министерства.

В задачи министерства входит: Обеспечение предоставления гражданам и организациям услуг на основе современных ИКТ с использованием элементов электронного правительства; развитие технической и технологической основы информационного общества в Калужской области; комплексная оптимизация государственных и муниципальных услуг по сферам общественных отношений; обеспечение предоставления гражданам и организациям государственных и муниципальных услуг по принципу "одного окна" по месту пребывания [1].

Правовой базой, создаваемой системы, являются: Постановление Правительства Калужской области от 20.12.2013 N 710 (ред. от 18.09.2015) "Об утверждении государственной программы калужской области "информационное общество и повышение качества государственных и муниципальных услуг в калужской области", распоряжение от 14 апреля 2014 г. n 26р-ау "об утверждении методических рекомендаций по внедрению проектного управления в органах исполнительной власти", приказ от 24 апреля 2013 г. n 96 "об утверждении методических рекомендаций по организации системы проектного управления мероприятиями по информатизации в государственных органах".

Задачи разрабатываемой системы: создание проекта, хранение информации по проекту, формирование отчетности по проектам.

Работа над проектом включает в себя: создание проекта и отправку его сотрудникам для дополнения информации по проекту, в случае, если это составная часть какого – либо проекта, то указывается основной проект. (Рисунок 1) После завершения процедуры создания и уточнения проекта у специалистов, проект отправляется министру, который подтверждает его, либо отказывает в принятии проекта к исполнению.

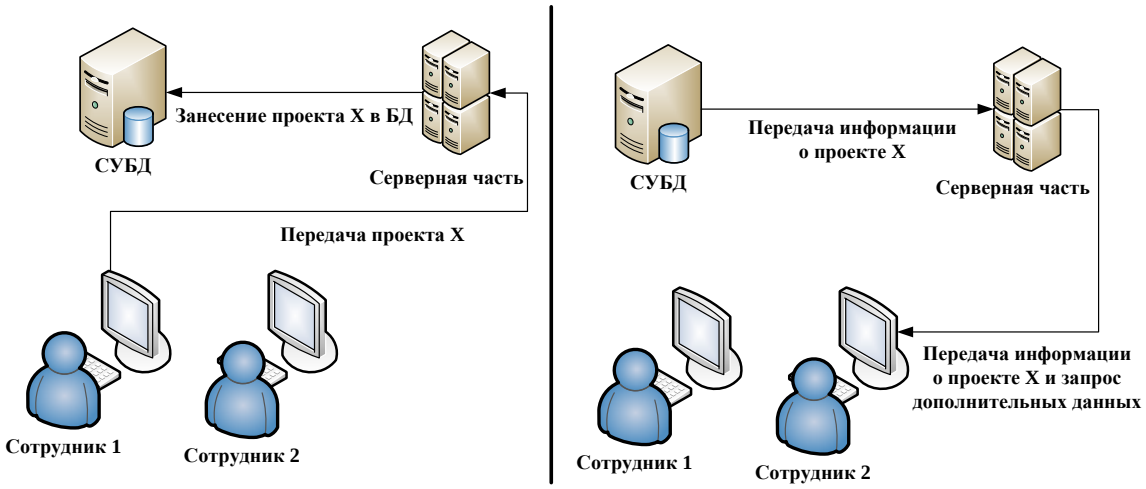


Рис. 1. Создание и уточнение проекта

Система состоит из Клиентской части, Серверной части и СУБД. Клиентская часть приложения отвечает за подключение пользователя к серверной части, после аутентификации пользователь получает доступ к базе данных системы на правах, определенных его ролью в системе. Серверная часть принимает запросы пользователей, проверяет их соответствие роли пользователя и выдает необходимую информацию из базы данных. В задачи серверной части входит формирование отчетной документации по проектам и отправка ее по требованию соответствующему пользователю. Важной задачей серверной части является оповещение сотрудников о необходимости принятия решения по проекту и его модификации в базе данных.

Клиентскую часть планируется использовать на персональных компьютерах с операционной системой Windows. Интерфейс приложения проектируется средствами WinApi, а программная часть проектируется на языке C++. Клиентское приложение должно быть отказоустойчивым, надежным и безопасным в использовании.

Выбор в качестве инструмента разработки интерфейса WinApi обусловлен тем, что данный набор функций предоставляет возможность для взаимодействия с операционной системой windows без привлечения дополнительных библиотек, что повышает скорость выполнения приложения и гарантирует его переносимость на другие персональные компьютеры под управлением операционной системы Windows [2].

Выбор в качестве инструмента разработки приложения языка C++ обусловлено тем, что данный язык поддерживает различные стили и технологии программирования, может быть легко расширен за счет подключения необходимых библиотек, обеспечивает высокую степень контроля над созданием программы [3].

Серверная часть на начальном этапе будет реализована для персонального компьютера с операционной системой Windows.

Планируемый интерфейс будет так же реализован средствами WinApi, а программная часть написана на языке C++. В дальнейшем, с развитием системы и возможным ее переносом на сервер Министерства, будет рассматриваться возможность разработки Web-интерфейса и реализации программной части интегрированными средствами разработки.

В качестве СУБД планируется использовать Firebird, главным образом из-за ее свободного распространения. Выбор Firebird обусловлен наличием полной поддержки хранимых процедур и триггеров, мощного внутреннего языка, который позволяет писать хранимые процедуры и триггеры и возможность сведения к минимуму работы системного администратора [4]. С развитием разрабатываемой системы СУБД может быть заменена на один из коммерческих аналогов, к примеру, на Microsoft Access [5].

В качестве средства администрирования планируется использование IBExpert. Выбор IBExpert обусловлен наличием мощного SQL редактора, отладчика хранимых процедур и триггеров, отчетов по метаданным и менеджеров пользователей и их привилегий [6].

Безопасность системы обеспечивается в первую очередь разграничением прав доступа пользователей к информации, и процедуре аутентификации пользователей. Для обеспечения безопасности при передаче данных по сети планируется использование криптографического алгоритма ГОСТ 28147-89. Выбор «ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» обоснован бесперспективностью атаки полным перебором, эффективностью реализации, защитой от «навязывания» ложных данных [7].

Для того чтобы организовать защищенную передачу ключа, необходимо использовать алгоритм шифрования RSA-OAEP. Данный алгоритм выбран для передачи ключа, поскольку он является достаточно надежным для разовой передачи небольшого сообщения [8].

Среди достоинств системы можно отметить простоту реализации и обслуживания, достаточный уровень безопасности, интерфейс программы будет прост и интуитивно понятен, что позволит не тратить много времени на освоение программы. Пользователю при создании проекта будут предлагаться формы, которые состоят из названий пункта заполнения и прямоугольных полей для ввода. Заполнив их, пользователь получит фактически готовый проект.

Среди недостатков системы можно отметить отсутствие взаимодействия с другими системами, такими как единая информационная система и узкое направление применения.

В дальнейшем, система может быть улучшена следующими способами:

— Перенос серверной части и базы данных на высокопроизводительный сервер министерства и соответствующую доработку отдельных модулей;

— Расширение спектра решаемых задач, в частности, добавление функционала системы автоматизации закупочной деятельности и взаимодействие с государственными системами по данному вопросу в соответствие с 44-ФЗ и 223-ФЗ;
— Исправление ошибок и недочетов системы.

Вывод: Данная система решает поставленные перед ней задачи, но может быть расширена и доработана, как для повышения производительности и качества обслуживания, так и для расширения функционала.

Список литературы

[1] Постановление Калужской области от 20 декабря 2013 г. N 710. URL: http://www.admoblkaluga.ru/sub/min_inform/agreements/pprko710_2013_12_20.php (дата обращения 21.10.2015).

[2] Справочник по Windows API. URL: http://w32api.narod.ru/functions_abc.html (Дата обращения 21.10.2015).

[3] Справочник по языку C++. URL: https://msdn.microsoft.com/ru-ru/library/3bstk3k5.aspx (Дата обращения 21.10.2015).

[4] Официальный сайт Firebird. URL: http://www.firebirdsql.org/ (Дата обращения 22.10.2015).

[5] Официальный сайт Microsoft Office Access. URL: https://products.office.com/ru-RU/access?legRedir=true&CorrelationId=5fbe9c1e-7754-41be-a71c-304e465fe0cc (дата обращения 22.10.2015).

[6] Официальный сайт IBExpert. URL: http://www.ibexpert.net/ibe/ (Дата обращения 22.10.2015).

[7] Федеральное агентство по техническому регулированию и метрологии. URL: http://protect.gost.ru/document.aspx?control=7&id=139177 (Дата обращения 23.10.2015).

[8] RSAES-OAEP Encryption Scheme. Algorithm specification and supporting documentation. URL: http://www.inf.pucrs.br/~calazans/graduate/TPVLSI_I/RSA-oaep_spec.pdf (Дата обращения 24.10.2015).

Воронцов Антон Николаевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: anton.vorontsov1994@yandex.ru

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

В.В. Сорочан, К.В. Степаненко

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ АВТОМАТИЗАЦИИ В ТЕСТИРОВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

С развитием информационных технологий, повышаются требования к качеству выпускаемого программного обеспечения (ПО). Повысить качество можно посредством тестирования, которое позволяет выявить присутствующие недоработки. От качества тестирования на этапе разработки ПО зависит вероятность возникновения проблем во время работы программы.

Тестирование программного обеспечения - это проверка соответствия между реальным и ожидаемым поведением программы, осуществляемая на конечном наборе тестов, выбранном определенным образом [1]. Все виды тестирования программного обеспечения, в зависимости от преследуемых целей, можно условно разделить на следующие группы: функциональное, нефункциональное, связанное с изменениями.

Функциональные тесты базируются на функциях и особенностях, а также взаимодействии с другими системами, и могут быть представлены на всех уровнях тестирования: компонентном или модульном (Component/Unit testing), интеграционном (Integration testing), системном (System testing) и приемочном (Acceptance testing). Функциональные виды тестирования рассматривают внешнее поведение системы. Как правило, функции описываются в требованиях, функциональных спецификациях или в виде случаев использования системы [2]. Автоматизация такого вида тестирования достаточно распространена. Она позволяет ускорить процесс тестирования и свести к минимуму «человеческий фактор». Так же после написания автоматических тестов потребуется меньше затрат на поддержку и анализ результатов чем в случае тестирования вручную [3].

Наиболее распространенной формой автоматизации является тестирование приложений через графический пользовательский интерфейс. В этом случае есть возможность тестировать не только интерфейс пользователя, но также и функциональность, выполняя операции, вызывающие бизнес логику приложения. Такого рода сквозные тесты дают больший эффект, чем просто тестирование функционального слоя. Популярность такого тестирования объясняется двумя факторами: во-первых, приложение тестируется тем же способом, которым его будет использовать человек, во-вторых, можно тестировать приложение, не имея при этом доступа к исходному коду.

Выбор инструмента тестирования в конкретном случае зависит от объекта тестирования и требований к тестовым сценариям, так как

инструменты тестирования не могут поддерживать абсолютно все технологии, используемые при разработке приложений.

В системе "1С:Предприятие 8" начиная с платформы версии 8.3 появился новый механизм автоматизированного тестирования. Механизм позволяет легко и быстро создавать различные сценарии тестирования, без необходимости написания сложных процедур и функций для имитации действий пользователя. При автоматизированном тестировании между собой взаимодействуют два клиентских приложения [4]. Одно, - это менеджер тестирования, на котором исполняется алгоритм теста. Второе, - это клиент тестирования, который воспроизводит интерактивные действия пользователя. В качестве менеджера тестирования может выступать толстый или тонкий клиент. Клиентом тестирования может быть любое из клиентских приложений: толстый клиент, тонкий клиент или веб-клиент. Встроенный язык содержит ряд специализированных объектов, позволяющих на клиенте тестирования имитировать действия пользователя: навигация по прикладному решению, выполнение интерактивных команд системы, ввод данных в поля форм, чтение данных, отображаемых в форме, и т.д. Преимуществом автоматизированного тестирования является простота и наглядность разработки тестов. Поскольку тест оперирует только интерактивными действиями пользователя, то разработчику не нужно знать структуры конфигурации на уровне реквизитов объектов. При изменении, например, кода конфигурации нет необходимости переделывать тест, поскольку на клиенте тестирования по-прежнему будут выполняться те же самые действия с теми же самыми элементами управления. Механизм автоматизированного тестирования может быть использован тестировщиками для записи последовательности действий, приводящих к ошибке. Записанные данные можно отправить разработчикам для исправления обнаруженной ошибки. Также автоматизированное тестирование может применяться для выявления в конфигурации избыточных блокировок и взаимоблокировок [5]. Однако у автоматизированного тестирования есть и недостатки, так написанные тесты всегда будут выполняться однообразно, а выполняя тест вручную, можно обратить внимание на некоторые детали и, проведя несколько дополнительных операций, найти дефект. На разработку автоматизированных тестов требуются большие затраты, так как фактически идет разработка приложения, которое тестирует другое приложение. В сложных автоматизированных тестах также есть фреймворки, утилиты, библиотеки и прочее. Естественно, все это нужно тестировать и отлаживать, что требует времени.

Для принятия решения о целесообразности автоматизации тестирования приложения необходимо решить перевешивают ли преимущества внедрения системы затраты на её разработку. В большинстве случаев автоматизированное тестирование применяется в совокупности с ручным.

Список литературы

[1]. ПроТестинг. Тестирование программного обеспечения - основные понятия и определения. URL: http://www.protesting.ru (дата обращение 23.10.2015)

[2]. ПроТестинг. Виды Тестирования Программного Обеспечения. URL: http://www.protesting.ru (дата обращение 23.10.2015)

[3]. Дастин Э., Рэшка Дж, Пол Дж. Автоматизированное тестирование программного обеспечения. Москва, Лори, 2003, 592 с.

[4]. 1С:Предприятие 8. Автоматизированное тестирование, механизм URL: http://v8.1c.ru/overview (дата обращение 23.10.2015)

[5]. Автоматизированное тестирование в «1С:Предприятие 8.3» URL: http://курсы-по-1с.рф (дата обращение 23.10.2015)

Сорочан Виталий Викторович - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: vsorochan@mail.ru

Степаненко Ксения Витальевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: stepanenkoxenia@gmail.com

Ю.Е. Гагарин, С.Н. Гагарина

ВОЗМОЖНОСТЬ УЧЕТА ПОГОДНЫХ ФАКТОРОВ ПРИ ОПРЕДЕЛЕНИИ ОБЪЕМОВ РЕАЛИЗАЦИИ УСЛУГ МЕТОДАМИ ТЕОРИИ ИГР

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

На объем реализации коммунальных услуг населению значительное влияние оказывают конкретные местные условия: социально-экономические, природно-климатические, градостроительные, демографические. Вместе с тем, объем реализации коммунальных услуг определяется субъективными факторами, отражающими индивидуальные особенности и образ жизни населения региона.

Вышерассмотренные факторы являются источником неопределенности объемов реализации коммунальных услуг.

Кроме того, спрос на коммунальные услуги может подвергаться суточным и сезонным колебаниям. Так, в коммунальном секторе спрос на энергоносители будет различен в зависимости от районов проживания населения и также характеризуется большой неравномерностью по часам суток, дням недели, месяцам и сезонам года.

Результаты анализа потребления электроэнергии, газа, тепловой энергии населением региона показывают наряду с сезонной неравномерностью и годовую неравномерность потребления исследуемых коммунальных услуг, которая может быть обусловлена влиянием природных факторов, как, например, колебаниями температуры воздуха. Это предопределяет необходимость разработки новых подходов к прогнозированию объемов реализации услуг в условиях неопределенности.

В настоящее время одним из наиболее распространенных инструментов обоснования социально-экономических прогнозов посредством методов математического моделирования является теория игр.

При определении объемов реализации коммунальных услуг населению в холодный и теплый период времени года возможны различные ситуации. Например, в холодный период времени года возможно потепление или похолодание. Аналогичные ситуации возможны и для теплого периода времени года.

Ситуации, в которых выбор оптимального решения осуществляется не одним лицом, принимающим решение (ЛПР), а в которых целям ЛПР противостоит мыслящий противник, называются конфликтными. Теория, в которой рассматриваются подобные задачи принятия решений, известна как теория игр [1].

В отличие от реального конфликта игра ведется по определенным правилам, которые четко определяют права и обязанности участников игры, объем информации каждой стороны о другой, а также исход игры (выигрыш и проигрыш каждого участника). В игровом конфликте участвуют два противника, именуемые игроками, каждый из которых имеет некоторое множество (конечное или бесконечное) возможных выборов, которые называются стратегиями.

Выбор оптимальной стратегии для игрока A – это выбор стратегии A_i, которая обеспечивает ему максимально возможный выигрыш, независимо от стратегии игрока B.

С точки зрения игрока A, ему необходимо выбрать такую стратегию A_i, которая максимизирует минимально возможный выигрыш $\alpha = \max_i \min_j a_{ij}$ – максиминная стратегия (максимин). Величина α определяет нижнюю цену игры. Меньше, чем α, игрок A выиграть не может. Для игрока B оптимальной стратегией является та, при которой максимально возможный выигрыш игрока A оказывается наименьшим и в любом случае не превосходит $\beta = \min_j \max_i a_{ij}$. Величина β (минимакс) определяет верхнюю цену игры.

Максиминная стратегия игрока A так же, как и минимаксная стратегия игрока B, является наиболее осторожной, перестраховочной стратегией, и она гарантируют игроку B, что максимально возможный выигрыш игрока A оказывается наименьшим и в любом случае не превосходит минимакса, или, иначе, верхней цены игры. Точно так же при любом поведении игрока B игроку A гарантирован минимально возможный выигрыш (наибольший по сравнению с остальными стратегиями) не меньше нижней цены игры (максимина). Принцип осторожности, диктующий игрокам выбор таких стратегий, называется принципом минимакса.

Теория игр используется для исследования многократно повторяющихся конфликтных ситуаций. Если игроки будут от игры к игре придерживаться одной и той же стратегии, рекомендуемой принципом минимакса, то один из них может оказаться в наихудшей ситуации при внезапной смене стратегии другим игроком. Здесь проявляется общее правило для игр без седловой точки: игрок, играющий по определенной (детерминированной) стратегии, оказывается в более худшем положении по сравнению с игроком, который меняет стратегию случайным образом.

При принятии решения относительно объемов реализации коммунальных услуг населению с учетом изменения погоды игроками являются: организация коммунального комплекса (ОКК), и погода,

являющаяся неценовым фактором при формировании спроса на данную услугу [2].

Возможны три стратегии ОКК:

A_1 – потребление коммунальных услуг населением при средней температуре воздуха;

A_2 – потребление коммунальных услуг населением при отклонении от средней температуры воздуха: в холодный период времени года потепление, в теплый – похолодание;

A_3 – потребление коммунальных услуг населением при отклонении от средней температуры воздуха: в холодный период времени года – похолодание, в теплый – потепление.

Стратегиями погоды являются:

B_1 – холодный период времени года;

B_2 – теплый период времени года.

Как видно, существует шесть ситуаций, описывающих все комбинации из трех стратегий ОКК и двух стратегий игрока – погоды.

Предложенный метод прогнозирования на основе теории игр позволяет определить оптимальную стратегию ОКК, обеспечивающую ей независимо от погоды средний доход от реализации услуг.

Исследования проведены при финансовой поддержке Российского фонда фундаментальных исследований и Правительства Калужской области (проект № 14-41-03085).

Литература:

[1] Грешилов А.А. Математические методы принятия решений. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2006, 584 с.

[2] Гагарина С.Н., Гагарин Ю.Е. Интервальное прогнозирование объемов спроса на услуги субъектов естественных монополий с учетом неопределенности информации. Вестник университета (Государственный университет управления), 2013, № 22, с. 101-110.

Гагарин Юрий Евгеньевич - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: Yriigagarin@yandex.ru

Гагарина Светлана Николаевна - канд. экон. наук, доцент КГУ им. К.Э. Циолковского. E-mail: g_ug@mail.ru

Ю.С. Белов, Р.В. Либеров, Б.М. Логинов, Н.Н. Митрюшина

ЗАКОНОМЕРНОСТИ БЕСКОНТАКТНОГО ВЗАИМОДЕЙСТВИЯ СКОЛЬЗЯЩИХ ДИСЛОКАЦИЙ С ДИСЛОКАЦИОННЫМИ ПЕТЛЯМИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Процесс пластической деформации непосредственно связан с эволюционным развитием дислокационной структуры. В случае движения дислокаций в материалах подверженных радиационному облучению, возможно контактное и бесконтактное взаимодействие скользящих дислокаций с краевыми дислокационными петлями. Настоящая работа посвящена выявлению закономерностей бесконтактного взаимодействия дислокаций.

Взаимодействие гибкой скользящей дислокации с краевыми дислокационными петлями с плоскостями залегания (0001), компланарными плоскости движения гибкой дислокации и отстоящими от нее на различных расстояниях ± v проводилось для случая v≠0. Для краевых дислокационных петель $b''=0$, $\beta=\pi/2$, поэтому уравнение равновесия скользящей дислокации в полей напряжений краевой дислокационной петли приводится к виду:

$$\frac{\chi}{\rho}=\bar{\tau}_{yz}^{\perp}+\bar{\tau}, \qquad (1)$$

где $\chi=k2\pi(1-\nu)b/b^{\perp}=1{,}1172$, $b/b^{\perp}=(c/a)^{-1}=(1{,}856)^{-1}$.

Поиск равновесных конфигураций гибкой дислокации при различных уровнях приведенного внешнего напряжения $\bar{\tau}$ следует производить при значениях параметров $\overline{x^{*}}=10$ и $|\upsilon|\le 2{,}0$.

Вследствие антисимметрии сдвиговых напряжений $\bar{\tau}_{yz}^{\perp}$ краевой дислокационной петли относительно оси $\bar{x}$ графики зависимости $\bar{y}(0)$ от $\bar{\tau}$ центросимметричны относительно начала координат. Это означает, что для заданной плоскости скольжения равновесные конфигурации гибкой дислокации, рассчитанные при $\bar{\tau}$ и характеризующиеся параметрами $\bar{y}(0)<0$ (или $\bar{y}(0)<0$), совпадают с конфигурациями, рассчитанными для $-\bar{\tau}$ и описываемыми параметрами $\bar{y}(0)<0$ (или ($\bar{y}(0)>0$). Поэтому для получения всех возможных равновесных конфигураций гибкой дислокации достаточно найти решения уравнения (1) либо только для положительных значений внешнего напряжения $\bar{\tau}>0$ при положительных

и отрицательных значениях параметра $\bar{y}(0)$, либо для случая, когда внешнее напряжение $\bar{\tau}$ может быть как положительным, так и отрицательным, а параметр $\bar{y}(0) > 0$.

Участки кривых $\bar{y}(0)$ от $\bar{\tau}$ с положительными значениями производной $d\bar{y}(0)/d\bar{\tau}$ отвечают устойчивым, а с отрицательными значениями –неустойчивым состояниям гибкой дислокации. Проведенный анализ показал, что при заданном уровне внешнего напряжения в зависимости от расстояния υ до плоскости скольжения возможно существование от 1 до 9 различных равновесных конфигураций гибкой дислокации.

Формы кривых $\bar{y}(0)$ в зависимости от $\bar{\tau}$ отличаются большой сложностью и характеризуются существованием семи критических точек $\bar{\tau}_{-}^{(i)}$, $i = 1,2,...,7$ для $\upsilon < 0$ и пяти критических точек $\bar{\tau}_{+}^{(i)}$, $i = 1,2,3,4,7$ для $\upsilon > 0$ в которых $d\bar{y}(0)/d\bar{\tau} = \infty$. Критические точки определяют критические напряжения $\bar{\tau}_{\pm}^{(i)}$, при которых происходит смыкание ветвей, описывающих устойчивые и неустойчивые состояния гибкой дислокации.

Роль критических напряжений в процессе прохождения гибкой дислокации через поле напряжений призматической дислокационной петли можно проиллюстрировать, рассматривая эволюцию состояний гибкой дислокации при постепенно увеличивающемся уровне внешнего напряжения $\bar{\tau}$. В качестве примера рассмотрим случай, когда гибкая дислокация скользит в плоскости $\upsilon > 0$. В отсутствии внешнего поля $\bar{\tau} = 0$ равновесная конфигурация гибкой дислокации определяется точкой E'. При наложении однородного внешнего поля гибкая дислокация искривляется так, что $\bar{y}(0)$ начинают изменяться в направлении, указанном стрелкой. При достижении напряжения $\bar{\tau} = \bar{\tau}_{+}^{(4)}$ гибкая дислокация скачком переходит из состояния с $\bar{y}(0) < 0$ в другое с $\bar{y}(0) > 0$ (точка N). При дальнейшем увеличении $\bar{\tau}$ равновесные конфигурации гибкой дислокации характеризуются точками отрезка NC. При $\bar{\tau} = \bar{\tau}_{+}^{(3)}$ гибкая дислокация преодолевает поле петли, отрываясь от точек закрепления. Таким образом, напряжение $\bar{\tau} = \bar{\tau}_{+}^{(3)}$ в этом случае следует считать напряжением прохождения $\bar{\tau}_{пр}$. В тех случаях, когда $\bar{\tau}_{+}^{(4)} > \bar{\tau}_{+}^{(3)}$, гибкая дислокация при $\bar{\tau} = \bar{\tau}_{+}^{(4)}$ преодолевает поле петли, не останавливаясь у ее противоположного края. Подобная ситуация наблюдается и для плоскостей $\upsilon < 0$. Поскольку для любого $\upsilon > 0$ и $\upsilon < 0$ $\bar{\tau}_{+}^{(1)} < \bar{\tau}_{+}^{(2)}$, $\bar{\tau}_{+}^{(2)} < \bar{\tau}_{+}^{(4)}$ и $\bar{\tau}_{-}^{(1)} < \bar{\tau}_{-}^{(2)}$, $\bar{\tau}_{-}^{(2)} < \bar{\tau}_{-}^{(4)}$, соответствующие устойчивые состояния, не будут реализовываться в

процессе прохождения гибкой дислокации через призматическую дислокационную петлю. Следовательно, критические напряжения $\bar{\tau}_{+}^{(1)}$, $\bar{\tau}_{+}^{(2)}$, $\bar{\tau}_{-}^{(1)}$, $\bar{\tau}_{-}^{(2)}$, $\bar{\tau}_{-}^{(3)}$, $\bar{\tau}_{-}^{(6)}$ не определяют процесс прохождения гибкой дислокации. Определяющими процесс прохождения являются напряжения $\bar{\tau}_{+}^{(3)}$, $\bar{\tau}_{+}^{(4)}$, $\bar{\tau}_{+}^{(7)}$, $\bar{\tau}_{-}^{(4)}$, $\bar{\tau}_{-}^{(5)}$, $\bar{\tau}_{-}^{(7)}$ при которых происходит скачкообразный переход гибкой дислокации из одного устойчивого положения в другое.

При отрицательных значениях параметра v плоскость залегания краевой дислокационной петли находится под плоскостью скольжения гибкой дислокации и, в этом случае ведущий вклад в торможение скользящей дислокацией оказывает фронтальная половина дислокационной петли. Анализ полученных комплектов равновесных форм гибкой дислокации при различных значениях параметров $\bar{\tau}$ и υ позволяет сделать следующие заключения:

1. Заметное полевое влияние дислокационной петли на скользящую дислокацию начинает проявляться, когда расстояние между скользящей дислокацией и фронтальным краем дислокационной петли становиться меньше радиуса дислокационной петли.

2. При относительных значениях уровня внешнего сдвигового напряжения $\bar{\tau}$ не превышающих критической величины $\bar{\tau}_{кр}$ =0,13, дислокационная петля остается неподвижной.

3. При изменении граничных условий скользящей дислокации в диапазоне значений от y_k^* до y_{k+i}^* краевая дислокационная петля сохраняет способность удерживать скользящую дислокацию.

4. Увеличение уровня внешнего сдвигового напряжения до критического значения $\bar{\tau}_{кр} = 0{,}13$ приводит к тому, что силы Пайерлса уже не могут противостоять полевому воздействию скользящей дислокации и дислокационная петля начинает перемещаться.

5. В тех случаях, когда плоскость залегания краевой дислокационной петли находится ниже плоскости скольжения гибкой дислокации и удалена от нее на расстояние v не менее 0,15, скользящая дислокация не может увлечь за собой дислокационную петлю, при этом дальнейшее увеличение уровня внешнего напряжения сдвига приводит к преодолению скользящей дислокацией области полевого воздействия дислокационной петли в динамическом режиме.

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Либеров Роман Владимирович – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: rliberov@yandex.ru

Логинов Борис Михайлович – д-р физ.-мат. наук, зав. каф. КФ МГТУ им. Н.Э. Баумана. E-mail: loginov@kaluga.ru

Митрюшина Наталья Николаевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: natalya-mitryushina@yandex.ru

Ю.С. Белов, С.Г. Гуров

ИСПОЛЬЗОВАНИЕ ЛИНЕЙНОГО ПРЕДСКАЗАНИЯ И СПЕКТРАЛЬНЫХ ЧАСТОТ В ПРЕОБРАЗОВАНИИ ГОЛОСА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Преобразование голоса (voice conversion) – процесс, целью которого является преобразование голоса одного говорящего в голос другого говорящего. Изменение голоса может преследовать разную цель. Среди основных направлений можно выделить два: получение реалистичного звучания измененного голоса и получение некоторого необычного, фантастичного звучания. Для реализации последнего достаточно обрабатывать речевой сигнал как обычный, не заостряя внимания на его особенностях и делая многие допущения. Например, развитие электронной музыки привело к появлению огромного количества разнообразных аудио-эффектов, применяя которые можно получить самый невероятный образ голоса. В задаче реалистичного изменения голоса необходимо производить анализ сигнала перед его обработкой. Не существует алгоритмов, хорошо подходящих для обработки всех звуков речи. К тому же, один и тот же элементарный звук человек может произносить по-разному в зависимости от своего эмоционального, физического состояния, от места звука в слове, и т.д. Индивидуальные особенности произношения, культурный и языковой фактор, медицинские патологии — все это также оказывает влияние на произносимый звук.

Линейное предсказание (linear prediction) - это один из основных методов, используемых в обработке речи. Эта модель входного фильтра может быть использована для разделения речевого сигнала на коэффициенты линейного предсказания, которые моделируют акустику речевого тракта и для разделения речевого сигнала на сигнал возбуждения. Сигнал возбуждения может быть получен с помощью фильтра линейного предсказания,

$$r(t) = x(t) - \sum_{k=1}^{m} a_k x(t-k), \qquad (1)$$

где – это входной речевой сигнал, – порядок фильтра A(z).

Коэффициенты линейного предсказания обычно оцениваются покадровым способом с использованием либо автокорреляции, либо ковариационных методов. Метод автокорреляции широко используется потому что он всегда гарантирует, что полученные фильтры устойчивые.

Для дальнейшей обработки, коэффициенты линейного предсказания часто преобразуются в линейные спектральные частоты. Полностью обратное преобразование может быть осуществлено путем первоначального нахождения корней многочленов

$$P(z) = A(z) + z^{-(m+1)}A(z^{-1}),$$
$$Q(z) = A(z) - z^{-(m+1)}A(z^{-1}). \quad (2)$$

Затем, линейные спектральные частоты формируются с помощью угловых положений комплексных корней в порядке возрастания. Линейные спектральные частоты используются в различных областях обработки речи по многим причинам. Например, они предлагают нам выгодные свойства с точки зрения квантования, интерполяции и другой обработки, а также гарантируют устойчивость фильтра.

Линейные спектральные частоты также широко используются в преобразовании голоса. Они кодируют спектр речи более эффективно, чем другие наборы параметров. Это можно объяснить близостью их природы к природе формантных частот.

Для преобразования голоса требуются некоторые измерения расстояния. Расстояние между двумя векторами линейных спектральных частот может быть вычислено, например, используя взвешенную среднеквадратичную ошибку с помощью диагональной матрицы весов,

$$d(\omega, \hat{\omega}) = (\omega - \hat{\omega})^T W(\omega - \hat{\omega}) = \sum_{k=1}^{m} W_k(\omega_k - \hat{\omega}_k)^2. \quad (3)$$

Веса могут быть использованы для аппроксимации свойств человеческого слуха. Они определяются по формуле

$$W_k = c_k \left| H(e^{j2\pi f_k/f_s}) \right|^{0.6}, \quad (4)$$

где обозначает частоту -го элемента линейных спектральных частот, – частота дискретизации, обозначает синтезирующий фильтр $H(z) = 1/$. Кроме того, при работе с 10-мерными векторами линейных спектральных частот с частотой дискретизации равной 8 кГц, устанавливается в единицу для всех за исключением $c_9 =$ и $c_{10} =$.

В дополнение к взвешенному среднеквадратичному отклонению, другим полезным популярным показателем измерения расстояния между двумя спектрами является искажение спектра. Оно определяется в дБ как

$$SD = \sqrt{\frac{1}{f_u - f_l}\int_{f_l}^{f_u}\left(20log_{10}\frac{|H(e^{j2\pi f/f_s})|}{|\widehat{H}(e^{j2\pi f/f_s})|}\right)^2 df}, \quad (5)$$

где и обозначают нижний и верхний частотные пределы интегрирования. Главным преимуществом этого метода является тот факт, что существуют общепринятые критерии, которые основываются на искажении спектра для ощущения спектральной прозрачности, т.е. критерии, которые гарантируют, что прозрачность достигается при соблюдении следующих трех критериев:

Среднее искажение спектра должно быть менее 1 дБ;

Отсутствие посторонних кадров с искажением спектра более 4 дБ;

Менее 2% кадров имеют искажение спектра в диапазоне от 2 до 4 дБ.

Список использованных источников

[1]. Helander E. Maping techniques for voice conversion. Sc.Dr. thesis. Tampere University of Technology, Tampere, 2012.

[2]. Helander E., Nurminen J., Gabbouj M., Analysis of LSF frame selection in voice conversion. *SPECOM*, Moscow, 2007, pp. 651–656.

[3]. Линейное предсказание. URL: https://ru.wikipedia.org/wiki/Линейное_предсказание (дата обращения - 26.10.2015)

[4]. Rabiner L., Schafer R. Theory and Applications of Digital Speech Processing, *Prentice-Hall*, 2011

[5]. Glottal signal, vocal tract resonances and output sound. URL: http://newt.phys.unsw.edu.au/jw/glottis-vocal-tract-voice.html (дата обращения 29.10.2015)

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Гуров Станислав Геннадьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: gurov.it@mail.ru

А.М. Донецков, М.И. Калупин

ИССЛЕДОВАНИЕ СКОРОСТИ ВЫПОЛНЕНИЯ ПРОГРАММ НА АССЕМБЛЕРЕ И ЯЗЫКАХ ВЫСОКОГО УРОВНЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Как известно, одним из главных плюсов языка программирования ассемблер является его скорость работы. Связано это с тем, что ассемблер предоставляет полноценную возможность работы с процессором, что, во-первых, позволяет достигать максимальной скорости выполнения программы, и во-вторых, позволяет достичь преимущества в размере конечного кода программ.

Высокоуровневые языки, несмотря на наличие возможности выполнения некоторых низкоуровневых операций, требуют добавления в основной код программы кода на языке ассемблера, путём, так называемой, ассемблерной вставки.

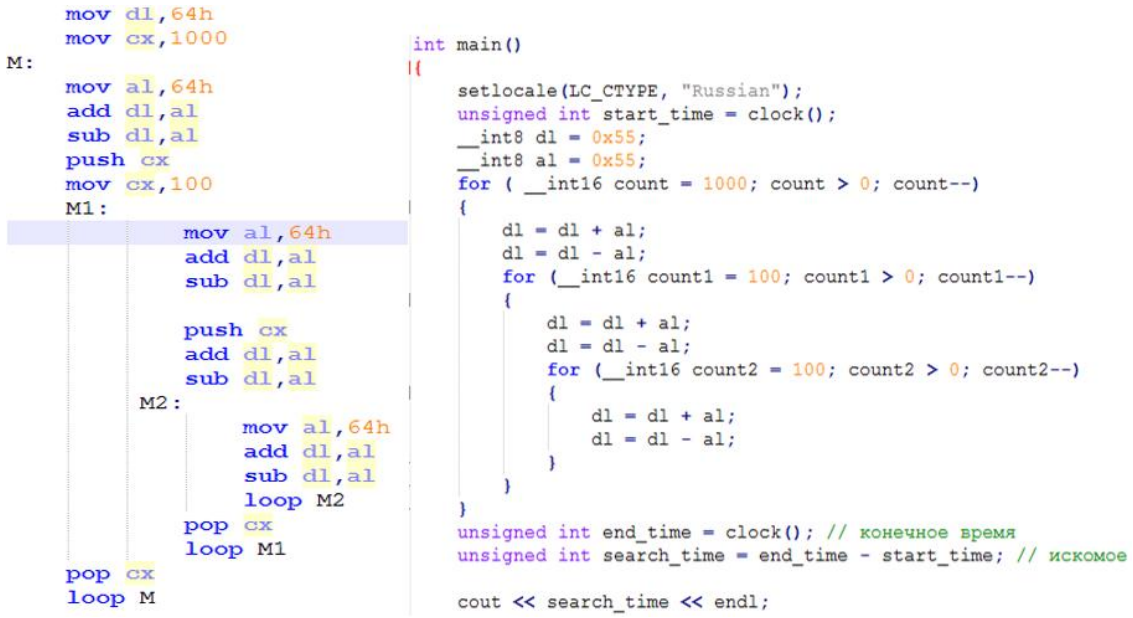
Благодаря мощностям современных компьютеров, разница в выполнении кода на языках программирования высокого уровня и низкого практически не заметна. Но на практике все же можно узнать эти различия.

Используем две одинаковые программы, написанные на разных языках программирования, а именно ассемблер(tasm) и C++, и определим скорость выполнения каждой из программ.

На языке высокого уровня, а именно C++ программа с использованием функций сложения и вычитания в цикле на десять миллионов операций затрачивает в среднем 52 миллисекунды (Рисунок 1).

При запуске программы, используя ассемблерную вставку в C++, выполнение программы заняло 21 миллисекунду (Рисунок 1). Что более чем в два раза превышает скорость выполнения аналогичной программы написанной на “чистом” коде C++.

Интересно заметить, что при использовании программы DosBox, частично эмулирующей операционную среду MS-DOS и аппаратную часть IBM PC, ассемблерная программа выполняется 7 секунд. Что намного больше чем в предыдущих случаях. Это связано с особенностями эмуляции DosBox.



```
    mov dl,64h
    mov cx,1000
M:
    mov al,64h
    add dl,al
    sub dl,al
    push cx
    mov cx,100
    M1:
        mov al,64h
        add dl,al
        sub dl,al

        push cx
        add dl,al
        sub dl,al
      M2:
            mov al,64h
            add dl,al
            sub dl,al
            loop M2
        pop cx
        loop M1
    pop cx
    loop M
```

```
int main()
{
    setlocale(LC_CTYPE, "Russian");
    unsigned int start_time = clock();
    __int8 dl = 0x55;
    __int8 al = 0x55;
    for ( __int16 count = 1000; count > 0; count--)
    {
        dl = dl + al;
        dl = dl - al;
        for (__int16 count1 = 100; count1 > 0; count1--)
        {
            dl = dl + al;
            dl = dl - al;
            for (__int16 count2 = 100; count2 > 0; count2--)
            {
                dl = dl + al;
                dl = dl - al;
            }
        }
    }
    unsigned int end_time = clock(); // конечное время
    unsigned int search_time = end_time - start_time; // искомое

    cout << search_time << endl;
```

Рис. 1. Программа с использованием функций сложения и вычитания (язык ассемблера - слева, C++ - справа)

Используя в C++ с ассемблерную вставку, программа с использованием функций умножения и деления (mul/div) в цикле из десяти миллионов операций затрачивает 92 миллисекунды. С использованием эмулятора DosBox затрачивается 14 секунд. Эта же программа на “чистом” коде C++ затрачивает 136 миллисекунд.

Из проделанных опытов, можно сделать вывод, что даже не смотря на современные мощности персональных компьютеров, различия в скорости выполнения программа написанных на ассемблере и языках высокого уровня довольно значительные. При написании программ, требующих высокого быстродействия не следует пренебрегать ассемблерным кодом. Ассемблер будет актуален еще очень долгое время.

Донецков Анатолий Михайлович – канд. техн. наук, старший преподаватель КФ МГТУ им. Н.Э. Баумана. E-mail: dam@kaluga.ru

Калупин Максим Игоревич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: maksim.kalupin@gmail.com

В.Н. Власов, К.М. Гришанов, С.В. Нифонтов, А.Н. Проскурнин

ИТЕРАЦИОННОЕ РЕШЕНИЕ ЗАДАЧИ ВЗАИМОДЕЙСТВИЯ ДИСЛОКАЦИЙ С ДИСЛОКАЦИОННЫМИ СКОПЛЕНИЯМИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Особенности пластической деформации и деформационного упрочнения кристаллических материалов в существенной степени определяются способностью прохождения скользящих дислокаций через различие дислокационные скопления. Анализу данного вопроса посвящен целый ряд работ, при этом используются различные уровни приближения. Поскольку самодействие дислокаций может оказывать существенное влияние на исследуемые процессы, в настоящей работе рассмотрена задача о прохождении гибких дислокаций через дислокационные сетки при строгом учете, как самодействия дислокации, так и тонкой структуры полей внутренних напряжений, создаваемых дислокационными сетками.

Схема, иллюстрирующая расположение плоского дислокационного скопления и взаимодействующей с ним гибкой дислокации, приведена на рис. 1. Скопление состояло из двух бесконечных рядов винтовых дислокаций, расположенных в плоскости (111). Дислокации ряда 1 имели векторы Бюргерса $\vec{b}_1 = \frac{1}{2}a[\bar{1}01]$ и пересекали плоскость базиса в точках, отстоящих друг от друга на расстоянии L_1. Дислокации ряда 2 были параллельны плоскости $(\bar{1}11)$, имели векторы Бюргерса $\vec{b}_2 = \frac{1}{2}a[101]$ и находились на расстоянии L_2 друг от друга. Скользящая дислокация считалась гибкой, располагалась в плоскости $(\bar{1}11)$, $Z = const$ и имела вектор Бюргерса $\vec{b} = \frac{1}{2}a[\bar{1}0\bar{1}]$. Было рассмотрено два случая, когда дислокации ряда 1 на скользяще дислокацию оказывают отталкивающее действие, а дислокации ряда 2 - притягивающее, и наоборот.

Под действием однородного внешнего напряжения возможно движение скользящей дислокации из бесконечности, где она имеет винтовую ориентацию, к плоскому скоплению и проникновение через него. Процесс движения гибкой дислокации рассматривался в квазистатическом приближении, т.е. принималось, что при изменении уровня внешнего напряжения базисная дислокация успевает принять равновесную форму.

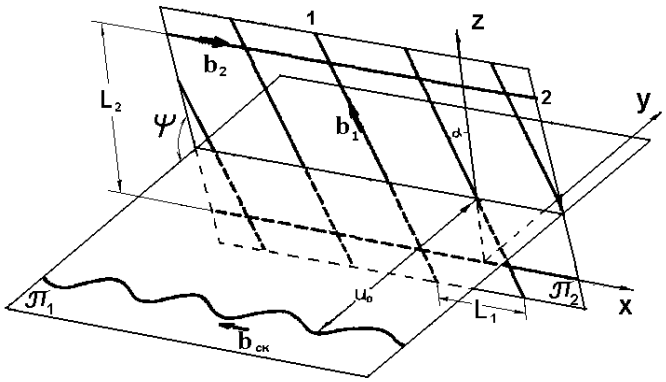


Рис. 1. Схема расположения взаимодействующих дислокаций

При заданном уровне внешнего напряжения τ равновесная форма гибкой дислокации $U(x)$ определялась как решение уравнения (1):

$$F_i^{BH} + \sum_{i \neq j} F_{ij}^{B3} + F_i^C - F_i^{TP} = 0 \quad ; \; i, j = 1,2,\ldots,k \; , \qquad (1)$$

где F_i^{BH} - внешняя сила, действующая на *i*-ую дислокацию; F_{ij}^{B3} - сила, с которой *j*-ая дислокация действует на *i*-ую дислокацию; F_i^C - сила самодействия *i*-ой дислокации; F_i^{TP} - сила сопротивления движению *i*-ой дислокации со стороны решетки.

Для решения задачи была выбрана система координат, плоскость XOY которой являлась компланарной плоскости скольжения пробной дислокации $(\bar{1}11)$ - плоскости π_1 , при этом самой плоскости π_1 соответствовала плоскость Z=const. Дислокации сетки располагались в плоскости (111) - π_2 . Сетка характеризовались параметрами L_1 - расстоянием между дислокациями первого сорта и L_2 - расстоянием между дислокациями второго сорта.

Равновесная форма скользящей дислокации определялась в виде: Y=U(x). При этом значения функции U(x) в точках X= n·L_1 , где $n = 0,\pm1,\pm2,...$ характеризуют меру приближения скользящей дислокации к дислокационной сетке, а значения функции U(x) в точках X= $\left(\frac{2n+1}{2}\right)\cdot L_1$, где $n = 0,\pm1,\pm2,...$ характеризуют степень искривленности гибкой скользящей дислокации. Относительное содержание в сетке дислокаций разного сорта является значимой характеристикой определяющей особенности взаимодействия скользящей дислокации с дислокационной сеткой. Для оценки относительного содержания дислокаций разного сорта была выбрана величина æ=$(1-L_1/L_2)$. Когда дислокаций первого сорта мало, величина L_1 большая и в пределе æ → (– ∞). Когда дислокаций второго сорта мало, величина L_2 большая и в пределе æ → +1 Особенности взаимодействия скользящей дислокации с дислокационной сеткой зависят от относительного расположения плоскости расположения

скользящей дислокации, то есть другой значимой характеристикой процесса взаимодействия является величина Z/L_2.

В целях удобства и наглядности анализ задачи поводился в безразмерных единицах $\frac{X}{L_1}$, $\frac{Y}{L_1}$, $\frac{U(0)}{L_1}$, $\frac{U(0,5)}{L_1}$, $\frac{Z}{L_2}$, $\tau \cdot L_1$, æ=(1-$\frac{L_1}{L_2}$). Физические характеристики выбирались применительно к кристаллам меди: вектор Бюргерса b=2,56·10^{-10}м; модуль сдвига G=54,6 ГПа; коэффициент Пуассона ν=0,32; $\psi = \arccos(-1/4\sqrt{6}) \cong 95{,}86^0$; значения стартового напряжения f_i^0=0,28 МПа.

При рассмотрении взаимодействия скользящих дислокаций со скоплениями может встретиться два варианта, когда L_1 сохраняется постоянным, а L_2 изменяется и обратный вариант. Настоящая модель допускает рассмотрение обоих этих вариантов. Первый вариант соответствует ситуации, когда расстояние $L_1 = L_1^* = Const$, а L_2 меняется от ∞ до 0. Во втором варианте $L_2 = L_2^* = Const$, а L_1 меняется от ∞ до 0. Изменение расстояний L_1 и L_2 по-разному меняет величину и знак нескомпенсированной дальнодействующей компоненты поля дислокационной сетки. Случай æ=+1 соответствует ситуации, когда существует только ряд 1, создающий отталкивающее (в случае $a > 0$) или притягивающее (в случае $a < 0$) дальнодействующее напряжение. При æ =0 соотношение плотностей в двух рядах дислокаций $L_2^* / L_1^* = K_\circ$ таково, что дислокационная сетка не создает дальнодействующего поля напряжений. Отрицательные значения æ отвечают притягивающему (при $a > 0$) и отталкивающему (при $a < 0$) дальнодействующему полю. При $L_1 = L_1^*$ можно получить совокупность решений для первого варианта, а для нахождения решения для второго варианта по известному первому достаточно L_2 положить равным $L_2^* = Const$ и заменить на $L_2^*(1-æ)/K_\circ$, τL_1 на $\tau L_2^* / K_\circ$, где $K_\circ = L_2^* / L_1^*$. Вклад в самодействие учитывался на интервале, соответствующем трем “волнам” оправа и слева от рассматриваемого участка дислокационной линии. Контрольные расчеты показали, что вклад в самодействие более отдаленных участков дислокации оказывается меньше точности расчетов, принятой при решении настоящей задачи. Отметим также, что в условиях настоящей задачи, когда имело место формирование четверных дислокационных узлов, во избежание раскачивания решения приходилось использовать мелкие итерационные шаги. В результате сходимость итерационного процесса с точностью до 10^{-2} н·м$^{-1}$ достигалась за ~400 шагов.

Власов Виктор Николаевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: vnvlasov@mail.ru

Гришанов Кирилл Михайлович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: cyrilgrishanov94@gmail.com

Нифонтов Сергей Викторович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: nifontow.serezha@yandex.ru

Проскурнин Андрей Николаевич- канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: an.proskur@yandex.ru

С.С. Гришунов, А.В. Бурмистров

МАТЕМАТИЧЕСКИЕ МОДЕЛИ, ИСПОЛЬЗУЕМЫЕ В СИСТЕМАХ РАСПОЗНАВАНИЯ ДИКТОРА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Введение. Распознавание диктора является биометрическим методом верификации пользователя, использующим индивидуальные речевые особенности человека [1]. В технологиях распознавания диктора существуют 3 основных подходах. Первый подход заключается в использовании долгосрочных усреднений акустических характеристик, таких как спектр речевого сигнала или уровень частот. Такой подход использовался на ранних этапах развития систем верификации по голосу. Путем усреднения других факторов, влияющих на акустические характеристики, таких как вариации фонем, можно также получить информацию, связанную с диктором. Однако процесс усреднения снижает уровень информации, зависящей от диктора, а стабильная статистика может быть получена только из достаточно продолжительного сегмента речи [2].

Второй и наиболее распространенный подход заключается в построении модели для каждого диктора, используя дикторозависимые характеристики. Сравнивая акустические характеристики, поданные на вход, и сохраненные характеристики, можно различить дикторов. К этому типу относятся такие модели как модель квантования векторов, модель гауссовых смешений, скрытые модели Маркова.

Третий подход заключается в использовании для различения дикторов специальных методов, например нейронных сетей или машины опорных векторов [3].

Vector Quantization (VQ) - квантование векторов. Идея квантования векторов заключается в генерации специального словаря, использующегося для распределения дискретных наборов векторов речевых характеристик. Используя векторы характеристик $a_1, a_2, .., a_I$, которые характеризуют возможные значения характеристик диктора, можно разделить пространство векторов характеристик S на M частей. Каждое разделение пространства должно формировать выпуклые неперекрывающие друг друга области. Каждая часть пространства S_i характеризуется соответствующим центральным вектором b_i. Разбиение совершается так, чтобы минимизировать среднее искажение по всему обучающему набору. Среднее искажение определяется по формуле:

$$D = \frac{1}{I}\sum_{i=1}^{I} \min_{1 \le j \le M} d\left(a_i, b_j\right) \tag{1}$$

где $d\left(a_i, b_j\right)$ это расстояние между векторами a_i и b_j.

На стадии обучения, собирая вектора характеристик дикторов, формируется словарь. На стадии распознавания находятся средние расстояния между векторами характеристик и средними векторами. Для принятия окончательного решения сравниваются *M* средних искажений. Окончательное решение определяется по формуле:

$$i^* = \arg\min_{1 \le i \le M} D^i \tag{2}$$

Gaussian Mixture Model (GMM) – модель гауссовых смешений. Модель гауссовых смешений представляет собой взвешенную сумму *M* компонентов плотности распределения составляющих модели:

$$p\left(\vec{x} \mid \lambda\right) = \sum_{i=1}^{M} p_i b_i\left(\vec{x}\right),$$

где $\vec{x}$ - вектор характеристик размерности *D*, p_i - веса смешения, удовлетворяющие условию $\sum_{i=1}^{M} p_i = 1.$

Каждый компонент является *D*-мерной гауссовой функцией распределения:

$$b_i\left(\vec{x}\right) = \frac{1}{\left(2\pi\right)^{D/2}\left|Cov_i\right|^{1/2}} \exp\left\{-\frac{1}{2}\left(\vec{x} - \vec{\mu}_i\right)' \sum_{i}^{-1}\left(\vec{x} - \vec{\mu}_i\right)\right\} \tag{3}$$

где $\vec{\mu}_i$ вектор математического ожидания, Cov_i — ковариационная матрица.

Плотность распределения модели смешения гаусса определяется векторами математического ожидания, ковариационными матрицами и весами для каждого компонента модели. Эти параметры все вместе записываются в виде

$$\lambda = \left\{p_i, \mu_i, Cov_i\right\}$$

В задаче распознавания диктора каждый диктор представляется в модели своим параметром λ.

Обучение системы заключается в определении параметров модели, наиболее полно подходящих распределению характеристик диктора. Существует несколько алгоритмов обучения, например алгоритм максимального сходства. На стадии распознавания строятся модели для каждого диктора, используя входной вектор и параметр λ. Далее необходимо определить какая модель наиболее подходит входным характеристикам, т.е. нужно найти максимальную вероятность принадлежности характеристик диктору. Результат можно получить по формуле:

$$\hat{S} = \arg\max_{1 \le k \le S} \sum_{t=1}^{T} p\left(\vec{x}_t \mid \lambda_k\right) \tag{4}$$

Hidden Markov Models (HMM) – скрытые модели Маркова. Положим $s_i, i \ge 1$ состояния модели. Если допустимы все возможные переходы состояний из s_i в s_j, такая модель называется эргодической. Эргодические марковские модели применяются в текстонезависимом определении диктора, в случае зависимости от текста используются модели, в которых допустимы только хронологические переходы состояний (слева направо). Скрытые модели Маркова отличаются от обычных тем, что в таких моделях неизвестна последовательность состояний, известны только наблюдаемые результаты.

Скрытая модель Маркова характеризуется:

1) количеством возможных состояний *N*;

2) вероятностью перехода состояния:

$$A = \left\{a_{ij}\right\} = P\left[\, q_t = S_j \mid q_{t-1} = S_i \,\right],$$

где q_t - состояние системы в момент *t*;

3) вероятностью наблюдаемого символа в *j*-м состоянии $B = b_j(k)$;

4) начальной вероятностью состояния $\pi = \pi_i = P\left(q_1 = S_i\right)$

Эти параметры все вместе записываются в виде

$$\lambda = \left\{A,\, B,\, \pi\right\}$$

Обучение системы заключается в определении параметров модели, наиболее полно подходящих распределению характеристик диктора. Наиболее распространенными являются алгоритмы обучения Баума-Уэлча и алгоритм Витерби [5]. Оба этих алгоритма основаны на критерии максимального подобия.

На стадии распознавания вычисляются вероятности наблюдения *O* на основе каждой из моделей, далее вычисляется вероятность *i*-ой модели:

$$P(S_i \mid O) \approx \frac{P(O \mid S_i)}{\sum_j P(O \mid S_j)} \tag{5}$$

Максимальная из вероятностей определяет диктора.

Support Vector Machine (SVM) – машина опорных векторов. Машина опорных векторов – это двоичный классификатор, который принимает решение путем построения линейной (плоскостной или гиперплоскостной) границы, разделяющей классы [4]. Гиперплоскость описывается уравнением:

$$\vec{x} \cdot \vec{\omega} + b = 0 \tag{6}$$

где $\vec{\omega}$ - нормаль к поверхности

Подставив в уравнение плоскости точку, по знаку результата можно определить с какой стороны от плоскости лежит точка, т.е. к какому классу она относится.

Гиперплоскость выбирается согласно критерию максимального запаса, т.е. выбирается такая разделяющая плоскость, которая максимизирует расстояние до ближайшей точки по обе стороны от плоскости. Это достигается путем минимизации квадрата нормы вектора $\vec{\omega}$, удовлетворяющих неравенству $(\vec{x}_i \cdot \vec{\omega} + b)\, y_i \geq 1$ для всех i. Решение $\vec{\omega}_0$ - это линейная комбинация небольшого подмножества данных $\vec{x}_s$, $S \in \{1, ..., N\}$, называемого опорными векторами. Для опорных векторов выполняется равенство $(\vec{x}_s \cdot \vec{\omega}_0 + b)\, y_s = 1$.

Не всегда возможно разделить объекты гиперплоскостью, чтобы избавиться от этого недостатка вводят переменные погрешности ε_i. Тогда минимизировать нужно выражение:

$$\|\vec{\omega}\|^2 + C\sum_i L(\varepsilon_i) \tag{7}$$

где C – параметр риска, L – функция потери (в самом простом варианте $L(\varepsilon_i) = \varepsilon_i$)

Вывод. Были рассмотрены классические модели систем распознавания диктора. Большинство современных систем основано на третьем подходе, использующем для определения диктора специальные методы классификации. Широкое распространение получили системы, основанные на машинах опорных векторов и на нейронных сетях.

Список литературы

[1]. Степаненков М.В., Белов Ю.С. Распознавание личности по голосу: аналитический обзор. Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе. Т. 2. КФ МГТУ им. Н.Э. Баумана. Калуга, изд-во КФ МГТУ им. Н.Э. Баумана, 2015, с. 265-275.

[2]. Аграновский А.В., Леднов Д.А. Математическая модель распознавания речи с использованием протяженных контекстов. Наука и образование, 2004, вып. 11. URL: http://technomag.bmstu.ru/doc/46690.html (дата обращения 18.10.2015).

[3]. Miller D., Top D. Voice biometrics 2010: A transformative year for voice-based authentication. OpusResearch, 2010, N5. URL: http://opusresearch.net/wordpress/2010/05/13/voice-biometrics-2010-a-transformative-year-for-voice-based-authentication/ (accessed 20 October 2015).

[4]. Hautamäki V., Kinnunen T., Nosratighods M., Lee K.-A., Ma B., Li H. Approaching Human Listener Accuracy with Modern Speaker Verification. Interspeech, 2010, pp. 1473-1476.

[5]. Sorokin V.N., Tsyplikhin A.I. Speaker verification using the spectral and time parameters of voice signal. Journal of Communications Technology and Electronics, 2010, v.55, N12, pp. 1561-1574.

Гришунов Степан Сергеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: stepangrishunov@yandex.com

Бурмистров Александр Викторович – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: gold_medalist@hotmail.com.

Ю.С. Белов, Р.В. Либеров, Б.М. Логинов, Р.В. Клюквин

МОДЕЛИРОВАНИЕ КОНТАКТНОГО ВЗАИМОДЕЙСТВИЯ СКОЛЬЗЯЩИХ ДИСЛОКАЦИЙ С ДИСЛОКАЦИОННЫМИ ПЕТЛЯМИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В процессе радиационного облучения конструкционных материалов образуется большое количество дислокационных петель, взаимодействие которых со скользящими дислокациями может приводить к комплексным дислокационным образованиям. Для чисто краевой дислокационной петли в плоскости ее залегания поле напряжений во всех точках, за исключением точек на дислокационной линии, обращается в нуль. Поэтому в данных условиях возможно контактное взаимодействие скользящей дислокации с призматической петлей, хотя дислокационная реакция и не протекает. Исследование подобного контактного взаимодействия скользящей и призматической дислокаций в силу специфического закона распределения сдвиговых напряжений дислокационной петли в плоскости ее залегания представляет определенные трудности и требует специального рассмотрения.

Разновесные конфигурации $y(x)$ гибкой дислокации в поле дислокационной петли при наличии однородного внешнего напряжения τ_{yz} определяются из условия минимума полной энергии U системы:

$$U = \int_{-x^*}^{x^*} E(y')\sqrt{1+(y')^2}\,dx - \int_S\int b\left[\left(\tau_{xz}{}^{\perp} + \tau''_{xz}\right)\cos\beta + \left(\tau_{yz}{}^{\perp} + \tau''_{yz}\right)\sin\beta\right]dS - \int_S\int b\tau_{yz}\sin\beta\,dS \qquad (1)$$

где $E(y')$ – погонная энергия гибкой дислокации, $\tau_{xz}{}^{\perp}$, $\tau_{yz}{}^{\perp}$ и τ''_{xz}, τ''_{yz} – сдвиговые напряжения, создаваемые краевой и сдвиговой компонентами дислокационной петли с векторами Бюргера $\overrightarrow{b^{\perp}}$ и $\overrightarrow{b''}$. Поскольку выражение для сдвиговых напряжений $\tau_{YZ}^{\perp}$ краевой дислокационной петли при $\upsilon \to 0$ имеет особенность на линии $u = 1$, равновесные конфигурации гибкой дислокации не могут быть получены из уравнения равновесия подстановкой значения $\upsilon = 0$. Они должны определяться как предельные состояния гибкой дислокации при $\upsilon \to 0$. При этом структура особенности сдвиговых напряжений $\tau_{YZ}^{\perp}$ такова, что в отличие от уравнения равновесия, для полной энергии U системы при $\upsilon \to 0$ никаких особенностей не имеет. Поэтому поиск предельных равновесных конфигураций гибкой

дислокации удобнее производить минимизируя полную энергию U системы. Для полной энергии системы U при любом сколь угодно малом, но конечном $\upsilon = \pm\varepsilon,\ \varepsilon > 0$, выражение (1) может быть записано в виде:

$$U = \int_{-x^*}^{x^*} E(y')\sqrt{1+(y')^2}\,dx - \iint_S b\tau_{yz}^{\perp} dS - \iint_S b\tau_{yz} dS \tag{2}$$

Обычно при определении энергии дислокаций в заданном поле напряжений под S понимают площадь, заметаемую дислокацией при переходе из одного состояния в другое. В этом случае S соответствует площади, ограниченной дислокационной кривой $y_1(x)$ и осью X, т.е. поверхностный интеграл в (2) по dx должен вычисляться от $-x^*$ до x^*, а по dy – от 0 до $y_1(x)$.

Сдвиговые напряжения краевой дислокационной петли в (2) при малом $\upsilon = \pm\varepsilon,\ \varepsilon > 0$ задаются соотношением:

$$\tau_{YZ}^{\perp} = \pm\frac{Gb^{\perp}\sin\alpha}{2\pi R_0(1-\nu)}\left\{-\frac{\varepsilon\left[\ln 4(1+u) - \ln\sqrt{(1-u)^2+\varepsilon^2}\right]}{(1+u)\left[(1-u)^2+\varepsilon^2\right]}\left[\frac{(1-u)^2}{u} + \frac{\varepsilon^2(1+u^2)}{u(1+u)^2}\right] - \right.$$
$$\left. - \frac{\varepsilon}{(1+u)\left[(1-u)^2+\varepsilon^2\right]}\left[3u - \frac{1}{u} - \frac{4u\left(\varepsilon+u^2-1\right)^2}{(1+u)^2\left[(1-u)^2+\varepsilon^2\right]}\right]\right\} \tag{3}$$

Знаки $\pm$ относятся к случаям $\upsilon = \pm\varepsilon$, соответственно. В приближении постоянного линейного натяжения выражение (2) в безразмерных цилиндрических координатах u, α, υ можно преобразовать к виду:

$$\overline{U}(\upsilon = \pm\varepsilon) = \chi\overline{L} - \overline{\tau}\,\overline{S} - \int_{\tau}\left[\int \overline{\tau_{YZ}^{\perp}} u\,du\right]d\alpha, \tag{4}$$

где $\overline{U} = \dfrac{U}{\left(Gbb^{\perp}R_0/2\pi(1-\nu)\right)}$, $\chi = \dfrac{2k\pi(1-\nu)b}{b^{\perp}}$, $\overline{L} = \dfrac{L}{R_0}$, $\overline{S} = \dfrac{S}{R_0^2}$,

$d\overline{S} = u\,du\,d\alpha$. Интегрирование по α в (4) проводится по всем углам α, для которых существует $u_1(\alpha)$.

Вычислим энергию $\overline{U}^{\perp}$ гибкой дислокации в поле краевой дислокационной петли, определяемую в выражении (4). Согласно (3), $\overline{U}^{\perp}(\upsilon = \pm\varepsilon)$ равна сумме двух интегралов I_1 и I_2:

$$\overline{U}^{\perp}\left(\upsilon=\pm\varepsilon\right)=-\iint_{S}\overline{\tau_{YZ}^{\perp}}ududa=I_1+I_2=$$

$$=\pm\left\{\int_0^{\pi}\int_0^{u_1(\alpha)}-\frac{\varepsilon\sin\alpha\left[\ln 4\left(1+u\right)-\ln\sqrt{\left(1-u\right)^2+\varepsilon^2}\right]}{\left(1+u\right)\left[\left(1-u\right)^2+\varepsilon^2\right]}\left[\frac{\left(1-u\right)^2}{u}+\frac{\varepsilon\left(1+u^2\right)}{u\left(1+u\right)^2}\right]ududa+\right.$$

$$\left.+\int_0^{\pi}\int_0^{u_1(\alpha)}-\frac{\varepsilon\sin\alpha}{\left(1+u\right)\left[\left(1-u\right)^2+\varepsilon^2\right]}\left[3u-\frac{1}{u}-\frac{4u\left(\varepsilon^2+u^2-1\right)^2}{\left(1+u\right)^2\left[\left(1-u\right)^2+\varepsilon^2\right]}\right]ududa\right\} \qquad (5)$$

Из (5) видно, что в общем случае энергия гибкой дислокации в поле краевой дислокационной петли при $\upsilon=\pm\varepsilon,\ \varepsilon>0$ должна зависеть от того, каким образом гибкая дислокация размещается в области, где $\tau_{YZ}^{\perp}\neq 0$. Подынтегральная функция в первом интеграле I_1 соотношения (5) при $\varepsilon\to 0$ имеет предел, не зависящий от характера стремления к дислокационной линии, и равномерно сходится. Поэтому, при вычислении этого интеграла при $\varepsilon\to 0$, можно знак предела внести под знак интеграла. Тогда, учитывая что:

$$\lim_{\varepsilon\to 0}\frac{\varepsilon}{\left(1-u\right)^2+\varepsilon^2}=\pi\delta\left(1-u\right)$$

найдём:

$$\lim_{\varepsilon\to 0}I_1=\pm\int_0^{\pi}\int_0^{u_1(\alpha)}-\frac{\pi\delta\left(1-u\right)\sin\alpha}{\left(1+u\right)}\left[\ln 4\left(1+u\right)-\ln\left|1-u\right|\right]\left(1-u\right)^2 dud\alpha .$$

Воспользовавшись свойствами δ- функции, нетрудно показать, что для любой дислокационной конфигурации $u_1(\alpha)$ $\lim_{\varepsilon\to 0}I_1=0$. Следовательно:

$$\overline{U}^{\perp}\left(\upsilon=\pm\varepsilon\right)=I_2=$$

$$\pm\int_0^{\pi}\int_0^{u_1(\alpha)}-\frac{\varepsilon\sin\alpha\ ududa}{\left(1+u\right)\left[\left(1-u\right)^2+\varepsilon^2\right]}\left[\frac{3u^2-1}{u}-\frac{4u\left(\varepsilon^2+u^2-1\right)^2}{\left(1+u\right)^2\left[\left(1-u\right)^2+\varepsilon^2\right]}\right] \qquad (6)$$

Таким образом, выражение для полной энергии системы в случае взаимодействия гибкой дислокации с призматической дислокационной петлёй при $\upsilon=\pm\varepsilon,\ \varepsilon\to 0$ приобретает вид:

$$U\left(\underset{\varepsilon\to 0}{\upsilon=\pm\varepsilon}\right)=\chi\overline{L}-\overline{\tau}\overline{S}+\lim_{\varepsilon\to 0}I_2 \qquad (7)$$

Различные возможные равновесные конфигурации гибкой дислокации в общем случае должны получаться автоматически, путём минимизации энергии системы $\overline{U}$ (7). В силу симметрии расположения точек

закрепления гибкой дислокации относительно центра призматической дислокационной петли и симметрии поля $\tau_{YZ}^{\perp}$ нет смысла вычислять энергию взаимодействия гибкой дислокации с дислокационной петлёй для произвольной формы гибкой дислокации. Поэтому сначала задавался один тип физически допустимой конфигурации гибкой дислокации, совместимый с симметрией задачи. Затем находилась энергия системы, отвечающая выбранному типу дислокационной кривой. Путём ее минимизации устанавливалась возможность существования данной конфигурации, а также её параметры. Таким образом, путём перебора возможных физически допустимых форм можно было отобрать конфигурации гибкой дислокации, которые могут реально существовать, а также определить их параметры.

Анализ различных конфигурации гибкой дислокации, с точки зрения рассматриваемой задачи, показал наличие трех δ - образных пика внутренних напряжений $\tau_{YZ}^{\perp}$, которые «чередуются» в радиальном направлении в определённой последовательности, как по высоте, так и по знаку.

Благодаря симметрии сдвиговых напряжений $\tau_{YZ}^{\perp}$ относительно оси $\overline{Y}$ и асимметрии относительно оси $\overline{X}$, энергии $\overline{U}^{\perp}$ для симметричных конфигураций гибкой дислокации должны быть одинаковы при противоположных направлениях действующего внешнего напряжения. Вместе с тем, при $\upsilon = -\varepsilon, \varepsilon \to 0$ сдвиговые напряжения $\tau_{YZ}^{\perp}$ противоположны по знаку соответствующим значениям $\tau_{YZ}^{\perp}$, при $\upsilon = +\varepsilon, \varepsilon \to 0$. Поэтому характер взаимодействия скользящей дислокации с краевой дислокационной петлёй для $\upsilon = +\varepsilon, \varepsilon \to 0$ должен в принципе отличаться от ситуации при $\upsilon = -\varepsilon, \varepsilon \to 0$. Таким образом, для определения возможных конфигураций гибкой дислокации, достаточно рассмотреть конфигурации в области $\overline{y} > 0$ при $\overline{\tau} \geq 0$ и $\overline{\tau} \leq 0$, либо в области $\overline{y} > 0$ при $\overline{\tau} \geq 0$ и $\overline{y} < 0$ при $\overline{\tau} \geq 0$.

Все конфигурации гибкой дислокации можно разделить на несколько серий. Серия A отвечает случаям, когда гибкая дислокация не соприкасается с призматической дислокационной петлёй, либо пересекает её. Серии B и C соответствуют случаям, когда гибкая дислокация взаимодействует на некотором участке с кольцевыми пиками $\tau_{YZ}^{\perp}$.

Анализ особенностей дислокационных взаимодействий показал, что при образовании гибкой конфигурации типа А работа $\overline{U}^{\perp}$ против поля петли не совершается. Физически это определяется тем обстоятельством, что поле, создаваемое в плоскости $\upsilon = 0$, является самоуравновешенным. Поэтому, и в данном случае полная энергия U при $\upsilon = \pm\varepsilon, \varepsilon \to 0$ для

рассматриваемых конфигураций определяется собственной энергией дислокации и работой против сил внешнего поля (3.9).

Таким образом, если гибкая дислокация при $\upsilon = 0$ пересекает призматическую дислокационную петлю, между ними не происходит никакого взаимодействия. Поведение гибкой дислокации во внешнем поле напряжений в этом случае будет таково, как будто петля отсутствует.

Более сложно обстоит дело с нахождение конфигурации гибкой дислокации типа B и C, когда некоторая часть дислокации взаимодействует с особенностями сдвиговых напряжений $\tau_{YZ}^{\perp}$ дислокационной петли. Энергия $\overline{U}^{\perp}$ гибкой дислокации в поле краевой дислокационной петли будет зависеть от того, каким образом гибкая дислокация располагается внутри указанной области. Для определения параметров равновесных конфигураций B и C гибкой дислокации производилась вариация $\overline{U}$ по γ и φ. Полученные результаты показали, что минимуму полной энергии $\overline{U}$ отвечают конфигурации B_{21}, C_{12} $(\gamma = 1)$ для $\upsilon = +\varepsilon, \varepsilon \to 0$ и конфигурации B_{32}, C_{23} $(\gamma = 2)$ для $\upsilon = -\varepsilon, \varepsilon \to 0$. Следовательно, указанные решения должны быть устойчивыми. К аналогичному заключению можно придти и на основе качественного анализа сил, действующих на гибкую дислокацию в окрестности положения равновесия. Действительно, отклонение дислокаций от положений B_{21}, C_{12} при $\upsilon = +\varepsilon, \varepsilon \to 0$ и B_{32}, C_{23} при $\upsilon = -\varepsilon, \varepsilon \to 0$ должно приводить к возникновению сил, стремящихся вернуть гибкую дислокацию в исходное состояние.

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Либеров Роман Владимирович – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: rliberov@yandex.ru

Логинов Борис Михайлович – д-р физ.-мат. наук, зав. каф. КФ МГТУ им. Н.Э. Баумана. E-mail: loginov@kaluga.ru

Клюквин Роман Владимирович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: pomanklg@gmail.com

С.В. Нифонтов, Ю.С. Белов

ОБЗОР КЛАССИФИКАЦИЙ СИСТЕМ РАСПОЗНАВАНИЯ ДИКТОРА ПО ГОЛОСУ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Ведение. Каждый человек индивидуален, в частности индивидуальны его голосовые характеристики. Индивидуальность акустических голосовых характеристик определяется механикой колебаний голосовых складок, анатомией речевого тракта и системой управления артикуляцией [1].

Люди способны в процессе общения подсознательно различать голоса других людей, но для вычислительной техники это является нетривиальной задачей.

Исследования задач распознавания личности по голосу начались более сорока лет назад, однако в настоящее время исследования в этой области продолжаются, являются актуальными и могут найти практическое применение в следующих сферах:

— судебные экспертизы;
— разведка;
— безопасный доступ к различным ресурсам.

В зависимости от конкретных задач выделяют системы верификации и идентификации диктора.

Идентификация – процесс определения личности сравнением данного образца голоса диктора с шаблонами из базы данных. Результат идентификации – имя зарегистрированного в системе человека, шаблон которого является наиболее вероятно соответствующим входному образцу.

Верификация – процесс идентификации личности путем сравнения образца голоса диктора с хранимым в базе шаблоном. При верификации вместе с голосом также передается идентификатор личности, с помощью которого определяется шаблон сравнения. Результатом верификации – подтверждение или отрицание личности.

Системы распознавания личности по голосу также делятся на текстозависимые и текстонезависимые. В текстозависимых системах используются фиксированные, сгенерированные системой и предложенные пользователю фразы. Текстонезависимые системы обрабатывают произвольную речь.

Системы распознавания состоят из следующих модулей: модуля обработки сигналов, модуля моделей признаков и модуля принятия решений [2].

Модуль обработки сигналов вначале преобразует необработанный сигнал в последовательности векторов признаков, в которых удалены шумы и содержатся существенные для задач распознавания характеристики. В режиме регистрации модуль моделей, используя полученную от первого модуля последовательность векторов признаков, формирует модель пользователя системы. В режиме идентификации вектора признаков, извлеченные из

входного сигнала, сравниваются с хранящимися в базе данных моделями пользователей для определения степени схожести. Модуль принятия решений, используя степень схожести, дает конечный результат.

Выбор речевых характеристик. Невозможно оценить априори какие из речевых характеристик являются наиболее, а какие наименее подходящими для распознавания. Определение наиболее подходящих характеристик осуществляется перебором возможных вариантов признаков с последующей экспериментальной оценкой [3].

В настоящее время выделяются следующие виды речевых характеристик: низкоуровневые (обусловленные анатомическим строением речевого аппарата) и высокоуровневые (приобретённые, связанные с манерой произношения).

При обработке речевого сигнала используется кратковременный анализ - сигнал разбивается на временные окна фиксированного размера (обычно выбирается в пределах 10–30 мс). Предполагается, что в этих окнах параметры сигнала не изменяются. Для повышения точности представления сигнала между окнами делают перекрытие, равное половине длины окна. Затем к каждому окну применяются алгоритмы извлечения признаков, такие как спектральный анализ, метод линейного предсказания или другие.

Модели пользователей. В текстозависимых системах модели пользователей, содержат конкретные фразы, а также включают временные зависимости векторов признаков. В текстонезависимых системах модели пользователей представляют собой распределение признаков, а не временные зависимости [2].

Классические модели делятся на шаблонные модели и стохастические модели (параметрические и непараметрические модели) [4].

В шаблонных моделях, вектора признаков напрямую сравниваются друг с другом, в предположении, что один вектор неточная копия другого. Степень схожести зависит от количества несовпадений. Векторное квантование и алгоритм динамической трансформации временной шкалы– типовые примеры шаблонных моделей.

В стохастических моделях, каждый пользователь представляется заранее неизвестной, но фиксированной функцией плотности вероятности. В режиме обучения происходит оценка параметров функции плотности вероятности в зависимости от обучающей выборки. Идентификация осуществляется путем оценки вероятности исследуемого сигнала по отношению к моделям пользователей. Модель гауссовых смесей и скрытые марковские модели являются наиболее популярными стохастическими моделями [5].

Модели пользователей также разделяются на генеративные и дискриминационные в зависимости от процедуры обучения. Генеративные модели моделируют полученные для обучения данные, например, с помощью оценки функции плотности вероятности (модель гауссовых смесей). Дискриминационные модели основаны на построении границ между пользователями системы.

Методы классификации. Вычисление расстояния – применяется в шаблонных моделях. Самыми распространёнными методами вычисления

расстояния между векторами являются следующие: L1-норма, евклидово расстояние, расстояние Махалонобиса [3].

Метода ближайшего соседа заключается в сравнении каждого вектора тестовой последовательности с каждым вектором шаблона для нахождения минимального расстояния. Для итоговой оценки найденные расстояния усредняются.

В методе векторного квантования в отличие от метода ближайшего соседа множество обучающих векторов не сохраняется полностью, а преобразуется в множество (в основном фиксированного размера) кодовых векторов. Распространённым методом построения такого множества является алгоритм К-средних.

Модель гауссовых смесей широко используется в области распознавания дикторов. Данная модель представляет собой взвешенную сумму Гауссиан [1]:

$$p(x \mid \lambda) = \sum_{i=1}^{M} w_i p_i(x), \qquad (1)$$

где λ – модель диктора, M – количество компонентов модели, w_i – веса компонентов, такие, что $\sum_{i=1}^{M} w_i = 1$.

Функция плотности вероятности каждого компонента определяется формулой:

$$p_i = \frac{1}{(2\pi)^{\mathrm{D}} |\sum_{i=1}|^{\frac{1}{2}}} \exp\left(-\frac{1}{2}(x-\mu_i)^T \sum_{i=1}^{-1} (x-\mu_i)\right), \qquad (2)$$

где D – размерность пространства признаков, μ_i – вектор математического ожидания, $\sum_{i=1}$ – матрица ковариации. Для построения модели диктора необходимо определить векторы средних, матрицы ковариации и веса компонентов. Данную задачу решают с помощью EM-алгоритма (Expectation-maximization algorithm – используется в математической статистике для нахождения оценок максимального правдоподобия параметров вероятностных моделей). На вход подаётся обучающая последовательность векторов $X = \{x_1, ..., x_T\}$. Параметры модели инициализируются начальными значениями, затем на каждой итерации алгоритма происходит переоценка параметров.

Метод опорных векторов является бинарным классификатором, разделяющим модели на два класса гиперплоскостью. При верификации один класс состоит из целевых обучающих векторов (помеченных +1), а другой состоит из обучающих векторов – «самозванцев» (помещенных -1).

С помощью этих векторов находится разделяющая гиперплоскость. Формально, дискриминационная функция имеет вид [2]:

$$f(x) = \sum_{i=1}^{N} \alpha_i t_i K(x, x_i) + d, \quad (3)$$

где $t_i \in \{-1, +1\}$ – эталонные входные значения, $\sum_{i=1}^{N} \alpha_i t_i = 0$ и $\alpha_i > 0$. Опорные векторы x_i, их соответствующие веса α_i и смещение d определяются из обучающего множества в процессе оптимизации, функция ядра имеет вид:

$$K(x, y) = \Phi(x)^{\mathrm{T}} \Phi(y), \quad (4)$$

где $\Phi(x)$ – отображение входного пространства на пространство признаков ядра большей размерности.

Искусственные нейронные сети используются для распознавания различных образов, в том числе и дикторов по речи. Их главное преимущество заключается в том, что три модуля (модуль обработки сигналов, модуль моделей признаков и модуль принятия решений) могут быть объединены в одну простую сеть [5].

Заключение. В настоящее время развитие систем распознавания дикторов по голосу осуществляется по нескольким направлениям. Развитие модуля обработки сигнала происходит, в основном, в направлении поиска новых методов, имеющих робастное представление речевого сигнала (устойчивое к внешним шумам и искажениям) [3]. А методы создания моделей дикторов были развиты от простого усреднения векторов признаков до сложных генеративных и дискриминативных моделей.

Список литературы

[1] Сорокин В.Н., Вьюгин В.В., Тананыкин А.А. Распознавание личности по голосу: аналитический обзор. Информационные процессы, 2012, № 12, с. 1 – 30.

[2] Majetniak A. Tan Z. Speaker recognition using Universal Background Model on YOHO speech database. Aalborg, Aalborg University,2011, 61 p.

[3] Первушин Е.А. Обзор основных методов распознавания дикторов. Математические структуры и моделирование, 2011, № 24, с. 41-54.

[4] Campbell J. Speaker recognition: a tutorial. Proceedings ofthe IEEE, 1997, vol. 85, pp. 1437–1462.

[5] Kinnunen T., Li H. An overview of text-independent speaker recognition: From features to supervectors. Speech communication, 2010, vol. 52, pp. 12-40.

Нифонтов Сергей Викторович- студент КФ МГТУ им. Н.Э. Баумана. E-mail: nifontow.serezha@yandex.ru

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Г.С.Кузнецов, Ю.С. Белов

ОБЗОР СУЩЕСТВУЮЩИХ ПОДХОДОВ К РАСПОЗНАВАНИЮ ЛИЦ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Распознавания человеческих лиц является актуальной проблемой, так как за последние 10 лет количество исследований и публикаций по данной тематике выросло в несколько раз. Распознавание лиц можно применять в таких областях, как охранные системы, телеконференции, компьютерные игры и т.д.

В данном обзоре описаны основные подходы к распознаванию лиц: нейронные сети, скрытые Марковские модели, метод гибкого сравнения в графах, метод главных компонент.

Нейронные сети. Для решения данной проблемы лучше всего использовать сверточные нейронные сети, т.к. они обеспечивают частичную устойчивость к изменениям масштаба, смещениям, поворотам, смене ракурса и прочим искажениям. Архитектура нейронной сети состоит из двух типов: сверточные и подвыборочные, они чередуются друг с другом как показано на рисунке 1 [1].

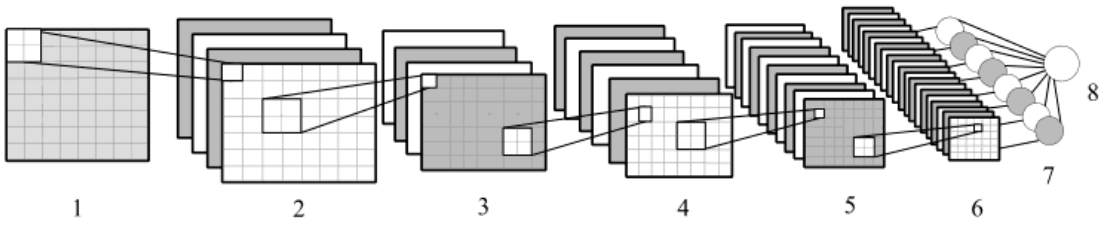


Рис. 1 Архитектура свёрточной нейронной сети: 1- вход; 2,4,6 – сверточные слои; 3,5 – подвыборочные слои; 7 – слои из обычных нейронов; 8 – выход

Происходит сканирование входящего изображения локальным рецептивным полем и информация записывается в каждый нейрон следующего слоя. Этот процесс продолжается в каждом слое нейронной сети. Таким образом, нейронная сеть извлекает характеристики изображения, инвариантные к масштабу изображения, ракурсу фотоснимка, повороту и т.д. На выходе устанавливается соответствие одному из классов изображений, хранимых в базе данных [2]. Недостатком нейронных сетей является: при добавление нового лица в базу данных требует переобучение сети, трудно формализуемый этап выбора архитектуры сети.

Скрытые Марковские модели. В данном методе используют статические свойства сигналов и учитывают непосредственно их пространственные характеристики, задействовав одномерные и псевдо-

двумерные линейные модели. В одномерной модели невозможны переходы в состояния с меньшим номером, поэтому более эффективное распознавание обеспечивает псевдо-двумерные линейные Марковские модели. Модель состоит из линейной модели с суперсостояними [3]. Каждое суперсостояние является отдельной линейной Марковской моделью.

Переход в новое суперсостояние возможен только тогда, когда система находится в финальном состоянии. По выбранному изображении проходит окно размером N x M пикселей. Суперсостояния отвечают разбиению изображения на столбцы, а последовательные переходы по состояниям внутри суперсостояния – проходу окна сверху вниз поданному столбцу. Недостатком данного подхода является то, что необходимо подбирать параметры модели для каждой базы данных.

Метод гибкого сравнения на графах. Лица предоставлены в виде графов с взвешенными вершинами и ребрами. В подобной системе распознавания графы могут представлять собой как прямоугольную решетку, так и структуру, образованную характерными точками лица как показано на рисунке 3.

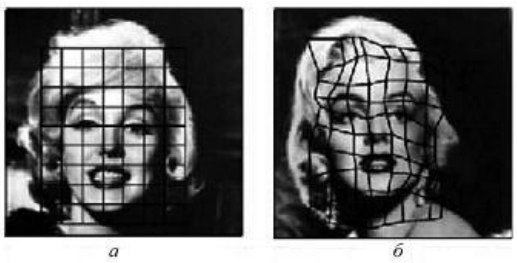


Рис. 3 Наложенная на изображение эластичная решетка и ее искаженная версия

На этапе распознавания эталонный граф остается неизменным, в то время как другой деформируется с целью наилучшей подгонки к первому. В вершинах графа вычисляются значения признаков, чаще всего используют комплексные значения фильтров Габора или их упорядоченные наборы, которые вычисляются в некоторой локальной области путем свертки значений яркости пикселей с фильтрами Габора. Деформация графа происходит путем смещения каждой из его вершин на некоторое расстояние в определенных направлениях относительно ее исходного местоположения и выбора такой позиции, при которой разница между значениями признаков в вершине деформируемого графа и соответствующей ей вершине эталонного графа будет минимальной. Недостатком данного метода является: высокая вычислительная сложность процедуры распознавания, низкая производительность метода при запоминании новых эталонов.

Метод главных компонент. Данный метод оперирует с векторами в некотором линейном пространстве. При распознавание человека по изображению лица входные векторы представляют собой отцентрированные

и приведенные к единому масштабу изображения лиц. Собственные векторы вычисленные для всего набора изображений лиц, называются собственными лицами. Метод главных компонент в применении к изображениям лиц также называют методом собственных лиц. С помощью вычисленных матриц входное изображение разлагается на набор линейных коэффициентов, называемых главными компонентами. Для каждого изображения лица вычисляются его главные компоненты. Обычно берется от 5 до 200 главных компонент. Остальные компоненты кодируют мелкие различия между лицами и шум. Процесс распознавания заключается в сравнении главных компонент неизвестного изображения с компонентами всех остальных изображений. Дополнительное повышение надежности достигается за счет применения анализа главных компонент к отдельным участкам лица таким, как глаза, нос, рот [4]. Недостатком данного подхода является то, что предъявляются высокие требования к условиями съёмки изображений. Изображения должны быть получены в близких условиях освещенности, одинаковом ракурсе и должна быть проведена качественная предварительная обработка, приводящая изображения к стандартным условиям.

Для распознавания людей используются разные технологии и алгоритмы, предъявляющие различные требования к изображениям лиц, идентифицируемых в кадре. Одни методы позволяют решать задачи контроля и учета людей и применяются в основном для автоматизации процессов идентификации и допуска сотрудников на территорию предприятия или учреждений.

Другие методы позволяют идентифицировать и искать людей в неорганизованных потоках и на видеозаписях с произвольными сценами. При этом сравнение лиц в кадре и лиц в базе данных сводиться к анализу особых точек и расстояний между ним, характерных и уникальных для каждого отдельного лица.

Список литературы

[1]. Goswami G., Bharadwaj S., Vatsa M., Singh R. On RGB-D Face Recognition using Kinect. URL: http://ieeexplore.ieee.org/ (дата обращения 05.10.2015).

[2]. Le Cun Y, Bengio Y. Convolutional for images, speech and time series. *The handbook of brain theory and neural networks* – 2005. – vol.7. - № 1. – P/ 255-258.

[3]. Yang G., Huang T. S. Human Face Detection in Complex Background. *Pattern Recognition*. vol. 27. No. 1. 2007. P. 53–63

[4]. Добеши И. Десять лекций по вейвлетам. *РХД Москва–Ижевск*, 2008, №3, с. 50-61.

Кузнецов Глеб Сергеевич- студент КФ МГТУ им. Н.Э. Баумана. E-mail: kalugazippo@yandex.ru

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

В.Е. Вершинин, М.Б. Логинова

ОБУЧЕНИЯ РАСПРЕДЕЛЁННЫХ ЛИНЕЙНО-РЕГРЕССИОННЫХ КЛАССИФИКАТОРОВ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

При работе в режиме реального времени стремительный рост объёмов данных, на основе которых строятся классифицирующие информационные модели, представляет собой трудноразрешимую проблему для многих современных средств интеллектуального анализа информации.

С одной стороны, причиной затруднений является необходимость обеспечения заданного уровня ошибки функционирования, что вынуждает применять сложные нелинейные подходы. С другой стороны, требования высокого быстродействия системы, в частности, организации быстрого обучения на новых данных, вынуждает прибегать к сэмплированию, понижению размерности и другим механизмам предобработки данных [1], вплоть до существенного упрощения модели, что негативно сказывается на точности работы системы.

Особенностью многих эффективных методов классификации (в частности, нейросетевых) является сохранение ими обучающей выборки для проведения дообучения на новых данных [2]. В случаях, когда объёмы обрабатываемых данных исчисляются десятками и сотнями тысяч записей, такие методы становятся малопригодными не только по причине длительного переобучения, но и из-за необходимости постоянной обработки (сохранения, извлечения, пересмотра) больших дополнительных объёмов информации.

Решением ряда отмеченных проблем является построение каскадированных распределённых систем [3]. Настоящая работа описывает распределённый метод обучения в режиме реального времени (РМОРВ) на основе линейно-регрессионных классификаторов применительно к системам, оперирующим высокоразмерными категорными данными.

Распределённый метод обучения в режиме реального времени функционирует в два этапа: первичное обучение и основной режим «работа-дообучение». Функционально первичное обучение состоит из следующих шагов:

1. Получение и предварительная обработка категорной базы данных $\mathbf{X}=(\mathbf{I},\mathbf{d})$ размерности $M\times N$, где $\mathbf{I}=(\mathbf{I}_1,\mathbf{I}_2,\ldots,\mathbf{I}_{N-1})$ – совокупность бинарных атрибутов размерности $M\times(N-1)$, на основе значений которых

строится общая классифицирующая модель, а $\mathbf{d}$ – M целевых категорных значений для обучения модели (классы).

2. Формирование первичного обучающего множества $\mathbf{X}^{tr}$ посредством случайной исключающей выборки M^{tr} репрезентативных записей из $\mathbf{X}$ с выделением основного обучающего множества $\mathbf{X}^{gn}$: $\mathbf{X}^{gn} = \mathbf{X} \setminus \mathbf{X}^{tr}$, $M^{gn} = M - M^{tr}$.

3. Проведение для всех $\mathbf{I}_i^{tr}, i = 1 \ldots N$ χ^2-теста [4] зависимости от целевого атрибута $\mathbf{d}^{tr}$.

4. Выбор P определяющих атрибутов, отвечающих максимальным значениям χ^2-теста.

5. Разделение первичного обучающего множества $\mathbf{X}^{tr}$ на $K = 2^P$ доменов $\mathbf{X}^{(tr,1)}, \mathbf{X}^{(tr,2)}, \ldots, \mathbf{X}^{(tr,K)}$ по значениям в P определяющих атрибутах.

6. Сохранение в векторе $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_K)$ размеров доменов $\mu_i = \left| \mathbf{X}^{(tr,i)} \right|$.

7. Независимая настройка классификаторов в каждом домене в соответствие с требованием минимизации ошибки:

$$\mathbf{b}^{(i)}: \quad \min \sum_{j=1}^{\mu_i} \left[\mathbf{x}_j^{(tr,i)} \times \mathbf{b}^{(i)} - d_j^{(tr,i)} \right]^2 \min, i = 1, \ldots, K \quad , \qquad (1)$$

где $\mathbf{b}^{(i)}$ – вектор-столбец коэффициентов линейной регрессии [5], рассчитанный для i-й модели на домене $\mathbf{X}^{(tr,i)}$, $\mathbf{x}_j^{(tr,i)}$ – j-ый обучающий пример из домена $\mathbf{X}^{(tr,i)}$, а $d_j^{(tr,i)}$ – j-ый элемент вектора $\mathbf{d}^{(tr,i)}$, отвечающий целевому значению вектора $\mathbf{x}_j^{(tr,i)}$.

Предварительная обработка данных в п.1 включает в себя бинаризацию категорных атрибутов, а так же удаление пропусков данных.

Обучение в режиме реального времени, являющееся основной фазой работы системы («дообучение» или «полное обучение»), происходит на M^{gn} записях основного обучающего множества и состоит из следующих шагов:

1. Инициализация пакетов – K пустых множеств $\mathbf{X}^{(tmp,i)} = \varnothing, i = 1, \ldots, K$ для временного хранения наборов обучающих пар.

2. Выбор m-ой обучающей пары $\left(\mathbf{x}_m^{(gn)}, d_m^{(gn)}\right)$ из основного обучающего множества $\mathbf{X}^{gn}$.

3. Соотнесение m-ой обучающей пары h-му домену ($1 \le h \le K$) в соответствие со значениями P определяющих атрибутов её входной компоненты $\mathbf{x}_m^{(gn)}$.

4. Проверка соответствия отклика $y_m^{(h)}$ построенной на h-ом домене регрессионной модели

$$y_m^{(gn,h)} = \mathbf{x}_m^{(gn)} \times \mathbf{b}^{(h)}, \tag{2}$$

для m-ой обучающей пары, её целевому значению $d_m^{(h)}$.

5. Если $\text{cat}\left(y_m^{(gn,h)}\right) = d_m^{(h)}$, т.е. категоризированный отклик для m-ой обучающей пары соответствует её целевому значению, перейти к п. 8.

6. Добавить в h-ый пакет m-ю обучающую пару:

$$\mathbf{X}^{(tmp,h)} = \mathbf{X}^{(tmp,h)} \cup \left(\mathbf{x}_m^{(gn)}, d_m^{(gn)}\right). \tag{3}$$

7. Если $\mu_h < \left|\mathbf{X}^{(tmp,h)}\right|$, добавить весь пакет в h-ый домен, очистить его

$$\mathbf{X}^{(tr,h)} = \mathbf{X}^{(tr,h)} \cup \mathbf{X}^{(tmp,h)}, \tag{4}$$

$$\mathbf{X}^{(tmp,h)} = \varnothing, \tag{5}$$

и пересчитать модель для h-го домена (коэффициенты $\mathbf{b}^{(h)}$) согласно (1).

8. Если не выбраны все пары из основного обучающего множества ($m < M^{gn}$), увеличить значение счётчика ($m = m + 1$) и перейти к п.2.

9. Если остались непустые пакеты, добавить их к соответствующим доменам

$$\mathbf{X}^{(tr,i)} = \mathbf{X}^{(tr,i)} \cup \mathbf{X}^{(tmp,i)} \quad \forall i : \mathbf{X}^{(tmp,i)} \neq \varnothing, \tag{6}$$

после чего пересчитать модели согласно (1).

10. По окончании обучения удалить из памяти все структуры, кроме определяющих атрибутов, доменов (для возможного дообучения в

дальнейшей работе) и рассчитанных для них коэффициентов регрессионных моделей.

В качестве полигона для экспериментального исследования РМОРВ была выбрана БД игры с нулевой суммой для двух сторон «Четыре в ряд» на прямоугольном поле 7x6 клеток. Каждая клетка поля могла находиться в 3 состояниях («X», «O» и «пусто»). БД включала 67556 записей (состояний игры), описывающих поле и целевой атрибут, объявляющий победителя («X», «O» или «ничья») при использовании в дальнейшем оптимальной стратегии. В результате предобработки данных, БД содержала 67556 записей со 123 бинарными атрибутами и целевым категорным атрибутом.

Результаты сравнительного анализа РМОРВ (при $P=2$) с традиционными подходами продемонстрировали высокую эффективность распределённого подхода и позволили выявить существенные недостатки традиционных регрессионных методов обусловленные применением более сложных методов классификации для конкурирующих подходов.

Список литературы

[1]. Айвазян С.А., Бухштабер В.М., Енюков Е.С., Мешалкин Л.Д. *Прикладная статистика. Классификация и снижение размерности.* Москва, Финансы и статистика, 2002, 608 с.

[2]. Хайкин С. *Нейронные сети: полный курс.* Москва, Вильямс, 2006, 1104 с.

[3]. Rachkovskij D. Linear classifiers based on binary distributed representations. *Inform. Theor. Appl,* 2007, vol. 14 (1), pp. 270–274.

Вершинин Владислав Евгеньевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: goliathonline@mail.ru

Логинова Мария Борисовна - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: loginovamb@yandex.ru

К.М. Гришанов, Ю.С. Белов

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ НЕЧЕТКИХ СИСТЕМ В РАСПОЗНАВАНИИ ОБРАЗОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Распознавание символов на сегодняшний день является одной из важнейших технологий, которая используется во многих сферах, таких как искусственный интеллект, машинное зрение, сопоставление с образцом и другие. Существует два типа систем распознавания символов: оптическое распознавание символов, также известное как офлайн распознавание символов и интеллектуальное распознавание символов, также известное как онлайн распознавание символов. В офлайн системах распознавания символов, рукописный или печатный текст переводится в цифровой формат. В онлайн системах распознавания символов распознавание основывается на направлении движения во время записи символа. Этот метод широко используется на сенсорных панелях, сенсорных экранах мобильных телефонов и других устройствах. Одни из наиболее часто используемых методов для реализации оптического распознавания символов это нейронные сети и нечеткая логика. В статье будет дан краткий обзор систем, основанных на нечеткой логике.

Традиционные языки программирования такие как Java, C++ и другие основываются на булевой логике. Такие языки программирования хорошо подходят для реализации систем с разделением времени, интернет приложений и многих других систем, поведение которых может быть также представлено с помощью математических моделей. Однако, для разработки систем, которые будут принимать человекоподобные решения, математические модели часто непригодны. Человеческие утверждения и оценки просто не поддаются булевой логике в отличие от традиционной математической дисциплины. Отсюда следует, что традиционные языки программирования, базирующиеся на математической логике, не эффективны для программирования и обоснования человекоподобных процессов принятия решений. Нечеткая логика, предложенная Лотфи Заде в 1965 году, дает преимущества для построения систем, основанных на человекоподобных решениях[1].

Основа для предложенной нечеткой логики состояла в том, что люди часто полагаются на неточные выражения такие как “большой”, “дорогой”, “дальний”. Но понимание компьютера ограничено моделями мышления: черный-белый, все-ничего, правда-ложь. В этом контексте, Лотфи Заде подчеркивал, что люди желают достигать максимально возможной точности, не учитывая неточный характер реальности.

Теория нечетких множеств, которая базируется на нечеткой логике была представлена Лотфи Заде в 1965 году как математический способ представления неопределенности в лингвистике и может быть обоснована обобщением классической теории множеств. Основная идея нечетких множеств довольно проста для понимания. В классическом множестве, которое есть набор отличных объектов, объекты области исследования делятся на две группы:

$\mu_A(u) = 1,$ если u принадлежит A, и

$\mu_A(u) = 0,$ если u не принадлежит множеству A

Элемент может либо принадлежать множеству, либо не принадлежать.

Нечеткие множества устраняют резкие границы, которые разделяют элементы на принадлежащие и не принадлежащие группе. В этом случае принадлежность множеству задается нечеткой функцией принадлежности, и объект может принадлежать множеству частично.

Степень принадлежности определяется через обобщенную характеризующую функцию, которая называется функция принадлежности:

$\mu_A(u): U \to [0,1],$ где U называется пространством рассуждения и A нечеткое подмножество U[2].

Значения функции принадлежности - это действительные числа из интервала [0,1], где 0 означает, что объект не принадлежит множеству, а 1 означает, что объект полностью принадлежит множеству. На рисунке 1 показана принципиальная разница между четким и нечетким множествами. Четкое множество имеет конкретные значения, в то время как значения нечеткого множества ранжированы.

Основным преимуществом, полученным из этого подхода, является возможность выразить неоднозначность человеческого мышления и субъективность (в том числе естественного языка) сравнительно неискаженным методом. Нечеткая логика подходит для использования в следующих задачах:

Рис. 1. Четкое и нечеткое множества

— В задачах, связанных с непрерывным явлением, которое тяжело разбить на дискретные части[3];
— В задачах, где математическая модель процесса не существует или существует, но слишком сложна для кодирования, либо слишком сложна для вычисления в операциях реального времени или требует большого количества памяти;
— В задачах с высоким уровнем шума;
— В задачах, которые включают взаимодействие людей и необходимость понимания человеческого описания или интуитивного мышления;
— В задачах, в которых экспертом задаются правила, лежащие в основе поведения системы, так же как нечеткие множества, которые представляют особенности каждой переменной.

Благодаря своим особенностям, методы нечеткой логики находят применение в таких областях как управление, распознавание образов, количественный анализ, логический вывод, поиск информации[4].

Основной недостаток нечетких систем состоит в том, что они не имеют достаточной способности к обучению настройки их нечетких правил и функций принадлежности. Обычно нечеткие правила задаются экспертами или операторами, которые предоставляют свой опыт или знание. Однако, когда модель нечеткой системы разработана, она часто слишком сложна для человека, чтобы определить все желаемые нечеткие правила или функции принадлежности оптимальным способом, в результате чего возникает неопределенность, неточность и сложность идентификационной системы.

Литература

[1]. Новак В., Перфильева И.Ю., Мочкорж И., Математические принципы нечеткой логики, 2006, с. 7-9

[2]. Борисов В.В., Федулов А.С., Зернов М.М., Основы теории нечетких отношений, 2014 с. 6-23.

[3]. K.B.M.R. Batuwita, “Meaningful Segmentation of Offline Individual Handwritten Numeric Characters,” 2006 IEEE International Conference on Fuzzy Systems Sheraton Vancouver Wall Centre Hotel, Vancouver, BC, Canada July 16-21, 2006.

[4]. Md. Shabiul Islam, M.S. Bhuyan, Sawal H. M. Ali, Masuri Othman, Burhanuddin Yeop Majlis, “VHDL Implementation of Fuzzy Based Handwriting Recognition System “ICSE2010 Proc. 2010, Melaka, Malaysia.

Гришанов Кирилл Михайлович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: cyrilgrishanov94@gmail.com

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

И.И. Кручинин, Р.А. Трубка

ПРЕДОБРАБОТКА ВХОДНЫХ СИГНАЛОВ НЕЙРОСЕТЕЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

При решения конкретных задач первое, с чем сталкивается пользователь любого нейропакета - это необходимость подготовки данных для нейросети. На практике же именно предобработка данных может стать наиболее трудоемким элементом нейросетевого анализа. Причем, знание основных принципов и приемов предобработки данных не менее, а может быть даже более важно, чем знание собственно нейросетевых алгоритмов.

ехнологическая цепочка предподготовки данных для нейросетевого анализа состоит из следующих этапов:

1. Кодирование входов-выходов: нейросети могут работать только с числами

2. Нормировка данных: результаты нейроанализа не должны зависеть от выбора единиц измерения.

3. Предобработка данных: удаление очевидных регулярностей из данных облегчает нейросети выявление нетривиальных закономерностей.

4. Обучение нескольких нейросетей с различной архитектурой: результат обучения зависит как от размеров сети, так и от ее начальной конфигурации.

5. Отбор оптимальных сетей: тех, которые дадут наименьшую ошибку предсказания на неизвестных пока данных.

6. Оценка значимости предсказаний: оценка ошибки предсказаний не менее важна, чем само предсказанное значение.

В отличие от обычных компьютеров, способных обрабатывать любую символьную информацию, нейросетевые алгоритмы работают только с числами, ибо их работа базируется на арифметических операциях умножения и сложения. Именно таким образом набор синоптических весов определяет ход обработки данных. Между тем, не всякая входная или выходная переменная в исходном виде может иметь численное выражение. Соответственно, все такие переменные следует закодировать - перевести в численную форму, прежде чем начать собственно нейросетевую обработку. Допустим, что в результате перевода всех данных в числовую форму и последующей нормировки все входные и выходные переменные отображаются в единичном кубе. Задача нейросетевого моделирования - найти статистически достоверные зависимости между входными и выходными переменными. Единственным источником информации для статистического моделирования являются примеры из обучающей выборки. Чем больше бит информации принесет каждый пример - тем лучше используются имеющиеся в нашем распоряжения данные. Рассмотрим произвольную компоненту нормированных (предобработанных) данных: Среднее количество информации, приносимой каждым примером, равно энтропии распределения значений этой компоненты. Если эти значения сосредоточены в относительно небольшой области единичного интервала,

информационное содержание такой компоненты мало. В пределе нулевой энтропии, когда все значения переменной совпадают, эта переменная не несет никакой информации. Напротив, если значения переменной $\tilde{x}_i^{\alpha}$ равномерно распределены в единичном интервале, информация такой переменной максимальна. Общий принцип предобработки данных для обучения, таким образом, состоит в максимизации энтропии входов и выходов. Можно выделить два основных типа нечисловых переменных: упорядоченные и категориальные. В обоих случаях переменная относится к одному из дискретного набора классов $\{c_1, c_2, \ldots, c_n\}$. Но в первом случае эти классы упорядочены - их можно ранжировать: $c_1 \succ c_2 \succ \ldots \succ c_n$, тогда как во втором такая упорядоченность отсутствует.

В качестве примера упорядоченных переменных можно привести сравнительные категории: плохо - хорошо - отлично, или медленно - быстро. Категориальные переменные просто обозначают один из классов, являются именами категорий. Ординальные переменные более близки к числовой форме, т.к. числовой ряд также упорядочен. Соответственно, для кодирования таких переменных остается лишь поставить в соответствие номерам категорий такие числовые значения, которые сохраняли бы существующую упорядоченность. Естественно, при этом имеется большая свобода выбора - любая монотонная функция от номера класса порождает свой способ кодирования. Из всех статистических функций распределения, определенных на конечном интервале, максимальной энтропией обладает равномерное распределение. Применительно к данному случаю это подразумевает, что кодирование переменных числовыми значениями должно приводить, по возможности, к равномерному заполнению единичного интервала закодированными примерами. При таком способе «оцифровки» все примеры будут нести примерно одинаковую информационную нагрузку. Исходя из этих соображений, можно предложить следующий практический рецепт кодирования ординальных переменных. Единичный отрезок разбивается на n отрезков - по числу классов - с длинами пропорциональными числу примеров каждого класса в обучающей выборке: $\Delta x_k = P_k/P$, где P_k - число примеров класса k, а P, как обычно, общее число примеров. Центр каждого такого отрезка будет являться численным значением для соответствующего ординального класса. Если классы не упорядочены, такова же должна быть и схема кодирования. В этом случае имеет смысл использовать более компактный, но симметричный код $n \to m$, когда имена n классов кодируются m - битным двоичным кодом. Причем, в новой кодировке активность кодирующих нейронов должна быть равномерна - иметь приблизительно одинаковое среднее по примерам значение активации. Это гарантирует одинаковую значимость весов, соответствующих различным нейронам.

Кручинин Илья Игоревич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ikruchi@gmail.ru

Трубка Роман Анатольевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: roman.trubka@mail.ru

Ф.А. Плотников, И.А. Косенков

ПРОБЛЕМА УЧЕТА ВРЕМЕНИ РАБОТНИКОВ НА СОВРЕМЕННЫХ ПРЕДПРИЯТИЯХ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Для чего необходим учет рабочего времени? Любой грамотный управленец знает, что сотрудник не может целиком и полностью отдаваться работе на протяжении всего рабочего дня. Для этого необходима огромная концентрация, абстрагирование от внешнего мира. С другой стороны, нельзя допускать, чтобы сотрудник злоупотреблял опозданиями, затянувшимися обедами, чаепитиями, перекусами и занятиями личными делами. Для каждого руководителя его сотрудник – это один из ценных интеллектуальных ресурсов. Для того чтобы этот ресурс был наиболее выгодно использован и нужен контроль, за его рабочим временем.

Согласно данным исследований, от 20 до 40% рабочего времени тратится не по назначению, то есть, не на рабочий процесс[1]. Это является следствием неправильного планирования. Таким образом, можно сделать вывод о том, что на предприятиях необходим контроль, за работой сотрудников и управление временем (тайм-менеджмент), это позволит осуществить сбор необходимой информации, проанализировать ее, независимо оценить, после чего сделать необходимые выводы, что, как следствие, позволяет увеличить производительность труда.

Задачи, которые позволяет решить система учета рабочего времени:

— - автоматическая регистрация времени прихода и ухода персонала;
— - мониторинг запущенных и активных приложений
— - контроль за активными лицензиями
— - мониторинг самых используемых приложений в отделе
— - возможность формирования отчета по каждому отдельному сотруднику, группе сотрудников или по всем сотрудникам сразу;
— - гибкая настройка системы, по множеству параметров, с целью оптимизировать продукт именно под данную задачу;
— - справедливое начисление заработной платы;
— - упрощенное ведение отчетности и планирования трудоемкости[2].

Особую сложность представляет контроль за сотрудниками, которые работают на компьютере. Несмотря на то, что де-юре, сотрудник находится на рабочем месте, никуда не отвлекаясь, де-факто, он может заниматься совсем не рабочими задачами и тратить время на личные дела. Также, чтобы оптимизировать рабочий процесс, необходимо знать наиболее используемые приложения, для того, чтобы в определенное время выделить под них больше ресурсов.

С одной стороны такие системы контроля помогают управленцам осуществлять контроль и позволяют более точно планировать работу в отделе, с другой стороны, ответственным сотрудникам они могут помочь для самоорганизации.

Для того чтобы осуществить контроль и увеличить производительность труда, чтобы гибко варьировать план работы и аргументированно воздействовать на своих подопечных, руководителю необходима информация, которая даст ему представление чем занимается каждый сотрудник в частности, либо общую картину по отделу. Для достижения этих целей на рынке имеется большое количество специализированного ПО, которое, далее в этой статье, будет проанализировано по следующим критериям

- Оценка простоя-бездействие пользователя, чаепития, отлучения
- Версия для ПК- наличие desktop версии
- Наличие автоматизированного подсчета времени
- Возможность создания скриншотов, для последующего их анализа
- Удобный и эргономичный интерфейс
- Мониторинг: подсчет времени работы в приложениях, документах, а также отслеживание интернет-активности
- Детализация: возможность создания категорий, добавления меток (тегов), комментариев
- Статистика: получение информации о времени, проведенном в приложении, на сайте, возможность построения сводных таблиц, графиков
- Экспорт данных: поддержка сторонних форматов, печать отчетов, таблицы, диаграммы, графики.
- Деление времени на полезное и непродуктивное[3].

Таблица1. Сравнительная характеристика программных продуктов

Программы / факторы	Простой	Версия для ПК	Автоматический подсчет времени	Скриншоты	Удобный интерфейс	Мониторинг	Детализация	Статистика	Экспорт данных	Деление времени
1.Yaware	+	-	+	+	+-	+	+	+	+	+
2.Стахановец	+	+	+	+	-	+	+	+	-	-
3.Motivate Clock	-	+	-	-	+-	+	-	+	-	+
4.CrocoTime	+	+	+	-	+	+	+	+	+	+
5.ABRA	-	+	-	-	+	-	-	+	-	+
6.Tachometer	+	+	+	+	+	+	+	+	-	+
7.Дисциплина	+	+	+	-	-	+	+	+	-	+

Проанализировав данные продукты можно сделать вывод, что ни один из них не является идеальным. В одних отсутствует специфический функционал, другие не лучшим образом оптимизированы с точки зрения передачи данных по сети, в третьих нет настраиваемого функционала под определенную задачу и отключения не нужных функций.

Самым главным недостатком всех продуктов является открытость собираемой информации, особенно это наблюдается у веб-сервисов. Таким образом, данная проблема не является полностью решеной, для ее решения лишь созданы механизмы, которые облегчают процесс сбора информации. Но они не позволяют четко контролировать оптимальность распределения времени персонала, а ведь время - это единственный невосполнимый ресурс в жизни каждого человека, это один из основных организационных ресурсов.

Список литературы:

[1] Генкин Б.М. Экономика и социология труда. Мосвка, Норма, 2010, 234с.

[2] Олимских Н.Н. Актуальные проблемы экономики труда. Ижевск, Удм. Ун-та, 2009, 340 с.

[3] Виханский О.С., Наумов А.И. Менеджмент Москва, Гардарика, 2009, 270 с.

Плотников Федор Алексеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: blackdef@bk.ru

Косенков Иван Алексеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: kosenkov.ia@gmail.com

А.А. Карышев, А.Ю. Щербатых

РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА ТРАНСПОРТНЫХ СРЕДСТВ НА ТЕРРИТОРИЮ ПРЕДПРИЯТИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время большое внимание уделяется автоматизации технологических и бизнес процессов на предприятиях. Автоматизация процессов позволяет значительно сократить расходы предприятия, ускоряет процесс обработки данных и облегчает труд работников.

В современных условиях актуальной является проблема автоматизация контроля доступа транспортных средств на территорию предприятий. Чаще всего эта проблема решается путем выдачи пропусков на въезд и выезд транспортных средств на бумажных носителях. Контроль за перемещением осуществляется сотрудником охраны, что не всегда удобно, часто приводит к задержкам по времени и ошибкам. Логичным решением проблемы является внедрение автоматизированной системы контроля доступа транспортных средств на территорию предприятия.

Внедрение автоматизированной системы позволит решить следующие проблемы:

— упрощение процедуры доступа на предприятие;
— снижение влияния человеческого фактора;
— упрощение процедуры контроля за въездом/выездом автотранспорта;
— сокращение времени на проверку.

Для автоматизации контроля доступа транспортных средств необходимо реализовать систему оптического распознавания номеров автомобилей. Оптическое распознавание символов (OCR) — это механический, а чаще электронный перевод изображений рукописного, машинописного или печатного текста в текстовые данные — последовательность кодов, использующихся для представления символов в компьютере [1].

OCR - системы могут достигать достаточно неплохой точности, распознавая порядка 99% для качественных изображений, составленных из обычных шрифтов. Однако, даже при таких результатах имеются ошибки, которые требуют человеческого контроля результатов, чтобы гарантировать соответствие оригиналу. Встречающиеся в реальной жизни тексты порой весьма далеки от совершенных, и процент точности распознавания для "зашумленных" текстов часто недопустим для распознания.

Появление шумов на изображении – является достаточно серьезной проблемой, т.к. даже малые шумы, в виде плохого освещения могут затенять определяющие части символа или преобразовывать один в другой при распознавании [1]. Нередко возникают разрывы и слияния символов (такие тексты нередко возникают и при сканировании или плохой

фокусировки камеры). Любой из этих эффектов может заставлять систему ошибаться, т.к. некоторые из OCR систем полагают, что каждая соединенная черная метка должна быть одиночным символом.

Автоматическое распознавание номерного знака (ANPR) - это способность фиксировать буквенно-цифровые символы номерного знака автомобиля, обеспечивать четкое считывание и передачу данных на компьютер, позволяя вручную или автоматически сопоставлять полученные номера с номерами, расположенными в базе данных[1].

Существует два распространенных способа осуществления фиксации номеров [1]:

— Оптическое распознавание каждого символа номерного знака и предоставление для них значений.
— Применение нейронной сети, которая позволяет последовательно устанавливать каждый номер и обеспечивает более надежное считывание. Сначала дается определение номерного знака, и затем применяются правила разбиения номера на буквенно-цифровые составляющие, устраняя тем самым фоновые помехи, создаваемые знаками отличия провинций, изображениями и другими деталями, которые можно увидеть на номерных знаках.

Для реализации проекта был выбран первый способ фиксации номеров. В качестве инструмента реализации была выбрана библиотека Puma.NET. Эта библиотека является одной из лучших бесплатных библиотек по распознаванию данных с изображений [2].

Рассмотрим основные возможности Puma.NET:

— распознавание множества печатаемых шрифтов;
— поддержка 27 языков, среди которых есть и русский;
— проверка правописания;
— автоматическое определение шрифтов (курсив, подчеркнутый и т.д.);
— сохранение структуры документа (абзацы, изображения, таблицы);
— улучшенное распознавание текста, расположенного под углом.

Основные классы библиотеки Puma.NET представлены на рисунке №1.

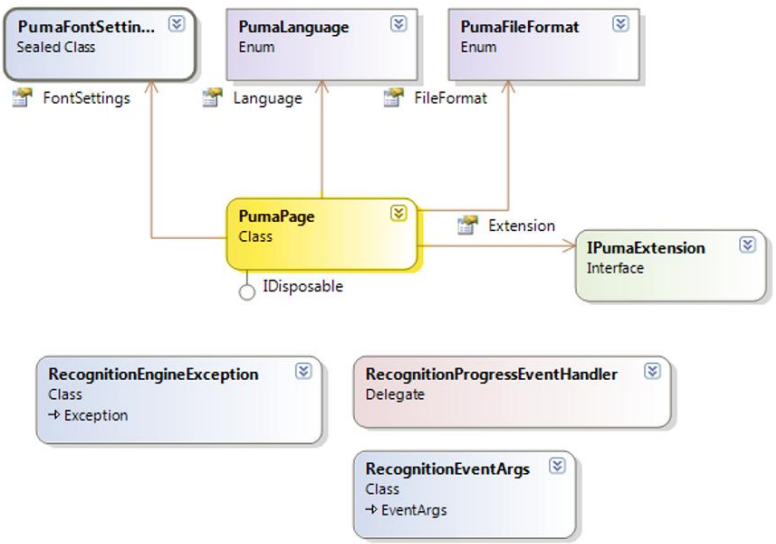


Рис. 1. Классы библиотеки Puma.NET

Рассмотрим основные классы библиотеки Puma.NET.

— PumaPage - основной класс, который обрабатывает одно изображение (страницы) и производит результаты распознавания в виде файла или строкового значения.
— PumaFontSettings - классовые группы параметров распознавания относительно шрифтов.
— PumaLanguage, PumaFileFormat – определяют доступные языки и форматы файлов для обработки.
— IPumaExtension – используется для расширения функциональности класса PumaPage.
— RecognitionProgressEventHandler, RecognitionEventArgs, RecognitionException - поддержание событий распознавания и обработка ошибок.

В результате работы были рассмотрены основные способы автоматического распознавания номеров. В качестве основы для системы распознавания автомобильных номеров была выбрана библиотека Puma.NET. Исследована иерархическая структура библиотека классов Puma.NET.

Список литературы

[1] Автоматическое распознавание номерного знака ANPR [Электронный ресурс] http://habrahabr.ru/company/croc/blog/158719/(Дата обращения 20.10.2015)

[2] Общие сведения о Puma.NET [Электронный ресурс]. http://pumanet.codeplex.com (Дата обращения 24.10.2015)

Карышев Андрей Анатольевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ak9105252055@yandex.ru

Щербатых Алексей Юрьевич- студент КФ МГТУ им. Н.Э. Баумана. E-mail: ak9105252055@yandex.ru

И.И. Кручинин, С.Г. Гуров, П.С. Казичкина

РАЗРАБОТКА БИБЛИОТЕКИ КЛАССОВ НЕЙРОСЕТЕЙ РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Среди различных структур нейронных сетей (НС) одной из наиболее известных является многослойная структура, в которой каждый нейрон произвольного слоя связан со всеми аксонами нейронов предыдущего слоя или, в случае первого слоя, со всеми входами НС. Такие НС называются полносвязанными. В многосвязанных сетях оптимальные выходные значения нейронов всех слоев, кроме последнего, как правило, не известны. Для нахождения наборов выходных сигналов, соответствующих входным, для каждого слоя НС, наибольшее распространение получил метод распространения сигналов ошибки от выходов НС к ее входам, в направлении, обратном прямому распространению сигналов в обычном режиме работы. Этот алгоритм обучения НС получил название процедуры обратного распространения ошибки [1].

В настоящей работе проводится разработка библиотеки классов для программирование НС на базе концепций объектно-ориентированного (ОО) программирования. Разработанная библиотека была составлена и использовалась в целях распознавания изображения, однако она может быть применима и в других приложениях. В файле neuron.k в листинге 1 приведены описания двух базовых и пяти производных (рабочих) классов: Neuro, Net и NeuroFF, NeuroBP, LayeFF, LayeBP, NetBP, а также описания нескольких общих функций вспомогательного назначения, содержащихся в файле supfun.cpp (листинг 4). Методы пяти вышеуказанных рабочих классов внесены в файлы neuro_ff.cpp, представленных в листингах 2 и 3. Такое, на первый взгляд искусственное разбиение объясняется тем, что классы с суффиксом _ff, описывающие прямопоточные нейронные сети (freeforward), входят в состав не только сетей с обратным распространением - _bp (back-propagation), но и других, например таких, как с обучением без учителя, которые будут рассмотрены в дальнейшем.

В ущерб принципам ОО программирования, шесть основных параметров, характеризующих работу сети, вынесены на глобальный уровень, что облегчает операции с ними. Параметр SigmoType определяет вид активационной функции. В методе NeuroFF::Sigmo перечислены некоторые его значения, макроопределения которых сделаны в заголовочном файле. Пункты HARLIMIT и THRESHOL даны для общности, но не могут быть использованы в алгоритме обратного распространения, так как соответствующие им активационные функции

имеют производные с особыми точками. Это отражено в методе расчета производной nEUROff::D_Sigmo, из которого эти два случая исключены. Величина Limi используется в методах IsConver для определения момента, когда сеть обучится и попадет в паралич. В этих случаях изменения весов становится меньше малой величины Limi. Параметр dSigma эмулирует плотность шума, добавляемого к образам во время обучения НС. Это позволяет из конечного набора "чистых" входных образов генерировать практически неограниченное число "зашумленных" образов. Дело в том, что для нахождения оптимальных значений весовых коэффициентов число степеней свободы НС – M должно быть намного меньше числа накладываемых ограничений – XY, где Y – число образов, предъявляемых НС во время обучения. Фактически, параметр dSigma равен числу входов, которые будут инвертированы в случае двоичного образа. Методы Radomize позволяют перед началом обучения установить весовые коэффициенты в случайные значения в диапазоне (-г,+г). Методы Propagate выполняют вычисления соответствующих коэффициентов перехода. Метод NetBP::CalError на основе передаваемого в качестве аргумента массива верных (желаемых) выходных значений НС вычисляет величины δ. Метод NetBP::Learn рассчитывает изменения весов, методы Update обновляют весовые коэффициенты. Метод NetBP::Cyc1e объединяет в себе все процедуры одного цикла обучения, включая установку входных сигналов. Различные методы PrintXXX и LayегBP:Show позволяют контролировать течение процессов в НС, но их реализация не имеет принципиального значения, и простые процедуры из приведенной библиотеки могут быть при желании переписаны, например, для графического режима. Это оправдано и тем, что в алфавитноцифровом режиме уместить на экране информацию о сравнительно большой НС уже не удается.

Сети могут конструироваться посредством NetBP(unsigned), после чего их нужно заполнять сконструированными ранее слоями с помощью метода nETBP::SetLayer, либо посредством NetBP(unsigned,...). В последнем случае конструкторы слоев вызываются автоматически. Для установления синоптических связей между слоями вызывается метод NetBP::FullConnect.

После того как сеть обучится, ее текущее состояние можно записать в файл (метод NetBP::SaveToFile), а затем восстановить с помощью метода NetBP::LoadFromFile, который применим лишь к только что сконструированной по NetBP(void) сети.

Сеть сконструированная в качестве примера а программе, приведенной в листинге 5, была обучена распознавать 26 букв, схематично заданных матрицами 10x8 точек за несколько тысяч циклов обучения. Обученная сеть успешно распознавала изображения, зашумленные более сильно, чем образы, на

которых она обучалась. Предложенная библиотека классов позволит создавать сети, способные решать широкий спектр задач, таких как построение экспертных систем, сжатие информации и многих других, исходные условия которых могут быть приведены к множеству парных входных и выходных наборов данных.

Список литературы

[1] Хайкин С. Нейронные сети: полный курс. Москва, Вильямс, 2006, 1104 с.

Кручинин Илья Игоревич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ikruchi@gmail.ru

Гуров Станислав Геннадьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: gurov.it@mail.ru

Казичкина Полина Сергеевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: paulinakazichkina@gmail.com

Ю.С. Белов, Т.С. Тихонова, Б.М.Логинов

РАЗРАБОТКА КВАЗИДИНАМИЧЕСКОЙ МОДЕЛИ ДЛЯ РАСЧЕТА МЕХАНИЧЕСКИХ СВОЙСТВ ПЕРИОДИЧЕСКИХ СТРУКТУР ГРУППЫ СИММЕТРИИ D_N

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Большое внимание исследователей к классу периодических структуры с группой симметрии D_N обусловлено уникальными физико-химические свойствами углеродных нанотрубок (УНТ), обладающих такой симметрией. Накопленный к настоящему времени научно-практический опыт позволяет говорить о вполне сформировавшихся методах теоретического и экспериментального анализа разнообразных свойств УНТ. Тем не менее, естественные трудности исследования микроскопических по своей природе УНТ на наноскопическом уровне, оставляют большое число нерешенных вопросов, как в плане получения адекватных количественных характеристик отдельных свойств, так и в плане используемых методов анализа. Применяемые методы теоретического анализа механических свойств УНТ содержат различные подходы и приближения, которые можно характеризовать как: квантово-механические, континуальные, конечно-элементные, молекулярно-динамические. Независимо от используемого метода, анализ механических свойств УНТ производится на основе поиска равновесных конфигурации нанотрубки, отвечающих энергетическому минимуму, в изменяющихся условиях внешнего воздействия. В каждом методе принимаемые упрощающие предположения накладывают свои ограничения, как на классы рассматриваемых процессов, так и совокупность исследуемых характеристик.

Настоящая работа посвящена разработке новой квазидинамической модели моделирования.

При фиксированных граничных условиях установившееся равновесное состояние УНТ с заданными геометрическими параметрами характеризуется нулевым балансом сил, действующих на каждый из атомов УНТ. В классическом приближении, силы, действующие на атомы УНТ с заданной структурой, определяются граничными условиями в соответствии с центральными силами парного взаимодействия $F(r)$. В свою очередь, силы парного взаимодействия определяется на основании потенциальной энергии парного взаимодействия $U(r)$:

$$F(r) = -\frac{\partial U}{\partial r}, \qquad (1)$$

где r - расстояние между атомами.

Не нарушая общности, для идентификации атомов УНТ будем использовать нотацию *i*-ых слоев и *j*-ых рядов атомов УНТ. Введем цилиндрическую систему координат, ось OZ которой совместим с осью симметрии УНТ. Полярный луч, расположенный в плоскости атомов последнего слоя УНТ, направим вдоль линии, пересекающей ось OZ и один из атомов слоя, который будет считать соответствующим первому ряду атомов УНТ. Тогда каждый атом УНТ идентифицируется упорядоченной парой чисел (*i*;*j*), а его пространственное расположение задается тройкой координат ($\varphi;\rho;z$). С учетом элементарной операции перехода из цилиндрической системы координат в Декартову ($x=\rho\cdot\cos\varphi$; $y=\rho\cdot\sin\varphi$; $z=z$), расстояние, например, между двумя ближайшими атомами $A_j^{(i)}$ и $A_{j+1/2}^{(i+1)}$ будет задаваться соотношением:

$$r_{j,(j+1/2)}^{i,(i+1)}=\sqrt{\left(\rho_j^{(i)}\cdot\cos\varphi_j^{(i)}-\rho_{j+1/2}^{(i+1)}\cdot\sin\varphi_{j+1/2}^{(i+1)}\right)^2+\left(\rho_j^{(i)}\cdot\sin\varphi_j^{(i)}-\rho_{j+1/2}^{(i+1)}\cdot\sin\varphi_{j+1/2}^{(i+1)}\right)^2+\left(z_j^{(i)}-z_{j+1/2}^{(i+1)}\right)^2} \quad (2)$$

а соответствующая сила парного взаимодействия, направленная вдоль отрезка соединяющего атомы $A_j^{(i)}$ и $A_{j+1/2}^{(i+1)}$, определяется в соответствии с (1).

Поскольку в процессе деформационного нагружения могут происходить изменения в структуре УНТ, приводящие, в частности, к образованию дефектов, корректный анализ механических свойств УНТ требует рассмотрения учета влияния не только атомов ближайшего круга, но и следующих за ними атомов.

Рассмотрим ситуацию внешнего воздействия. Будем считать, что на каждый атом первого слоя (*i*=1, *j*=1,2,…,k) действует растягивающая сила $\Delta f^{вн}$, коллинеарная оси OZ, при этом расположение атомов последнего слоя оказывается зафиксированным. Предположим, что в результате внешнего воздействия, атомы УНТ в результате своих перемещений $\Delta r_j^{(i)}=(\Delta\varphi_j^{(i)};\Delta\rho_j^{(i)};\Delta z_j^{(i)})$, перешли в новое равновесное состояние. В качестве первого приближения, составим уравнения баланса сил для атомов УНТ на основе учета их взаимодействия с атомами первого круга. До воздействия внешних сил, согласно начальным условиям, атомы УНТ находились в равновесном состоянии, поэтому, равновесное состояние атомов УНТ после приложения внешней нагрузки, должно устанавливаться на основе баланса изменений сил в узлах. В свою очередь, изменение сил парного взаимодействия в результате изменения расстояний между взаимодействующими атомами на величину Δr, на основании (1) можно представить как:

$$\Delta F(r)=\frac{\partial F}{\partial r}\cdot\Delta r=\frac{\partial}{\partial r}\left(-\frac{\partial U}{\partial r}\right)\cdot\Delta r=-\frac{\partial^2 U}{\partial r^2}\cdot\Delta r \quad (3)$$

Таким образом, для атомов УНТ, в соответствии с принятой нотацией, проекции уравнений баланса приращений сил в узлах на ось OZ имеют следующий вид:

$$
\begin{aligned}
&f^{вн} - \frac{\partial^2 U}{\partial (r_{1,1/2}^{(1,2)})^2} \cdot \frac{\partial (r_{1,1/2}^{(1,2)})}{\partial z} \cdot (\Delta z_1^{(1)} - \Delta z_{1/2}^{(2)}) - \frac{\partial^2 U}{\partial (r_{1,3/2}^{(1,2)})} \cdot \frac{\partial r_{1,3/2}^{(1,2)}}{\partial z} \cdot (\Delta z_1^{(1)} - \Delta z_{3/2}^{(2)}) = 0 \\
&f^{вн} - \frac{\partial^2 U}{\partial (r_{2,3/2}^{(1,2)})^2} \cdot \frac{\partial (r_{2,3/2}^{(1,2)})}{\partial z} \cdot (\Delta z_2^{(1)} - \Delta z_{3/2}^{(2)}) - \frac{\partial^2 U}{\partial (r_{2,5/2}^{(1,2)})} \cdot \frac{\partial r_{2,5/2}^{(1,2)}}{\partial z} \cdot (\Delta z_2^{(1)} - \Delta z_{5/2}^{(2)}) = 0 \\
&f^{вн} - \frac{\partial^2 U}{\partial (r_{3,5/2}^{(1,2)})^2} \cdot \frac{\partial (r_{3,5/2}^{(1,2)})}{\partial z} \cdot (\Delta z_3^{(1)} - \Delta z_{5/2}^{(2)}) - \frac{\partial^2 U}{\partial (r_{3,7/2}^{(1,2)})} \cdot \frac{\partial r_{3,7/2}^{(1,2)}}{\partial z} \cdot (\Delta z_3^{(1)} - \Delta z_{7/2}^{(2)}) = 0
\end{aligned}
\tag{4а}
$$

$$
\begin{aligned}
&f^{вн} - \frac{\partial^2 U}{\partial (r_{k,k-1/2}^{(1,2)})^2} \cdot \frac{\partial (r_{k,k-1/2}^{(1,2)})}{\partial z} \cdot (\Delta z_k^{(1)} - \Delta z_{k-1/2}^{(2)}) - \frac{\partial^2 U}{\partial (r_{k,1/2}^{(1,2)})} \cdot \frac{\partial r_{k,1/2}^{(1,2)}}{\partial z} \cdot (\Delta z_k^{(1)} - \Delta z_{1/2}^{(2)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{k,1/2}^{(1,2)})^2} \cdot \frac{\partial (r_{k,1/2}^{(1,2)})}{\partial z} \cdot (\Delta z_k^{(1)} - \Delta z_{1/2}^{(2)}) + \frac{\partial^2 U}{\partial (r_{1,1/2}^{(1,2)})^2} \cdot \frac{\partial r_{1,1/2}^{(1,2)}}{\partial z} \cdot (\Delta z_1^{(1)} - \Delta z_{1/2}^{(2)}) - \frac{\partial^2 U}{\partial (r_{1/2,1/2}^{(2,3)})^2} \cdot \frac{\partial r_{1/2,1/2}^{(2,3)}}{\partial z} \cdot (\Delta z_{1/2}^{(2)} - \Delta z_{1/2}^{(3)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{1,3/2}^{(1,2)})^2} \cdot \frac{\partial (r_{1,3/2}^{(1,2)})}{\partial z} \cdot (\Delta z_1^{(1)} - \Delta z_{3/2}^{(2)}) + \frac{\partial^2 U}{\partial (r_{2,3/2}^{(1,2)})^2} \cdot \frac{\partial r_{2,3/2}^{(1,2)}}{\partial z} \cdot (\Delta z_2^{(1)} - \Delta z_{3/2}^{(2)}) - \frac{\partial^2 U}{\partial (r_{3/2,3/2}^{(2,3)})^2} \cdot \frac{\partial r_{3/2,3/2}^{(2,3)}}{\partial z} \cdot (\Delta z_{3/2}^{(2)} - \Delta z_{3/2}^{(3)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{2,5/2}^{(1,2)})^2} \cdot \frac{\partial (r_{2,5/2}^{(1,2)})}{\partial z} \cdot (\Delta z_2^{(1)} - \Delta z_{5/2}^{(2)}) + \frac{\partial^2 U}{\partial (r_{3,5/2}^{(1,2)})^2} \cdot \frac{\partial r_{3,5/2}^{(1,2)}}{\partial z} \cdot (\Delta z_3^{(1)} - \Delta z_{5/2}^{(2)}) - \frac{\partial^2 U}{\partial (r_{5/2,5/2}^{(2,3)})^2} \cdot \frac{\partial r_{5/2,5/2}^{(2,3)}}{\partial z} \cdot (\Delta z_{5/2}^{(2)} - \Delta z_{5/2}^{(3)}) = 0
\end{aligned}
\tag{4б}
$$

$$
\begin{aligned}
&\frac{\partial^2 U}{\partial (r_{k-1,k-1/2}^{(1,2)})^2} \cdot \frac{\partial (r_{k-1,k-1/2}^{(1,2)})}{\partial z} \cdot (\Delta z_{k-1}^{(1)} - \Delta z_{k-1/2}^{(2)}) + \frac{\partial^2 U}{\partial (r_{k,k-1/2}^{(1,2)})^2} \cdot \frac{\partial r_{k,k-1/2}^{(1,2)}}{\partial z} \cdot (\Delta z_k^{(1)} - \Delta z_{k-1/2}^{(2)}) - \frac{\partial^2 U}{\partial (r_{k-1/2,k-1/2}^{(2,3)})^2} \cdot \frac{\partial r_{k-1/2,k-1/2}^{(2,3)}}{\partial z} \cdot (\Delta z_{k-1/2}^{(2)} - \Delta z_{k-1/2}^{(3)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{1/2,1/2}^{(2,3)})^2} \cdot \frac{\partial (r_{1/2,1/2}^{(2,3)})}{\partial z} \cdot (\Delta z_{1/2}^{(2)} - \Delta z_{1/2}^{(3)}) - \frac{\partial^2 U}{\partial (r_{1/2,k}^{(3,4)})^2} \cdot \frac{\partial r_{1/2,k}^{(3,4)}}{\partial z} \cdot (\Delta z_{1/2}^{(3)} - \Delta z_k^{(4)}) - \frac{\partial^2 U}{\partial (r_{1/2,1}^{(3,4)})^2} \cdot \frac{\partial r_{1/2,1}^{(3,4)}}{\partial z} \cdot (\Delta z_{1/2}^{(3)} - \Delta z_1^{(4)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{3/2,3/2}^{(2,3)})^2} \cdot \frac{\partial (r_{3/2,3/2}^{(2,3)})}{\partial z} \cdot (\Delta z_{3/2}^{(2)} - \Delta z_{3/2}^{(3)}) - \frac{\partial^2 U}{\partial (r_{1/2,1}^{(3,4)})^2} \cdot \frac{\partial r_{1/2,1}^{(3,4)}}{\partial z} \cdot (\Delta z_{1/2}^{(3)} - \Delta z_1^{(4)}) - \frac{\partial^2 U}{\partial (r_{1/2,2}^{(3,4)})^2} \cdot \frac{\partial r_{1/2,2}^{(3,4)}}{\partial z} \cdot (\Delta z_{1/2}^{(3)} - \Delta z_2^{(4)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{5/2,5/2}^{(2,3)})^2} \cdot \frac{\partial (r_{5/2,5/2}^{(2,3)})}{\partial z} \cdot (\Delta z_{5/2}^{(2)} - \Delta z_{5/2}^{(3)}) - \frac{\partial^2 U}{\partial (r_{5/2,2}^{(3,4)})^2} \cdot \frac{\partial r_{5/2,2}^{(3,4)}}{\partial z} \cdot (\Delta z_{5/2}^{(3)} - \Delta z_2^{(4)}) - \frac{\partial^2 U}{\partial (r_{5/2,3}^{(3,4)})^2} \cdot \frac{\partial r_{5/2,3}^{(3,4)}}{\partial z} \cdot (\Delta z_{5/2}^{(3)} - \Delta z_3^{(4)}) = 0
\end{aligned}
\tag{4в}
$$

$$
\begin{aligned}
&\frac{\partial^2 U}{\partial (r_{k-1/2,k-1/2}^{(2,3)})^2} \cdot \frac{\partial (r_{k-1/2,k-1/2}^{(2,3)})}{\partial z} \cdot (\Delta z_{k-1/2}^{(2)} - \Delta z_{k-1/2}^{(3)}) - \frac{\partial^2 U}{\partial (r_{k-1/2,k-1}^{(3,4)})^2} \cdot \frac{\partial r_{k-1/2,k-1}^{(3,4)}}{\partial z} \cdot (\Delta z_{k-1/2}^{(3)} - \Delta z_{k-1}^{(4)}) - \frac{\partial^2 U}{\partial (r_{k-1/2,k}^{(3,4)})^2} \cdot \frac{\partial r_{1/2,1}^{(3,4)}}{\partial z} \cdot (\Delta z_{k-1/2}^{(3)} - \Delta z_k^{(4)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{1/2,1/2}^{(l-2,l-1)})^2} \cdot \frac{\partial (r_{1/2,1/2}^{(l-2,l-1)})}{\partial z} \cdot (\Delta z_{1/2}^{(l-2)} - \Delta z_{1/2}^{(l-1)}) - \frac{\partial^2 U}{\partial (r_{1/2,k}^{(l-1,l)})^2} \cdot \frac{\partial r_{1/2,k}^{(l-1,l)}}{\partial z} \cdot (\Delta z_{1/2}^{(l-1)} - \Delta z_k^{(l)}) - \frac{\partial^2 U}{\partial (r_{1/2,1}^{(l-1,l)})^2} \cdot \frac{\partial r_{1/2,1}^{(l-1,l)}}{\partial z} \cdot (\Delta z_{1/2}^{(l-1)} - \Delta z_1^{(l)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{3/2,3/2}^{(l-2,l-1)})^2} \cdot \frac{\partial (r_{3/2,3/2}^{(l-2,l-1)})}{\partial z} \cdot (\Delta z_{3/2}^{(l-2)} - \Delta z_{3/2}^{(l-1)}) - \frac{\partial^2 U}{\partial (r_{3/2,1}^{(l-1,l)})^2} \cdot \frac{\partial r_{3/2,1}^{(l-1,l)}}{\partial z} \cdot (\Delta z_{3/2}^{(l-1)} - \Delta z_1^{(l)}) - \frac{\partial^2 U}{\partial (r_{3/2,2}^{(l-1,l)})^2} \cdot \frac{\partial r_{3/2,2}^{(l-1,l)}}{\partial z} \cdot (\Delta z_{3/2}^{(l-1)} - \Delta z_2^{(l)}) = 0 \\
&\frac{\partial^2 U}{\partial (r_{5/2,5/2}^{(l-2,l-1)})^2} \cdot \frac{\partial (r_{5/2,5/2}^{(l-2,l-1)})}{\partial z} \cdot (\Delta z_{5/2}^{(l-2)} - \Delta z_{5/2}^{(l-1)}) - \frac{\partial^2 U}{\partial (r_{5/2,2}^{(l-1,l)})^2} \cdot \frac{\partial r_{5/2,2}^{(l-1,l)}}{\partial z} \cdot (\Delta z_{5/2}^{(l-1)} - \Delta z_2^{(l)}) - \frac{\partial^2 U}{\partial (r_{5/2,3}^{(l-1,l)})^2} \cdot \frac{\partial r_{5/2,3}^{(l-1,l)}}{\partial z} \cdot (\Delta z_{5/2}^{(l-1)} - \Delta z_3^{(l)}) = 0
\end{aligned}
\tag{4г}
$$

$$\frac{\partial^2 U}{\partial(r_{k-1/2,k-1/2}^{(l-2,l-1)})^2}\cdot\frac{\partial(r_{k-1/2,k-1/2}^{(l-2,l-1)})}{\partial z}\cdot(\Delta z_{k-1/2}^{(l-2)}-\Delta z_{k-1/2}^{(l-1)})-\frac{\partial^2 U}{\partial(r_{k-1/2,k-1}^{(l-1,l)})^2}\cdot\frac{\partial r_{k-1/2,k-1}^{(l-1,l)}}{\partial z}\cdot(\Delta z_{k-1/2}^{(l-1)}-\Delta z_{k-1}^{(l)})-\frac{\partial^2 U}{\partial(r_{k-1/2,k}^{(l-1,l)})^2}\cdot\frac{\partial r_{k-1/2,k}^{(l-1,l)}}{\partial z}\cdot(\Delta z_{k-1/2}^{(l-1)}-\Delta z_{k}^{(l)})=0$$

$$\frac{\partial^2 U}{\partial(r_{1/2,1}^{(l-1,l)})^2}\cdot\frac{\partial(r_{1/2,1}^{(l-1,l)})}{\partial z}\cdot(\Delta z_{1/2}^{(l-1)}-\Delta z_{1}^{(l)})+\frac{\partial^2 U}{\partial(r_{3/2,1}^{(l-1,l)})^2}\cdot\frac{\partial r_{3/2,1}^{(l-1,l)}}{\partial z}\cdot(\Delta z_{3/2}^{(l-1)}-\Delta z_{1}^{(l)})-f^{вн}=0$$

$$\frac{\partial^2 U}{\partial(r_{3/2,2}^{(l-1,l)})^2}\cdot\frac{\partial(r_{3/2,2}^{(l-1,l)})}{\partial z}\cdot(\Delta z_{3/2}^{(l-1)}-\Delta z_{2}^{(l)})+\frac{\partial^2 U}{\partial(r_{5/2,2}^{(l-1,l)})^2}\cdot\frac{\partial r_{5/2,2}^{(l-1,l)}}{\partial z}\cdot(\Delta z_{5/2}^{(l-1)}-\Delta z_{2}^{(l)})-f^{вн}=0$$

$$\frac{\partial^2 U}{\partial(r_{5/2,3}^{(l-1,l)})^2}\cdot\frac{\partial(r_{5/2,3}^{(l-1,l)})}{\partial z}\cdot(\Delta z_{5/2}^{(l-1)}-\Delta z_{3}^{(l)})+\frac{\partial^2 U}{\partial(r_{7/2,3}^{(l-1,l)})^2}\cdot\frac{\partial r_{7/2,3}^{(l-1,l)}}{\partial z}\cdot(\Delta z_{7/2}^{(l-1)}-\Delta z_{3}^{(l)})-f^{вн}=0 \qquad (4д)$$

$$\frac{\partial^2 U}{\partial(r_{k-1/2,k}^{(l-1,l)})^2}\cdot\frac{\partial(r_{k-1/2,k}^{(l-1,l)})}{\partial z}\cdot(\Delta z_{k-1/2}^{(l-1)}-\Delta z_{k}^{(l)})+\frac{\partial^2 U}{\partial(r_{1/2,k}^{(l-1,l)})^2}\cdot\frac{\partial r_{1/2,k}^{(l-1,l)}}{\partial z}\cdot(\Delta z_{1/2}^{(l-1)}-\Delta z_{k}^{(l)})-f^{вн}=0$$

Здесь серия уравнений (4а) соответствует уравнениям баланса сил в проекции на ось OZ для атомов первого слоя, (4б), (4в) – для атомов второго и третьего слоев, (4г), (4д) – для атомов предпоследнего $(l-1)$-ого и последнего l-ого слоев. Системы уравнений баланса для других проекций имеют аналогичную структуру. В соответствии с записанными уравнениями, постановка граничных условий допускает несколько вариантов. Например, можно задавать величину прикладываемой внешней силы $f^{вн}$ и находить смещения атомов, считая атомы последнего слоя закрепленными, а можно задавая смещения атомам первого слоя находить смещения атомов в остальных слоях, при этом системы уравнений принимают вид:

$$\hat{L}_{mn}(U, r_{mn}, q_t)\cdot\Delta\vec{Q}=0,\ m,n=1,2,\ldots,N,\ t=1,2,3, \qquad (5)$$

где $\hat{L}_{mn}(U, r_{mn}, q_t)$ – дифференциально-матричный оператор, r_{mn} – расстояние между m-ым и n-ым атомами, q_t – цилиндрическая координата, $\Delta\vec{Q}$ – вектор столбец перемещений атомов, N – число атомов УНТ. Следует обратить внимание на тот факт, что система (5) не является однородной, поскольку в данной постановке задачи смещения атомов первого и последнего слоев являются заданными величинами. В числе важных особенностей системы уравнений (5) необходимо отметить структуру дифференциально-матричного оператора $\hat{L}_{mn}(U, r_{mn}, q_t)$, которая легко приводится к ленточному типу. При этом ширина ленты ς зависит от степени рассматриваемого приближения и равняется числу атомов УНТ, заключенных в соответствующем круге приближения. С учетом сказанного, вычислительная сложность задачи в рассмотренной постановке оказывается порядка $O(N\cdot\varsigma^2)$, что фактически соответствует $O(N)$.

Апробация разработанного метода проводилась применительно к трем УНТ типа «кресло» (5,5) различной длины d, содержащим 200, 400 и 800 атомов. Процедура внешнего нагружения сводилась к пошаговому перемещению первого слоя атомов УНТ, с величиной шага $\eta = \Delta d / d = 0{,}1\%$. В качестве потенциала межатомарного взаимодействия был выбран потенциал Леннарда-Джонса с параметрами, отвечающими характеристикам углеродной связи [1]. При каждом шаге смещения первого слоя атомов УНТ итерационные процедуры поиска равновесных конфигураций продолжались до тех пор, пока в результате p-ой итерации максимальная величина относительной погрешности в перемещении атомов не превышала уровня ε = 3%. Предварительный анализ результатов, полученных вплоть до значений относительной деформации в 10%, позволяет констатировать высокую эффективность метода, высокую скорость итерационной сходимости и практически линейный характер вычислительной сложности.

Литература

[1]. Mastny E.A., Pablo J.J. Melting line of the Lennard-Jones system, infinite size and full potential, J. Chem. Phys., 2007, vol. 127, pp. 1063–1071.

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Тихонова Татьяна Сергеевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: tatjasha1802@yandex.ru

Логинов Борис Михайлович – д-р физ.-мат. наук, зав. каф. КФ МГТУ им. Н.Э. Баумана. E-mail: loginov@kaluga.ru

В.Е. Вершинин, С.С. Гришунов, М.Б. Логинова

РАЗРАБОТКА СИСТЕМЫ РАСПОЗНАВАНИЯ И КЛАССИФИКАЦИИ МНОГОМЕРНЫХ ОБЪЕКТОВ ПЕРЕСЕКАЮЩИХСЯ КЛАССОВ НА ОСНОВЕ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время значительные усилия исследователей в области искусственного интеллекта направлены на разработку методов решения задач классификации и распознавания объектов по плохо обусловленной исходной информации. Подобные задачи возникают при обработке зашумленных сигналов с датчиков технологических процессов, результатов социологических опросов, прогнозировании в геологии, диагностике в биологии и медицине.

Затрудняющим условием распознавания объектов зачастую является пересечение классов объектов по всем количественным и качественным признакам, вследствие чего неприменимы вероятностно-статистические методы анализа информации.

Как правило, решение отмеченного класса задач осуществляется на основе создаваемых экспертных систем, база знаний которых с неизбежностью включает интегрированный опыт экспертов, который, в свою очередь может содержать скрытые противоречия и не учитывать все пересечения ветвей решений и комбинации значений признаков и атрибутов, что, в конечном счете, может существенно снижать ценность получаемых результатов.

Таким образом, разработка новых подходов, методов и моделирование на их основе процессов классификации, распознавания и диагностики объектов по совокупности их количественных и качественных признаков в разнотипном признаковом пространстве в условиях пересечения и многозначности классов объектов, когда, в силу изначальной неопределенности оказывается невозможным применять методы статистического анализа, основанные на аксиоматической теории вероятностей, несомненно, является актуальной и важной задачей.

Способы вычисления функций принадлежности объектов к нечетким множествам, нечеткие меры доверия, возможности и необходимости событий и меры учета неопределенности в ситуациях, когда недостаточна модель полной группы несовместных событий, на которых основана теория вероятностей, а также способы вычисления меры необходимости пересечения и объединения множеств, способов свертки нечетких множеств, получения критерия для ранжирования многозначных объектов

и для сравнения разнотипных признаков по надежности диагностики неизвестных объектов достаточно хорошо изучены и известны [1].

В настоящей работе проводится описание разработанных систем распознавание и классификации многомерных объектов пересекающихся классов на основе представлений теории нечетких множеств. Разработанная система состояла из двух модулей – модуля предобработки и модуля распознавания.

Задачей модуля предобработки являлось создание опорных вектор-функций принадлежности, представляющих собой интегральные характеристики экспертных баз данных для каждого класса.

Модуль предобработка содержал три основных блока – блок экспертной базы данных, блок вектор-функций принадлежности и блока предобработки данных.

В экспертную базу данных помещались исходные массивы $\{\boldsymbol{P_K}\}$ составленные из $\boldsymbol{N}$ – мерных векторов $\boldsymbol{K}$ классов:

$$\vec{X}^{(N)}_{K,P_k} = \left(x^{(1)}_{k,p}, x^{(2)}_{k,p}, \ldots, x^{(N)}_{k,p}\right)^T ; \text{ p = 1, 2, …, } P_k \text{ ; k = 1, 2, … , } \boldsymbol{K}.$$

Массивы векторов $\vec{X}^{(N)}_{K,P_k}$ поступали в блок предобработки, где для каждого из них производился расчет массива вектор-функций принадлежности:

$$\vec{M}^{(N)}_{K,P_k} = \left(\mu^{(1)}_{k,p}(x^{(1)}), \mu^{(2)}_{k,p}(x^{(2)}), \ldots, \mu^{(N)}_{k,p}(x^{(N)})\right)^T,$$
$$\text{p = 1, 2, …, } P_k \text{ ; k = 1, 2, … , } \boldsymbol{K},$$

на базе которого, для каждого класса производился расчет опорного массива интегральных экспертных вектор-функций принадлежности:

$$\vec{H}^{(N)}_K = \left(\eta^{(1)}_k(x^{(1)}), \eta^{(2)}_k(x^{(2)}), \ldots, \eta^{(N)}_k(x^{(N)})\right)^T, \text{ k = 1, 2, … , } \boldsymbol{K},$$

где $\eta^{(n)}_k(x^{(n)}) = \mu^{(n)}_{k,1}(x^{(n)}) \cup \mu^{(n)}_{k,2}(x^{(n)}) \cup \ldots \cup \mu^{(n)}_{k,P_k}(x^{(n)}) = \bigcup_{p=1}^{P_k} \mu^{(n)}_{k,p}(x^{(n)})$, p = 1, 2, …, P_k ; k = 1, 2, … , $\boldsymbol{K}$.

Совокупности интегральных экспертных вектор-функций принадлежности $\vec{H}^{(N)}_K$, полученные на основе ***ЭБД*** для каждого класса помещались далее в блок векторных функций принадлежности (***ВФП***) и

представляли собой массив опорных интегральных экспертных ***ВФП*** необходимый для последующих расчетов.

В задачи интерфейса модуля предобработки, помимо традиционных – ввод-вывод, просмотр и редактирование содержимого и характеристик блоков, входило также предоставление возможности выбора параметров и типа огибающей контура вектор-функции принадлежности, а также предоставление возможности выбора процедуры вычисления теоретико-множественной операции объединения. В работе было рассмотрено три типа контура огибания ВФП: треугольный, гиперболический и колоколообразный, и, четыре типа процедур вычисления теоретико-множественной операции объединения введенных в теорию нечетких множеств: Заде, Хамачером, Ягером, и Дюбуа-Праде.

Назначение модуля распознавания и классификации следует из его названия. Этот модуль состоял из четырех блоков: блока транспортировки, блока свертки, блока ранжирования и блока архива решений.

Значения координат входного вектора $\vec{Z}^{(N)} = \left(z^{(1)}, z^{(2)}, \ldots, z^{(N)}\right)^T$, подлежащего распознаванию и классификации, поступали в транспортный блок, и, после проверки на целостность и непротиворечивость передавались в модуль предобработки, в блок ВФП, где на основании массива опорных интегральных экспертных вектор-функций принадлежности:

$$\vec{H}_K^{(N)} = \left(\eta_k^{(1)}(x^{(1)}), \eta_k^{(2)}(x^{(2)}), \ldots, \eta_k^{(N)}(x^{(N)})\right)^T, \text{ k = 1, 2, … , } \boldsymbol{K},$$

производился расчет значений для каждого класса ***K*** векторов-функций принадлежности:

$$\vec{M}_K^{(N)}(z) = \left(\mu_k^{(1)}(z^{(1)}), \mu_k^{(2)}(z^{(2)}), \ldots, \mu_k^{(N)}(z^{(N)})\right)^T, \text{ k = 1, 2, … , } \boldsymbol{K}.$$

Рассчитанные значения ВФП $\vec{M}_K^{(N)}(z)$ возвращались в модуль распознавания и классификации в транспортный блок, и, после проверки на целостность и непротиворечивость передавались далее в блок свертки, в котором для каждого класса ***K*** , для входного вектора $\vec{Z}^{(N)}$ производился расчет свертки $M_K(z)$ на основе выражения:

$$M_K(z) = \mu_k^{(1)}(z^{(1)}) \cap \mu_k^{(2)}(z^{(2)}) \cap \ldots \cap \mu_k^{(N)}(z^{(N)}) = \bigcap_{n=1}^{N} \mu_k^{(n)}(z^{(n)}),$$

$$k = 1, 2, \ldots, \boldsymbol{K}.$$

Полученные значения свертки $M_K(z)$ поступали далее в блок ранжирования, в котором производилось их ранжирование и упорядочение с последующим выводом значений $M_K(z)$ в архив решений и на экран.

Интерфейс модуля распознавания и классификации, по мимо стандартного набора процедур связанных с вводом, выводом, просмотром и редактированием, обеспечивал возможность выбора видов и типов опорных ВФП, и возможность выбора типа процедур вычисления теоретико-множественной операции пересечения введенных в теорию нечетких множеств: Заде, Хамачером, Ягером, и Дюбуа-Праде.

Список литературы

[1] Zimmermann H.Z. Fuzzy Set Theory and Its Applications. London, Kluwer Academic Publishers, 2007, 499 p.

Вершинин Владислав Евгеньевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: goliathonline@mail.ru

Гришунов Степан Сергеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: stepangrishunov@yandex.com

Логинова Мария Борисовна - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: loginovamb@yandex.ru

Е.М. Аксютина, С.А. Гинзгеймер, Р.В. Клюквин, С.В. Рыбкин

РАСЧЕТ СМЕЩЕНИЙ ГРАНИЦ ЗОНЫ ПРОВОДИМОСТИ ПРИ МЕХАНИЧЕСКОМ ВОЗДЕЙСТВИИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В случае, если на кристаллическую структуру, имеющую свободные электроны в зоне проводимости (электронная проводимость), или при неполном заполнении электронами валентной зоны (дырочная проводимость) действует внешнее электрическое поле, приводящее к нарушению состояния термодинамического равновесия, то оно порождает процесс переноса заряда. Носители заряда под действием электрического поля дрейфуют в направлении противоположном направлению электрического поля для электронной проводимости и в направлении, совпадающим с направлением поля, в случае дырочной проводимости. Коэффициент μ_{ij}, связывающий компоненты дрейфовой скорости носителей v_d^i с компонентами внешнего электрического поля E_j называется подвижностью:

$$v_d^i = \mu_{ij} E_j , \tag{1}$$

Плотность электрического тока связана с дрейфовой скоростью:

$$j_i = qnv_d^i , \tag{2}$$

где n – концентрация носителей заряда, а q - величина заряда одного носителя.

Тогда компоненты вектора плотности тока могут быть выражены:

$$j_i = qn\mu_{ij} E_j , . \tag{3}$$

Входящая в состав правой части (3) компонента $qn\mu_{ij}$ – называется удельной проводимостью и является величиной обратной удельному сопротивлению:

$$\frac{1}{\rho_{ij}} = \sigma_{ij} = qn\mu_{ij} . \tag{4}$$

При деформации кристаллических структур наблюдается зависимость удельного сопротивления от механического напряжения (тензорезистивный эффект).

Области тензорезистивного эффекта в указанном случае соответствует диапазон малых давлений, в котором сопротивление линейно падает с ростом . Численно эта зависимость может быть выражена:

$$\frac{\Delta\rho_{ij}}{\rho_0} = -\frac{\Delta\sigma_{ij}}{\sigma_0} = \sum_{k,l=1}^{3} \pi_{ijkl} X_{kl} \,, \tag{5}$$

где ρ_0 и σ_0 – удельное сопротивление и удельная проводимость недеформированного проводника, $\Delta\rho_{ij}$ и $\Delta\sigma_{ij}$ – изменения этих величин, вызванные деформацией, π_{ijkl} - компоненты тензора пьезосопротивления 4-го ранга, X_{kl} - компоненты тензора механического напряжения 2-го ранга.

Вследствие симметрии тензор $\hat{T}$ является симметричным и имеет только 6 независимых компонент, которые можно считать компонентами шестимерного вектора:

$$X_1 = X_{11},\ X_2 = X_{22},\ X_3 = X_{33},\ X_4 = X_{23},\ X_5 = X_{31},\ X_6 = X_{12}, \tag{6}$$

то же самое справедливо для тензоров $\hat{\rho}$ и $\hat{\sigma}$. Тогда в шестимерном пространстве:

$$\frac{\Delta\rho_i}{\rho_0} = -\frac{\Delta\sigma_i}{\sigma_0} = \sum_{j=1}^{6} \pi_{ij} X_j \ . \tag{7}$$

В случае гидростатического давления:

$$\frac{\Delta\rho}{\rho_0} = -\frac{\Delta\sigma}{\sigma_0} = \left(\pi_{11} + 2\pi_{12}\right) X \,. \tag{8}$$

Зависимость удельной проводимости от напряжения может быть выражена:

$$\Delta\rho\left(X\right) = \frac{d\sigma}{dX}\Delta X = q\mu\frac{\partial n}{\partial X}\Delta X + qn\frac{\partial \mu}{\partial X}\Delta X \,. \tag{9}$$

Однако, данные о влиянии давления на концентрацию носителей заряда в диапазоне малых значений X (до 10^8Па) говорят об очень слабой зависимости $n\left(X\right)$, таким образом можно считать $\frac{\partial n}{\partial X} = 0$. Тогда из (9) следует:

$$\frac{\Delta\sigma\left(X\right)}{\sigma_0} = \frac{\Delta\mu\left(X\right)}{\mu_0}, \tag{10}$$

что позволяет оценить влияние механического напряжения на подвижность носителей заряда, исходя из экспериментальных данных о пьезоспротивлении материала.

Тогда для случая гидростатического давления:

$$\frac{\Delta\mu(X)}{\mu_0} = -(\pi_{11} + 2\pi_{12})X \ , \tag{11}$$

что дает для электронной проводимости $\left(\frac{\Delta\mu(X)}{\mu_0}\right)_n = -5.2\cdot10^{-11}\,Па^{-1}\cdot X$ для дырочной проводимости $\left(\frac{\Delta\mu(X)}{\mu_0}\right)_p = -4.4\cdot10^{-11}\,Па^{-1}\cdot X$, при этом необходимо учитывать, что X принимает отрицательные значения в случае сжатия и положительные в случае растяжения.

Деформации кристаллических структур вносят существенные изменения в их физические свойства. Изменяется электропроводность материала, подвижность носителей заряда, проявляется тензорезистивный эффект. Это связано с деформацией кристаллической решетки, изменением межатомного расстояния, а, следовательно, сдвигом энергетических зон, определяющих электрические свойства вещества. Действительно, взаимное расположение и ширина валентной и запрещенных зон, а также зоны проводимости характеризует проводник, диэлектрик или полупроводник.

Напряжение $\hat{\sigma}$ и деформация $\hat{\varepsilon}$ в кристаллах описываются тензорами 2-го ранга, которые связаны между собой тензором упругости 4-го ранга:

$$\sigma_{ij} = \sum_{ij} c_{ijkl}\cdot\varepsilon_{kl} \ . \tag{12}$$

Для расчета деформации при известных значениях напряжений используется:

$$\varepsilon_{kl} = \sum_{ij} s_{klij}\cdot\sigma_{ij} \ , \tag{13}$$

где s_{klij} - компоненты тензора податливости, который связан с тензором упругости:

$$\hat{s} = \hat{c}^{-1} . \tag{14}$$

В состав каждого из тензоров $\hat{s}$ и $\hat{c}$ входит 81 компонента, однако вследствие симметрии независимыми являются только 21 из них, в этом случае более удобным является представление в следующем виде:

$$\sigma_j = \sum_i c_{ij}\varepsilon_i \left(i, j = 1,2,3,...6\right), \tag{15}$$

$$\varepsilon_j = \sum_i s_{ij}\sigma_i \left(i, j = 1,2,3,...6\right). \tag{16}$$

Для кристаллов кубической сингонии, к которым относятся алмазоподобные кристаллы, их количество сокращается до 3: c_{11}, $c_{12,}$ c_{44} и s_{11}, $s_{12,}$ s_{44}:

$$\hat{c} = \begin{pmatrix} c_{11} & c_{12} & c_{12} & 0 & 0 & 0 \\ c_{12} & c_{11} & c_{12} & 0 & 0 & 0 \\ c_{12} & c_{12} & c_{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & c_{44} & 0 & 0 \\ 0 & 0 & 0 & 0 & c_{44} & 0 \\ 0 & 0 & 0 & 0 & 0 & c_{44} \end{pmatrix} \tag{17}$$

$$\hat{s} = \begin{pmatrix} s_{11} & s_{12} & s_{12} & 0 & 0 & 0 \\ s_{12} & s_{11} & s_{12} & 0 & 0 & 0 \\ s_{12} & s_{12} & s_{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & s_{44} & 0 & 0 \\ 0 & 0 & 0 & 0 & s_{44} & 0 \\ 0 & 0 & 0 & 0 & 0 & s_{44} \end{pmatrix} \tag{18}$$

где компоненты отличные от нуля связаны между собой:

$$s_{11} = \frac{c_{11} + c_{12}}{c_{11}^2 + c_{11}c_{12} - 2c_{12}^2}$$

$$s_{12} = \frac{c_{12}}{c_{11}^2 + c_{11}c_{12} - 2c_{12}^2} \tag{19}$$

$$s_{44} = \frac{1}{c_{44}}$$

Усилие, приводящее к деформации кристалла, может прикладываться в произвольном направлении и, поэтому, его пересчет в систему координат, связанную с осями кристалла.

Если усилие прикладывается в направлении вектора *(x',y',z')*, то для его перевода в систему координат *(x,y,z)* понадобится матрица трансформации $\hat{u}$, которая определяется двумя поворотами: сначала плоскость *xy* поворачивается вокруг оси *z* на угол $-\varphi$, а затем вокруг оси *y* на угол $-\theta$:

$$\hat{u} = \begin{pmatrix} \cos\varphi & -\sin\varphi\cos\theta & \sin\varphi\sin\theta \\ \sin\varphi & \cos\varphi\cos\theta & -\cos\varphi\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \tag{20}$$

Тогда тензор деформаций в системе координат, связанной с осями кристалла:

$$\hat{\sigma}^{\hat{e}\eth} = \hat{u}\hat{\sigma}\hat{u}^{T} \tag{21}$$

В настоящей работе были проведены расчеты тензоров деформации для алмазоподобных кристаллов на примере Si для случаев приложения усилия *P* вдоль осей [100] и [110]:

$$\hat{\varepsilon}_{\langle 100\rangle} = \begin{pmatrix} s_{11}\cdot P & 0 & 0 \\ 0 & s_{12}\cdot P & 0 \\ 0 & 0 & s_{12}\cdot P \end{pmatrix} \tag{22}$$

$$\hat{\varepsilon}_{\langle 110\rangle} = \begin{pmatrix} (s_{11}+s_{12})\cdot P/2 & s_{44}\cdot P/4 & 0 \\ s_{44}\cdot P/4 & (s_{11}+s_{12})\cdot P/2 & 0 \\ 0 & 0 & s_{12}\cdot P \end{pmatrix} \tag{23}$$

Деформации в кристаллических структурах приводят к изменению межатомного расстояния и, соответственно, параметров кристаллической решетки:

$$x_i' = x_i + \sum_j \varepsilon_{ij} x_i^j, i = 1,2,3\ , \tag{24}$$

где x – вектор недеформированной решетки, а x' – вектор деформированной решетки, а ε_{ij} - компоненты тензора деформаций.

Энергия электрона изменяется при деформации кристалла на величину:

$$\Delta\mathcal{E} = \mathcal{E} - \mathcal{E}_0 = \sum_{ij} \Xi_{ij}\varepsilon_{ij}\ , \tag{25}$$

где $\mathcal{E}_0$ - энергия при отсутствии деформации, Ξ_{ij} – компоненты тензора деформационного потенциала, ε_{ij} – компоненты тензора деформаций.

Известно, что минимумы зоны проводимости недеформированного кремния (долины) в пространстве квазиимпульсов при заданной величине

энергии имеют вид эллипсоидов вращения и ориентированы вдоль осей. В общем виде выражение для определения смещение края зоны проводимости *i*-й долины *j*-го типа (*j*=*X, L*) при деформации выглядит:

$$\Delta \mathcal{E}_c^{(i,j)} = \Xi_d^{(j)} \left(\varepsilon_{xx} + \varepsilon_{yy} + \varepsilon_{zz} \right) + \Xi_u^{(j)} \mathrm{a}_i^T \hat{\varepsilon} \mathrm{a}_i = \Delta^{(d)} + \Delta^{(u)}, \qquad (26)$$

где a_i единичный вектор *i*-ой долины минимальный для *j*-го типа, $\Xi_d^{(j)}$ и $\Xi_u^{(j)}$ - постоянные деформационного потенциала зоны проводимости *j*-го типа. Первое слагаемое $\Delta^{(d)}$ сдвигает энергетические уровни все долин одинаково и пропорциональна гидростатическому напряжению $\varepsilon_{xx} + \varepsilon_{yy} + \varepsilon_{zz}$. Разница в положениях энергетических уровней возникает благодаря второму слагаемому $\Delta^{(u)}$. Полученные значения $\mathrm{a}_i^T \hat{\varepsilon} \mathrm{a}_i$ для долин в случаях различных направлений одноосной деформации для кремния приведены в табл. 1.

Таблица 1. Значения компонент тензора податливости

	s_{11}	s_{12}	s_{44}
Si	$-21.3 \cdot 10^{-12}$ м^2/Н	$7.67 \cdot 10^{-12}$ м^2/Н	$12.6 \cdot 10^{-12}$ м^2/Н

Таким образом, имея значения компонент тензора деформаций, согласно (26) можно рассчитать смещения границы зоны проводимости в зависимости от прикладываемого усилия.

Полученные результаты показывают, что наблюдаются отличия в поведении границ зоны проводимости для разных энергетических зон и различных направлений приложения усилий. Это, в свою очередь, может позволить выбирать необходимую ориентацию кристаллической структуры с целью получения необходимых свойств материала.

Аксютина Екатерина Михайловна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: aks.kate93@gmail.com

Гинзгеймер Сергей Александрович - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: sagynzgaymer@mail.ru

Клюквин Роман Владимирович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: pomanklg@gmail.com

Рыбкин Сергей Владимирович - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ribkinsv@kaluga.ru

Ю.С. Белов, А.К. Жуков, Ю.Г. Шевцов

РЕШЕНИЕ ЗАДАЧ ПАРНОГО ВЗАИМОДЕЙСТВИЯ ДИСЛОКАЦИЙ НА ОСНОВЕ ИТЕРАЦИОННОГО ПРОЦЕССА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Процессы пластической деформации и деформационного упрочнения кристаллических материалов непосредственно связаны с движением и взаимодействием дислокаций.

Анализ результатов исследований множественного взаимодействия дислокаций показывает, что закономерности процессов могут зависеть от целого ряда особенностей и характеристик, при этом степень адекватности используемых приближений зависит от того насколько полно и корректно удается воспроизводить следующие три положения. Во-первых, дислокации по своей природе являются гибкими и способными плавно изменять свою форму, в соответствии с локальными характеристиками полей внутренних напряжений. Во-вторых, движение дислокаций реализуется по определенным системам скольжения, в соответствии с кристаллографической структурой исследуемого материала. В-третьих, дислокации создают поля внутренних напряжений, расчет которых в случае криволинейных дислокаций требует значительных машинных ресурсов.

Взаимное расположение дислокаций удобно характеризовать заданием параметра сближения h. Изменяя определенным образом величину этого параметра, например, меняя h от $-\infty$ до $+\infty$, можно имитировать процесс сближения и прохождения дислокаций друг через друга при их движении. Процесс взаимодействия дислокаций рассмотрим в квазистатическом приближении, полагая, что обе дислокации испытывают сопротивление своему движению типа сухого трения: $f_i^{\,0} = \tau_i^0 b_i$, где τ_i^0 - стартовое напряжение для i-ой взаимодействующей дислокации. Очевидно, две первоначально прямолинейные дислокации при сближении начнут искривляться только при:

$$\left|h^{(i)}\right| \le \frac{G_j}{2\pi\tau_i^{\,0}},$$

где $i \neq j$, т.е. когда сила взаимодействия в точке их скрещивания превысит силу трения. Искривление дислокаций будем характеризовать смещениями $U_1(Z)$ и $U_2(X)$ от их первоначальной прямолинейной конфигурации. При искривлении конфигурации дислокаций должны описываться соотношениями:

$$F_i + \sum_{i \neq j} F_{ij}^{B3} + F_i^c - f_i^{\,0} sign\left\{F_i + \sum_{i \neq j} F_{ij}^{B3} + F_i^c\right\} = 0 \quad ; \; i = 1,2,\ldots,k, \tag{1}$$

$$U_2\left(\pm x^*\right) = 0, \; \left.\frac{\partial U_2}{\partial x}\right|_{x = \pm x^*} = 0. \tag{2}$$

$$U_2(\pm x_i^{**}) = U_2^{**} \; ; \; \left.\frac{\partial U_2}{\partial x}\right|_{x = \pm x_i^{**}} = \pm U_{2x}^{**} \; ; \; \left.\frac{\partial U_2}{\partial x}\right|_{x = 0} = 0, \tag{3}$$

где F_i - внешняя сила, действующая на *i*-ую дислокацию; F_{ij}^{B3} - сила, с которой *j*-ая дислокация действует на *i*-ую дислокацию; F_i^C - сила самодействия *i*-ой дислокации; f_i^0 предельная сила сопротивления решетки, определяющее стартовое напряжение движения дислокации.

Компоненты силы (f_i) действующей на дислокационный элемент dl_k в поле напряжений σ_{nj} задаются соотношением: $f_i = e_{ijk} b_n \sigma_{nj} dl_k$, где e_{ijk} – тензор Леви-Чевитта, пересчет компонент тензора напряжений при переходе из одной системы координат в другую производился в соответствии со стандартной процедурой $\tilde{\sigma}_{ij} = \alpha_{im}\alpha_{jn}\sigma_{mn}$, где α_{ij} - матрица перехода из одной системы координат в другую: $\tilde{r}_i = \alpha_{ij} r_j$. При решении уравнений (1) дислокации рассматриваются состоящими из трех элементов двух полубесконечных прямых: $z^* \le |z| < \infty$ для первой дислокации и $x^* \le |x| < \infty$ для второй и отрезков криволинейной формы на участках $|z| < z^*$ и $|x| < x^*$, которые определяются набором опорных точек $(x_k, U_2(x_k))$ и $(z_k, U_2(z_k))$. На начальных этапах взаимодействия дислокаций при нарастающих значениях x^* и z^* краевые условия задаются в соответствии с (2):

$$U_1^{(n)}(\pm Z_n^*) = \left.\frac{\partial U_1}{\partial Z}\right|_{\pm Z^*{}_n} = 0 \qquad (4)$$

где n - номер, отвечающий соответствующим значениям параметра сближения $h^{(n)}$, $\pm x_n^*$, $\pm z_n^*$ интервалы на которых происходит смещение дислокаций при взаимодействии. Если при $h^{(n)} > h^{(n^*)}$ $(n > n^*)$ область смещения i-ой дислокации начинает сужаться, необходим переход к краевым условиям в форме (3):

$$\begin{gathered} U_1^{(n+1)}\left(\pm Z_{n+1}^{**}\right) = U_1^{(n)}\left(\pm Z_{n+1}^{**}\right);\ \left.\frac{\partial U_1^{(n+1)}}{\partial Z}\right|_{\pm Z_{n+1}^{**}} = \left.\frac{\partial U_1^{(n)}}{\partial Z}\right|_{\pm Z_{n+1}^{**}}, \\ U_2^{(n+1)}\left(\pm X_{n+1}^{**}\right) = U_2^{(n)}\left(\pm X_{n+1}^{**}\right);\ \left.\frac{\partial U_2^{(n+1)}}{\partial X}\right|_{\pm X_{n+1}^{**}} = \left.\frac{\partial U_{21}^{(n)}}{\partial X}\right|_{\pm X_{n+1}^{**}}. \end{gathered} \qquad (5)$$

Установление момента перехода от краевых условий (4) и (5) является важным для того, чтобы обеспечить нахождение физически корректной эволюции форм взаимодействующих дислокаций. Практика проведенных расчетов показала, что для более точного установления величины $h^{(n^*)} = h(x_{\max}^*)$ очень полезным является построение зависимостей $x^* = x^*(h)$, на которых $h\left(x_{\max}^*\right)$ является экстремальной точкой и легко определяется.

Решение уравнений (1) производилось в три этапа. Сначала находилось решение в приближении постоянного линейного натяжения при $k = 0{,}5$ и в предположении, что в процессе сближения искривляется

лишь одна из взаимодействующих дислокаций, а вторая дислокация является жесткой и остается прямолинейной в течение всего процесса взаимодействия. В этом случае система уравнений равновесия (1) сводится к одному нелинейному дифференциальному уравнению 2-ого порядка и его решение удобно проводить по методу радиуса кривизны.

Заметим только, что построение конфигурации дислокации начиналось с точек $Z = 0$ и $X = 0$, где $\partial u_1 / \partial z = 0$ и $\partial u_2 / \partial z = 0$. Путем вариации местоположения начальных точек $u_1(0)$ удовлетворялись краевые условия (4) или (5) с заданной точностью. Отметим также, что, поскольку в методе радиуса кривизны положения $k+1$ опорной точки находится по положению k-ой точки, в процессе расчета конфигурации дислокационной линии имеет место накопление ошибок. В связи с этим при расчете конфигураций дислокаций по методу радиуса кривизны использовался очень мелкий шаг, так что число опорных точек достигало 100-500. Затем рассматривалась задача о взаимодействии двух гибких дислокаций в приближении постоянного линейного натяжения. В этом случае система (1) сводилась к двум связанным интегро-дифференциальным уравнениям. Для нахождения решения в этом случае использовался итерационный метод, основанный на попеременном “замораживании” формы одной дислокации и нахождении равновесной конфигурации другой. Итерационный процесс продолжался до тех пор, пока разница в координатах последовательных приближений составляла не более 1,5%. Нахождение решения на каждом шаге итерационного процесса также проводилось по методу радиуса кривизны. Наконец, на основе полученных решений, производилась их коррекция с учетом сил самодействия. Подобная последовательность решения задачи не только облегчает поиск точного решения, но и снижает объем численных расчетов.

Проведенные расчеты показали, что процесс прохождения гибкой скользящей дислокации через плоские дислокационные скопления не сводится к продавливанию внешним напряжением гибкой дислокации по механизму Орована, а обусловлен потерей гибкой дислокацией устойчивости и происходит в динамическом режиме. Весьма важно также, что потеря устойчивости дислокации при критических значениях внешнего напряжения имеет место при весьма слабом искривлении дислокации. По этим причинам обычный критерий Орована для оценки напряжения прохождения в данном случае оказывается совершенно непригодным, поскольку приводит к ошибкам, превышающем два порядка величины.

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Жуков Антон Константинович –ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: ant_it@mail.ru

Шевцов Юрий Геннадьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: shevtsov.yuri92@gmail.com

Ю.С. Белов, С.Г. Гуров

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ВЫДЕЛЕНИЯ ГРАНИЦ ИЗОБРАЖЕНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Выделение границ (edge detection) — термин в теории обработки изображения и компьютерного зрения, частично из области поиска объектов и выделения объектов, основывается на алгоритмах, которые выделяют точки цифрового изображения, в которых резко изменяется яркость или есть другие виды неоднородностей.

В идеальном случае, результатом выделения границ является набор связанных кривых, обозначающих границы объектов, граней и оттисков на поверхности. Таким образом, применение фильтра выделения границ к изображению может существенно уменьшить количество обрабатываемых данных, из-за того, что отфильтрованная часть изображения считается менее значимой, а наиболее важные структурные свойства изображения сохраняются. Однако не всегда возможно корректно выделить границы в картинах реального мира даже средней сложности. Границы, выделенные из таких изображений, часто имеют такие недостатки как фрагментированность, отсутствие границ или наличие ложных, не соответствующих исследуемому объекту, границ.

Так как разные алгоритмы обнаружения границ работают по-разному, необходимо проанализировать, в каких ситуациях лучше тот или иной алгоритм.

Для исследования были выбраны следующие операторы:

— Оператор Марра-Хилдрета
— Оператор Кэнни

Оператор Марра-Хилдрета основан на вычислении корней оператора Лапласа, примененного к изображению, сглаженному фильтром Гаусса. Таким образом, общий алгоритм обнаружения границ Марра-Хилдрета заключается в следующем:

Сглаживание изображения фильтром Гаусса.

Применение двумерного оператора Лапласа. Эта операция эквивалентна взятию второй производной изображения.

Просмотр каждого пикселя сглаженного изображения для поиска изменений знака. Если изменение знака больше некоторого порогового значения, то этот пиксель помечается как крайний. В качестве альтернативы можно применить гистерезисную фильтрацию.

Оператор Кэнни до сих пор превосходит многие из новых алгоритмов. Данный алгоритм состоит из следующих этапов:

— Сглаживание. Размытие изображения для удаления шума. Используется фильтр, который может быть хорошо приближен к первой производной гауссиана.

— Поиск градиентов. Границы отмечаются там, где градиент изображения приобретает максимальное значение. Они могут иметь различное направление, поэтому используются четыре фильтра для обнаружения горизонтальных, вертикальных и диагональных ребер в размытом изображении.
— Подавление немаксимумов. Только локальные максимумы отмечаются как границы.
— Двойная пороговая фильтрация. Пиксели, яркость которых меньше определенного минимального порога, отбрасываются, а пиксели, яркость которых больше максимальной границы, принимаются в качестве граничных.
— Трассировка области неоднозначности. Итоговые границы определяются путём подавления всех границ, несвязанных с определенными (сильными) границами.

Сравнение алгоритмов. Необходимо определить несколько четких критериев, по которым можно оценить качество обработки изображений.

Существуют пять различных критериев, которые обычно используются для тестирования качества работы алгоритмов обнаружения границ:

Вероятность ложных пометок (пиксели помечены в качестве краевых, хотя на самом деле ими не являются);

Вероятность пропуска краевых пикселей (пиксели, которые должны быть помечены краевыми, пропущены);

Ошибка оценки угла направления границы;

Средний квадрат расстояния между вычисленными границами и реальными;

Устойчивость алгоритма к искаженным границам;

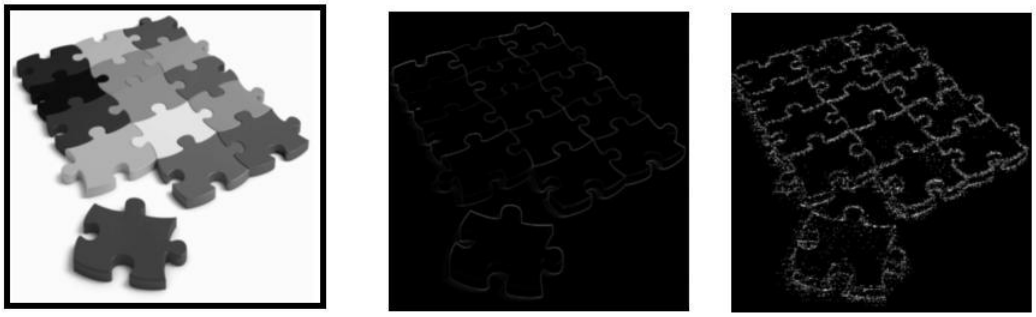


Рис. 1.

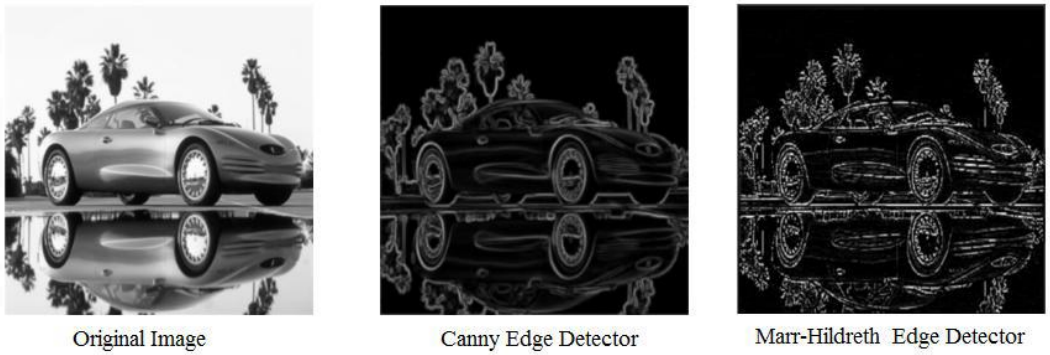


Рис. 2.

Визуально сравнивая два набора изображений (Рисунок 1, Рисунок 2), можно субъективно оценить работу выбранных алгоритмов обнаружения границ. Оператор Кэнни работает лучше, однако требует большего количества вычислений из-за сглаживания изображения фильтром Гаусса и последующего вычисления градиента.

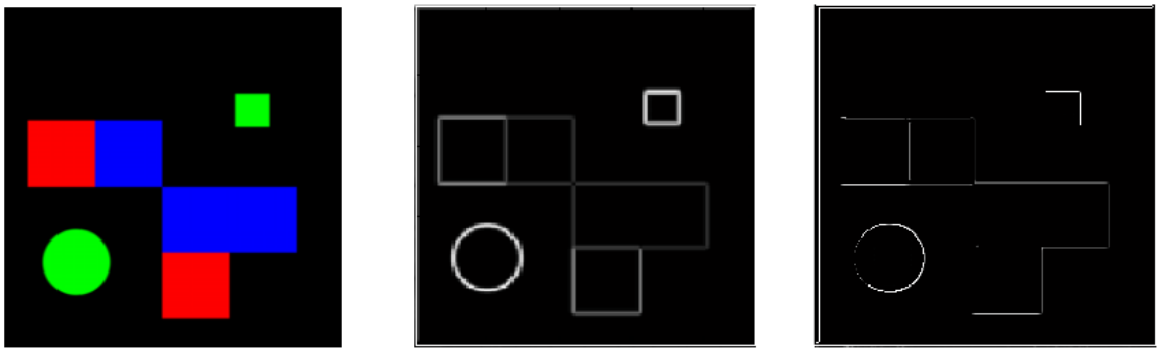


Рис. 3.

Рисунок 3 показывает способность алгоритмов обнаружения границ обрабатывать углы, а также широкий спектр наклонов границ окружности. Алгоритм Кэнни путает углы в связи с Гауссовской сглаженностью изображения. Так как направление границ меняется мгновенно, углы имеют ошибочное направление по отношению к соседним. Алгоритму Марра-Хилдрета не удается обнаружить многие видимые границы.

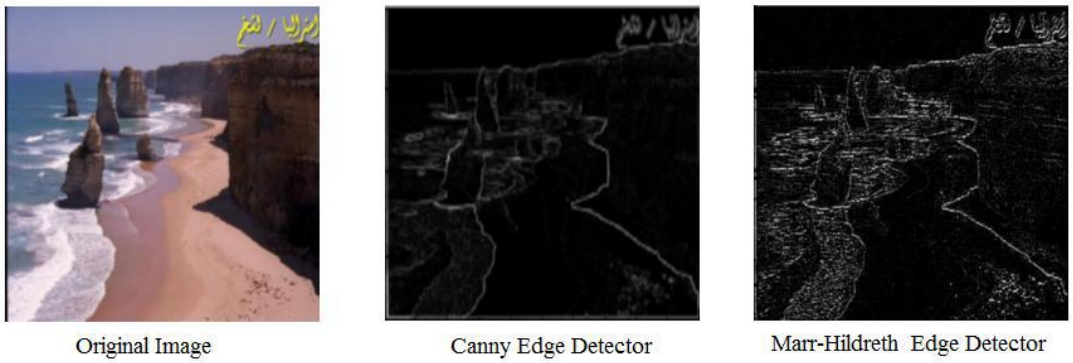


Рис. 4.

На рисунке 4 изображена береговая линия. У обоих алгоритмов возникли трудности с определением различных хребтов скалы. Пена волн также определена некорректно.

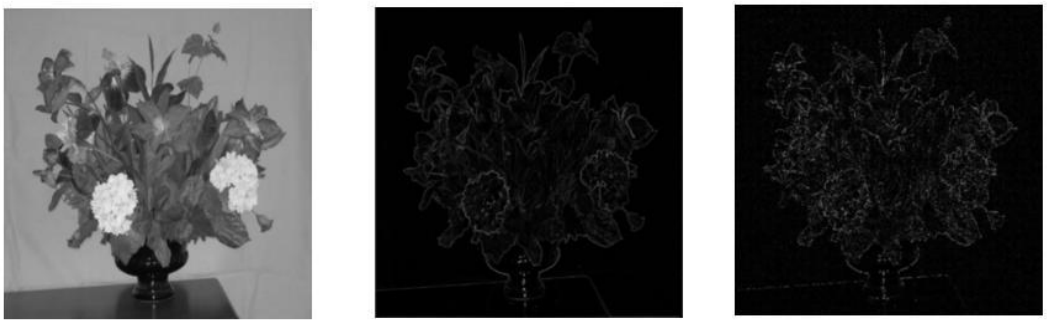


Рис. 5.

Рисунок 5 показывает более точно возможности каждого из алгоритмов. Алгоритм Марра-Хилдрета находит много границ, но они крапчатые. Алгоритм Кэнни дает хорошие очертания стола, вазы и многих цветов. Детали в середине букета пропущены, некоторые из них все же видны.

Выводы

Алгоритм Кэнни имеет три проблемы, которые необходимо решить для того, чтобы лучше определять границы: процент ошибок, локализация и отклик.

Алгоритм Марра-Хилдрета плохо справляется с локализацией, границы не всегда тонкие, но этот алгоритм намного лучше классических алгоритмов в случае с низким уровнем шума. При использовании гистерезиса данный алгоритм работает лучше. Тем не менее, алгоритм Марра-Хилдрета дает крапчатые и толстые границы.

Алгоритм Кэнни является предпочтительным, так как границы объекта получаются тонкими и непрерывными.

Список использованных источников

[1]. Petrou M., Petrou C. Image Processing: The Fundamentals, Wiley, New Jersey, 2010

[2]. Колючкин В.Я., Нгуен К.М., Чан Т.Х. Алгоритмы обработки информации всистемах технического зрения промышленных роботов. Инженерный журнал: наука и инновации, Москва, 2013

[3]. Edge detection. URL: https://en.wikipedia.org/wiki/Edge_detection (дата обращения - 22.10.2015)

[4]. R. Owens, "Lecture 6", Computer Vision IT412, 10/29/1997. URL: http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/OWENS/LECT6/node2.html (дата обращения - 22.10.2015)

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Гуров Станислав Геннадьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: gurov.it@mail.ru

А.Ю. Нестеров, Ю.С. Белов

ФОТОГРАММЕТРИЧЕСКОЕ СОЗДАНИЕ 3D ОБЪЕКТОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

3D модели широко используются в различных приложениях, включая компьютерные игры, программное обеспечение, приложения для обучения и моделирования, а так же в виртуальных картах города. Для многих из этих приложений крайне желательно, чтобы виртуальные 3D модели были основаны на реальных сценах и объектах. Ручное моделирование зарезервировано для экспертов, так как оно требует значительных навыков. По этой причине необходимо обеспечить автоматические или полуавтоматические простые в использовании методы создания 3D объектов.

Метод создания объектов на основе изображений специально разработан для сред с однородными и отражающими поверхностями, где трудно получить надежные наборы точек. Поэтому используется интерактивное приложение, которое требует ввода данных пользователем. Примитивы фигур подходят для пользовательских сегментаций в двух или более изображениях.

Первым шагом для создания 3D объектов является получение данных.

Методы получения данных образуют несколько выделенных изображений и/или облако точек сцены измерения. В данной статье будет рассмотрен метод фотограмметрического воссоздания 3D объектов.

Метод фотограмметрического воссоздания объектов оценивает точки обзора нескольких входных фотографий и дополнительно создает разбросанный или плотный набор точек сцены (Рис. 1) [1].

Рис. 1. Регистрация нескольких изображений и создание облака точек сцены

Метод фотограмметрического воссоздания собирает трехмерную информацию из одного или нескольких изображений (Рис. 2) [1]. Эпиполярная геометрия описывает свойства и геометрические соотношения между 3D-сценой и ее проекцией на двух или более 2D-изображениях.

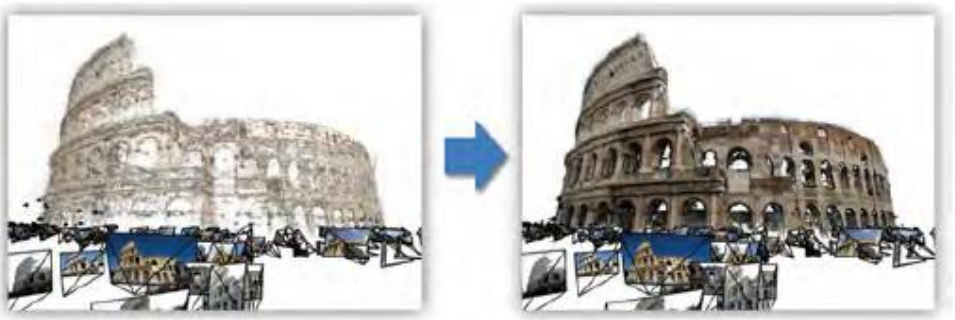


Рис. 2. Регистрация нескольких изображений и создание облака точек сцены

Первый этап фотограмметрического метода воссоздания включает в себя регистрацию всех входных изображений. Этот алгоритм получения структуры объекта из коллекции изображений (structure-from-motion) включает в себя вычисление внутренних и внешних параметров камеры. Для зарегистрированных изображений можно вычислить трехмерные позиции из двух или более соответствующих точек изображения. Многовидовые стерео (multiview stereo) алгоритмы используют эти условия и вычисляют плотное облако точек или триангулированные сетки сцены.

Алгоритм получения структуры объекта из коллекции изображений имеет дело с регистрацией нескольких изображений по отношению друг к другу, то есть вычисление внешних параметров камер. Эти внешние параметры – это положение камеры и ориентация камеры. Внутренние параметры камеры (фокусное расстояние, параметры искажения) могут быть вычислены или на стадии предварительной обработки калибровки для конкретной камеры, или их вычисление является частью алгоритма получения структуры объекта из коллекции изображений (самокалибровки).

Решения, основанные на сходствах, широко используются для регистрации изображений. Локальные точки обнаруживаются в каждом изображении, затем дескрипторы свойств используются для поиска соответствующих точек в других изображениях. Соответствие свойств и оценки параметров камеры производятся для пар изображений. Для каждой пары изображений, по крайней мере, пять точек в случае калиброванных изображений или восемь точек в случае самокалибровки необходимы для вычисления относительного положения и ориентации.

Сходные свойства объединены в треки, которые обозначают соответствующие точки среди нескольких видов для того, чтобы соединить несколько изображений. Наконец, установка трека используется для вычисления параметров камеры и последовательных 3D позиций для треков. Нелинейная оптимизация Левенберга-Марквардта одновременно оптимизирует 3D позиции всех треков и параметры камеры всех входных изображений, которые проецируются вблизи своих начальных 2D измерений. В результате облако 3D точек обеспечивает разбросанное представление сцены. Поэтому алгоритм получения структуры объекта из коллекции изображений также называется алгоритмом создания разбросанного представления сцены. На Рис. 3 представлен пример использования данного алгоритма [2].

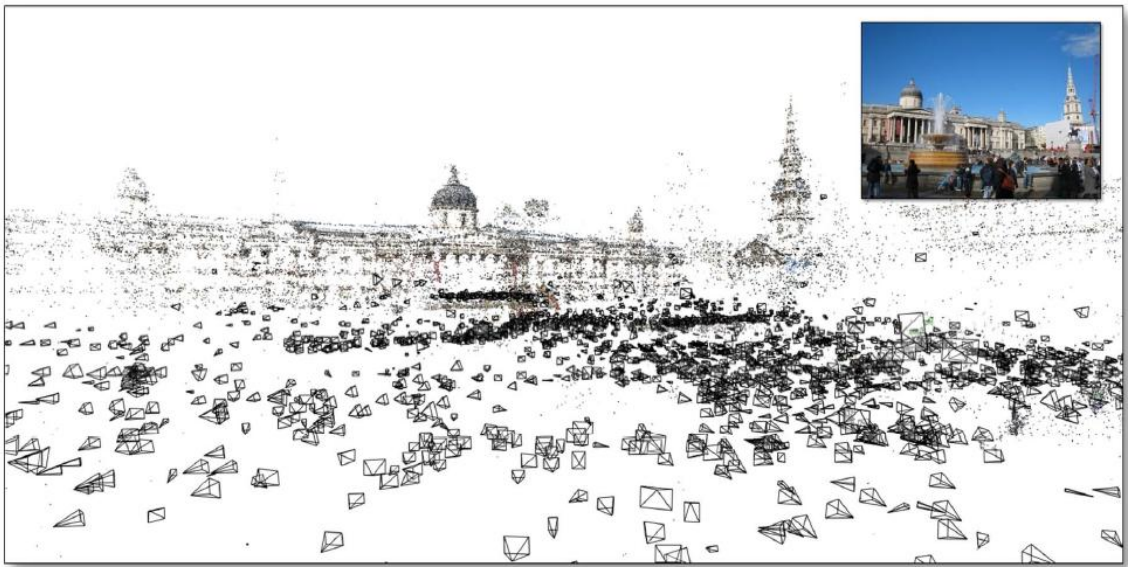


Рис. 3. Представление сцены с помощью structure-from-motion алгоритма

Основной проблемой этих подходов является большое количество данных. Быстрые решения достигается за счет сокращения пространства поиска для сходных изображений и эксплуатации современных графических аппаратных средств.

Алгоритм structure-from-motion производит разбросанное представление сцены, где регистрируются изображения и создаются только множество 3D точек. Последующий процесс (многовидовой стерео алгоритм) вычисляет плотное представление из зарегистрированных изображений. Многовидовые стерео алгоритмы пытаются установить 3D-положение всех пикселей в исходных изображениях. На выходе получаем или треугольные сетки или плотное множество точек, или же ориентированные участки поверхности. Воссозданные сетки обычно имеют очень большое количество треугольников.

Существует идея мультивидового стерео подхода Отто и Чау [3], которая заключается в создании карты глубины, значения глубины на пиксель для каждого используемого изображения. Пиксели, которые не могут быть надежно и точно подобранны остаются неопределенными.

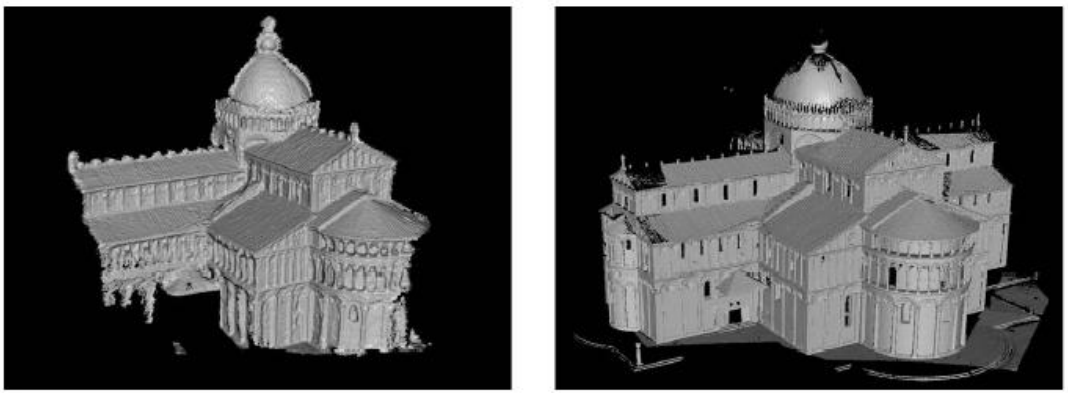


Рис. 4. Сравнение создания 3D моделей с помощью множества изображений (слева) и с использованием лазерного сканнера (справа)

Карты глубины для различных изображений могут быть объединены в единую 3D модель с использованием стандартных методов обработки геометрии. Это слияние карт глубины дает два основных преимущества. Во-первых, карты глубины обычно содержат различные шумы. Сочетание нескольких карт глубины может уменьшить эти артефакты, и поэтому улучшает качество воссозданной поверхности. Во-вторых, входные изображения изображают сцену с различных ракурсов и в разных условиях. Карты глубины, как правило, содержат различные части сцены. Следовательно, при их объединении также улучшается полнота созданной модели. На Рис. 4 (слева) показана 3D модель собора в Пизе, созданной из фото коллекции из 56 изображений [4]. Модель справа была воссоздана путем нескольких 3D сканирований с помощью лазерного сканнера и является наиболее близкой моделью. Созданная модель с помощью многовидового стерео алгоритма из 56 изображений совпадает с моделью, созданной с помощью лазерного сканнера на 25%.

Таким образом, для фотограмметрического создания 3D объектов необходима коллекция фотографий сцены, из которой вычисляется облако точек сцены путем применения алгоритма получения структуры из множества изображений; затем применяется многовидовой стерео алгоритм.

Список использованной литературы

[1]. Agarwal S., Furukawa Y., Snavely N., Curless B., Seitz S.M., Szeliski R. Reconstructing Rome. IEEE Computer, 2010 pp. 40–47.

[2]. Snavely N., Simon I., Goesele M., Szeliski R., Seitz S.M. Scene reconstruction and visualization from community photo collections. Proceedings of the IEEE, 2010, vol. 98 (8), pp. 1370–1390.

[3]. Otto G.P., Chau T.K.W. Region-growing algorithm for matching of terrain images. Image and Vision Computing, 1989, vol. 7 (2), pp. 83–94.

[4]. Goesele M., Snavely N., Curless B., Hoppe H., Seitz S.M. Multi-view stereo for community photo collections. ICCV, 2007.

Нестеров Андрей Юрьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: zub0194@gmail.com

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Т.С.Тихонова, Ю.С. Белов

ФУНКЦИОНИРОВАНИЕ ОСНОВНЫХ КОМПОНЕНТОВ СИСТЕМ СЛЕЖЕНИЯ ЗА ВЗГЛЯДОМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Технологии слежения за взглядом активно развиваются на протяжении последних двадцати лет. Основные принципы этих технологий были рассмотрены ранее [1].

Системы слежения за взглядом, использующие камеру, могут быть подразделены на несколько категорий [2, с.8]:

По типу камеры: системы, использующие инфракрасный (ИК) спектр; системы, использующие световой спектр, видимый человеку;

По типу источника света: системы, использующие дополнительные источники света; системы, использующие окружающий свет;

По количеству камер: системы, использующие одну камеру; системы, использующие несколько камер;

По месту размещения: наголовные системы; дистанционные системы.

Типичные компоненты таких систем включают в себя видеокамеру/видеокамеры и соответствующее ПО. Также часто частью системы бывает источник ИК света, так как он помогает увеличить точность в определении области, куда направлен взгляд.

Программная реализация подобных систем, как правило, делится на две части, одна обнаруживает глаза и их перемещения на изображении, другая использует информацию об обнаруженных глазах для определения того, куда смотрит пользователь. На рисунке 1 (слева) изображена упрощенная схема типичной системы слежения за взглядом [3].

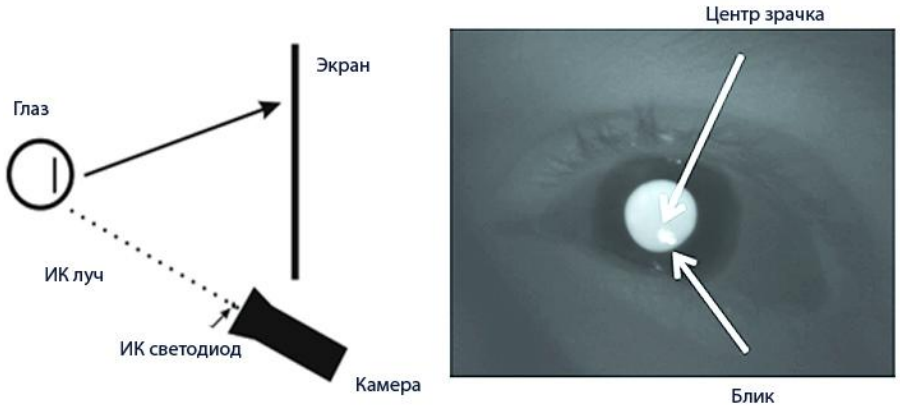


Рис.1 Слева - установка системы, использующая камеру. Справа – блик на роговице глаза.

Вначале устройство отслеживания взгляда (айтрекер) получает изображение с камеры и определяет положение глаз/глаза на картинке. На

направление взгляда пользователя оказывает влияние движение головы, поэтому ранние системы требовали, чтобы голова была зафиксирована. В настоящее время аппаратные составляющие стали более мобильными, что позволяет пользователю свободно двигать головой.

Камеры и их линзы играют центральную роль в системах слежения за взглядом. Устройствам слежения за взглядом необходимо изображение высокого разрешения для получения высокой точности при вычислении параметров взгляда. Фокусное расстояние (увеличение) определяет рабочее расстояние для айтрекера. Использование объектива с большим фокусным расстоянием (сильным увеличением) обеспечивает крупный план изображения глаза, что позволяет пользователю находиться дальше от камеры. Но при использовании таких камер, даже небольшие движения головой могут привести к значительному сдвигу глаз на изображении. До недавнего времени производители должны были выбирать между тем, дать ли пользователю свободу в движении головой или повысить точность. Наклонно-поворотные блоки позволяют камере двигаться, они могут быть использованы при получении изображения глаз, в то время как пользователь двигает головой. Но эти устройства могут быть недостаточно быстрыми в сравнении с движениями головы, а также они повышают стоимость таких систем. Частота кадров и задержка движений камеры определяют, сколько изображений в секунду способна сделать камера и через какой промежуток времени эти изображения будут доступны для последующей обработки. Предпочтительно, чтобы камера имела высокую частоту кадров и низкую задержку, так как это делает айтрекеры более отзывчивыми, но такие камеры значительно дороже и требуют улучшения условий освещения.

Последний компонент это источник света. Большинство айтрекеров используют инфракрасный (ИК) свет, что гарантирует то, что точка фокусировки взгляда сможет быть определена как днем, так и ночью, и даже при движении головой. ИК-свет обеспечивает достаточную освещенность при этом, не принося пользователю никаких неудобств, зрачок не сокращается. В результате получается меньше проблем при отслеживании взгляда.

Источник света создает отражение или блик на роговице глаза (Рисунок 1 справа). Направление взгляда вычисляется нахождением вектора между движущимся ярким или темным зрачком (рисунок 2) и отражением от источника ИК света от поверхности роговицы. Если смотреть на источник света то, естественно, положение блика будет близко к центру зрачка. Как только пользователь отводит взгляд от источника, расстояние между бликом от источника света и зрачком увеличивается. Таким образом, источник света позволяет вычислить вектор направления взгляда (впоследствии вектор переводится в экранные координаты). Положение блика роговицы остается довольно постоянным при вращении глаз и изменении направления взгляда, таким образом, давая понятие о положении глаз и головы. На практике, если пользователь поворачивается сам или поворачивает голову, блик роговицы

также перемещается. Поэтому довольно сложно различать движение головы и движение глаз при одном источнике света. ИК освещение в основном применяется в комнатных условиях. Оно позволяет не использовать отдельное устройство для определения положения головы, тем самым уменьшая стоимость айтрекеров.

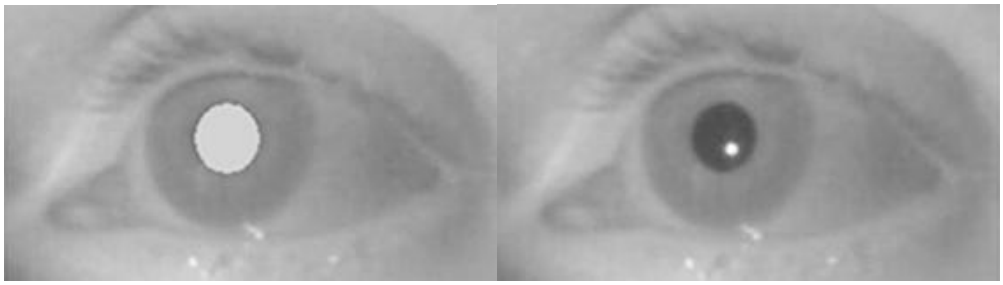


Рис.2 Слева – яркий зрачок. Справа – темный зрачок.

За последние десять лет технология слежения за глазами значительно поменяла свой внешний вид. Сначала системы были большими по размеру, неудобными для пользователя, так как приходилось часами сидеть неподвижно. Сейчас же эта технология стала намного дружественнее к пользователю. Созданы специальные мониторы со встроенной системой отслеживания взгляда, разработаны портативные устройства и мобильные устройства, которые позволяют производить наружные исследования. Но, к сожалению, на данный момент технология довольно дорога и недоступна обычному пользователю. Но, обратив внимание на скорость роста технического прогресса, можно с уверенностью сказать, что через пять лет эта технология войдет в повседневную жизнь.

Список литературы

[1]. Тихонова Т.С., Вершинин Е.В. Технология слежения за глазами. Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе. МГТУ им. Н.Э.Баумана. Калуга, Изд-во МГТУ им. Н.Э.Баумана, 2015, Том 2, 344 стр.

[2]. Onur Ferhat Eye-Tracking with webcam-based setups: implementation of a real-time system and an analysis of factors affecting performance. Dis. Master in Computer Vision and Artificial Intelligence. Barcelona, 2012, 48 p.

[3]. Päivi Majaranta, Hirotaka Aoki, Mick Donegan, Dan Witzner Hansen, John Paulin Hansen, Aulikki Hyrskykari , Kari-Jouko Räihä Gaze Interaction and Applications of Eye Tracking : Advances in Assistive Technologies. United States of America, IGI Global, 2011, 394 p.

Тихонова Татьяна Сергеевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: tatjasha1802@yandex.ru

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

Н.Н. Митрюшина, Ю.С. Белов

ЭТАПЫ КОМПЬЮТЕРНОЙ ДИАГНОСТИКИ РАКА ЛЕГКОГО

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Введение. Рак лёгкого является наиболее часто встречающейся злокачественной опухолью, а также наиболее распространённой причиной смерти от онкологических заболеваний в развитых странах. Согласно данным Международного агентства по изучению рака, ежегодно в мире регистрируется около 1 миллиона новых случаев рака лёгкого, и 60 % онкологических больных погибает в результате данного заболевания [2]. Диагностика рака легкого до последнего времени представляет сложную, до конца не решенную задачу.

Разработка эффективных систем компьютерной диагностики рака легких крайне важна, так как может повысить эффективность лечения и увеличить выживаемость пациента. Современные методы визуализации предоставляют специалисту огромный объем информации, требующей комплексного анализа за короткий промежуток времени. Системы компьютерного детектирования (Computer-aided detection, CADe) и автоматизированной диагностики (Computer-aided diagnosis, CADx) оказывают помощь врачам в интерпретации медицинских изображений.

Общие сведения. CAD системы позволяют сканировать цифровые изображения, полученные, например, в ходе проведения компьютерной томографии (КТ), на наличие типичных внешних признаков и выявлять подозрительные участки.

На данный момент, для детектирования и диагностики узлов в легких в качестве неинвазивных методов визуализации используются позитронно-эмиссионная томография (ПЭТ), компьютерная томография (КТ), компьютерная томография с низкой дозой облучения, и компьютерная томография с контрастным усилением. ПЭТ-сканирование применяется для определения природы узла (является ли новообразование доброкачественным или злокачественным). Раннее обнаружение узлов может быть основано на использовании КТ и КТ с низкой дозой облучения, способных восстанавливать анатомию грудной клетки и выявлять изменения. КТ с контрастным усилением позволяет реконструировать анатомию грудной клетки и производить оценку свойств выявленного узла.

Успешность конкретной CAD системы может быть определена с точки зрения точности диагностики, скорости и уровня автоматизации [3].

Схема работы типичной системы компьютерной диагностики рака легких представлена на Рис. 1. и включает в себя следующие этапы работы: сегментация легочных полей на изображениях, детектирование узлов в легких, сегментация узлов, диагностика узлов. Ниже приводится краткое описание каждого этапа.

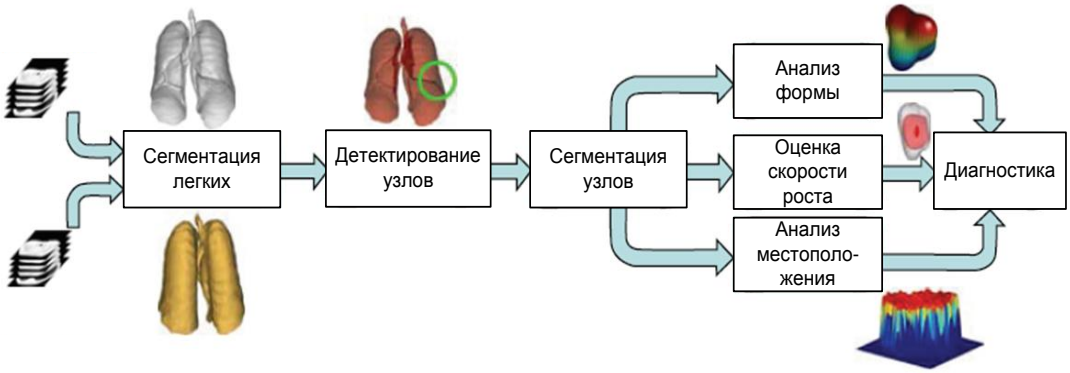


Рис. 1. Общая схема системы компьютерной диагностики рака легкого. Входными данными являются медицинские изображения, полученные с помощью соответствующего метода сканирования.

Сегментация легких. Необходима для уменьшения пространства поиска узлов в легких. Представляет из себя сложную задачу из-за неоднородностей в области легких и легочных структур (артерий, вен, бронхов, бронхиол), а также схожести их плотностей. Необходимо также уделить внимание ряду технических вопросов: уровень автоматизации метода, его чувствительность к параметрам сканирования, эффективность алгоритма при работе с различными типами входных изображений, способность обеспечить надлежащую сегментацию легких в случае тяжелых патологий, связанных с присутствием неоднородностей в легких пациента.

Детектирование и сегментация легочных узлов. Второй этап работы CAD системы заключается в нахождении местоположения узлов, которые отображаются внутри легочных полей в качестве белых круглых объектов с относительно низкой контрастностью.

Выявление новообразований в легких до сих пор остается сложной задачей. Трудность для систем CAD состоит в том, чтобы отличить истинные узелки от теней, сосудов и ребер. Кроме всего прочего, должны быть учтены различные факторы, в том числе способность обнаруживать узелки различных форм и возможность системы выявлять узелки на границах легких, полые узлы, а также узлы малого размера (менее 3 мм).

Методы обнаружения узлов в легочных полях при проведении КТ грудной клетки, как правило, включают в себя два этапа: 1) начальный поиск всех возможных узлов; 2) частичное устранение ложноположительных узелков (False Positive Nodules, FPNs) при сохранении положительных (True Positive Nodules, TPNs), то есть разделение всех выявленных объектов на возможные узлы и нормальные анатомические структуры.

Далее следует сегментация легочных узлов, точность которой напрямую влияет на такие важные клинические факторы, как минимальный размер измеримых поражений органа. Кроме этого, сегментация определяет и их местоположение на изображении. Эффективность дальнейшего определения природы новообразования будет также зависеть от ее точности.

Некоторые типы узлов (небольшого размера или частично твердые) представляют сложности для точной сегментации. Поскольку такие трудные случаи имеют важное клиническое значение, сегментация узелка играет решающую роль в успешном решении этих клинических задач.

Диагностика легочных узлов. После того, как узелки в легких обнаружены и сегментированы из соответствующих изображений грудной клетки, дальнейшей задачей становится определение, являются ли они злокачественными или доброкачественными. Для диагностики используются набор отличительных признаков узла, такие как размер, форма, особенности месторасположения.

ПЭТ/КТ. Исследователи объединили информацию от изображений, снятых с использованием КТ и ПЭТ отдельно, и изучили влияние такого слияния на точность диагностики. Эксперименты показывают, что при данном использовании ПЭТ/КТ достигается более точная диагностика, чем применение только одного из этих методов исследования [4]. Таким образом, можно говорить о том, что слияние ПЭТ/КТ может благоприятно повлиять на дальнейшее развитие систем компьютерной диагностики рака легкого. Тем не менее, отдельные моменты требуют дальнейшего изучения.

Заключение. На сегодняшний день системы компьютерной диагностики рака легких оказывают существенную помощь рентгенологам, однако они все еще не могут быть использованы в качестве полноценного способа постановки диагноза. Для исключения ложных срабатываний все нарушения, выявленные CAD, должны быть дополнительно интерпретированы специалистом. Дальнейшие усовершенствования этапов работы данных систем позволят увеличить эффективность их применения в диагностике рака легких.

ЛИТЕРАТУРА

[1]. Грищенков А.С., Рудь С.Д., Сигина О.А. и др. Компьютерная томография в диагностике рака легкого, осложненного вторичным воспалительным процессом // Радиология – практика, 2012. № 5. С. 8–15.

[2]. International Agency for Research on Cancer. Lung Cancer Estimated Incidence, Mortality and Prevalence Worldwide in 2012. URL: http://globocan.iarc.fr/Pages/fact_sheets_cancer.aspx (дата обращения: 22.10.2015)

[3]. A. El-Baz and J. Suri, Lung Imaging and Computer Aided Diagnosis, Taylor & Francis, 2011 – 496 p.

[4]. J. H. Min, H. Y. Lee, K. S. Lee et al., “Stepwise evolution from a focal pure pulmonary ground-glass opacity nodule into an invasive lung adenocarci-noma: an observation formore than 10 years,” Lung Cancer, vol. 69, no. 1, pp. 123–126, 2010.

Митрюшина Наталья Николаевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: natalya-mitryushina@yandex.ru

Белов Юрий Сергеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: ybs82@mail.ru

СЕКЦИЯ 11.

ПРОБЛЕМЫ СОВРЕМЕННОЙ ТВЕРДОТЕЛЬНОЙ ЭЛЕКТРОНИКИ

С.А. Адарчин, В.Г. Косушкин

ВЛИЯНИЕ ТЕМПЕРАТУРНОЙ ОБРАБОТКИ НА УСАДКУ ПЛАСТМАССО-ВЫХ МАТЕРИАЛОВ КОРПУСОВ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Применение пластмасс для изготовления корпусов полупроводниковых приборов и герметизации электронных устройств позволило реализовать массовое производство, что обеспечило их широкое применение. Вместе с тем, принято считать, что такой вариант корпусирования приборов не обеспечивает высокой надежности [1,2], что и обуславливает область применения пластмассовых корпусов.

Целью работы являлось установление причин возникновения параметрических отказов полупроводниковых приборов в пластмассовых корпусах.

В наших предыдущих работах [3-5] показано, что одной из причин возникновения параметрических отказов электронных датчиков являлись термоупругие напряжения, приводящие к деградационным процессам в полупроводниковых структурах измерительных преобразователей, как наиболее чувствительных узлах приборов. Механические напряжения могут возникать вследствие различных коэффициентов линейного расширения материалов прибора и корпуса и его работы в условиях переменных температур. Чувствительные элементы, изготовленные из монокристаллов кремния высокого структурного совершенства, в процессе эксплуатации могут приобретать множество дефектов, которые и становятся причиной изменения параметров работы приборов в процессе эксплуатации [5].

Как в процессе производства, так и в ходе эксплуатации приборов пластмассовые корпуса подвергаются значительным перепадам температуры, что также может быть причиной изменения параметров приборов.

Для достижения поставленной цели был проведен анализ стабильности геометрических размеров тестовых элементов из пластмассы при воздействии повышенной температуры.

Методика и результаты измерения стабильности геометрических размеров тестовых элементов.

Для анализа стабильности геометрических размеров использовались тестовые элементы, изготовленные из поликарбоната, схема которых показана на рисунке 1.

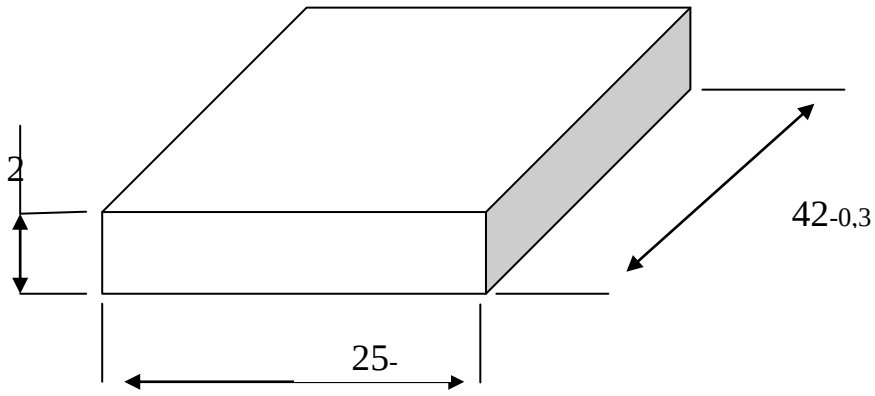


Рис. 1. Схема тестового элемента, размеры в мм

Выбор поликарбоната обусловлен его высокой технологичностью, дешевизной и широкой областью применения от светодиодной техники до корпусных деталей автомобилей.

Для оценки стабильности геометрических размеров проводили замеры длины и ширины тестовых элементов до и после термообработки. Термообработка проводилась в камере тепла при температуре +125 ^{0}C в течение 4 часов.

Замеры проводились в нормальных условиях на выборке в объеме 75 штук из партии в 7500 тестовых элементов.

В таблице 1 приведены результаты замеров.

Таблица 1.Изменение геометрических параметров тестовых элементов

Размер	Состояние тестового элемента	Математическое ожидание величины размера, мм	Величина дисперсии размеров	Абсолютное изменение размера после термообработки, мм	Относительное изменение размера после термообработки, %
42-0,3	До термообработки	41,84	0,0017	0,05	0,11
	После термообработки	41,89	0,0024		
25-0,21	До термообработки	24,72	0,0014	0,2	0,79
	После термообработки	24,92	0,0036		

Анализ полученных результатов. Выводы

В результате проведенных измерений выявлен эффект увеличения геометрических размеров тестовых структур после термообработки. Такое поведение полимеров может быть обусловлено возникновением связей высоких порядков в полимерных цепях. Выявленный эффект анизотропии может быть объяснен особенностями формирования структуры пластмассы в условиях экструзии.

Полученные результаты говорят о том, что при сборке полупроводниковых приборов в пластмассовые корпуса необходимо учитывать не только различия температурных коэффициентов сопрягаемых материалов в приборах, но и возможные отклонения геометрических размеров корпусов в технологических циклах корпусирования и герметизации приборов.

В результате проведенной работы экспериментально установлены изменения геометрических параметров тестовых структур, которые позволят в дальнейшем определить их влияние на изменение электрофизических параметров полупроводников, сопрягаемых с пластмассовыми корпусами. Что в свою очередь позволит оценить влияние технологии корпусирования на надежность полупроводниковых структур.

Литература

[1]. Зи С. Технология СБИС: -М.: Мир, 1986. 404с.

[2]. Готра З.Ю. Технология микроэлектронных устройств:-М.: Радио и связь, 1991.-528с.

[3]. Адарчин С.А., Кужненков А.С. Исследование процессов деградации микроэлектромеханических структур // 1-ая Российская конференция молодых ученых по математическому моделированию. – М. Изд-во МГТУ им. Н.Э. Баумана 2000 г. – С.138.

[4]. Адарчин С.А., Кужненков А.С. Исследование процессов деградации микроэлектромеханических структур датчиков давления // пятая международная научно-техническая конференция «Актуальные проблемы электронного приборостроения АПЭП-2000». – Новосибирск., 2000 г. - том 4.

[5]. Адарчин С.А., Косушкин В.Г., Адарчина Е.Н. Надежность автомобильных электронных компонентов в условиях воздействия знакопеременных нагрузок. «Инженерный журнал: наука и инновации» #7(31)/2014**DOI:** 10.18698/2308-6033-2014-7-1316

Адарчин Сергей Александрович - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: adarchin@rambler.ru

Косушкин Виктор Григорьевич - д-р техн. наук, зав. каф. КФ МГТУ им. Н.Э. Баумана. E-mail: kosushkin@gmail.com

Ю.П. Головатый, Н.А. Хахаев

МОДЕЛИРОВАНИЕ КОЛОРИМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК ГЕТЕРОСТРУКТУРЫ НА КВАНТОВЫХ ЯМАХ В СИСТЕМЕ GAN/INGAN

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Особенностью современной наноэлектроники является использование квантовых эффектов и ограничение движения носителей заряда в одном, двух или трёх измерениях. На этом принципе создаются практически все современные светодиоды, лазеры, фотоприемники и быстродействующие транзисторы. [1]

В настоящее время основными материалами для создания светодиодов белого свечения являются нитриды элементов III группы. Они обладают широким диапазоном запрещенной зоны и безвредны для окружающей среды. Высокая электронная подвижность и скорость насыщения, высокое поле пробоя и высокая теплопроводность также преимущества нитридов третьей группы.

Работа посвящена исследованию полупроводниковых многослойных наноструктур, пригодных для создания светодиодов белого свечения в системе GaN/InGaN с красным, зеленым и синем спектрами излучения, сформированными в одном кристалле. В работе производится расчет энергетических уровней и волновых функций носителей, электрических полей обусловленных спонтанной поляризацией и пьезоэффектом, спектров спонтанного излучения и координат цветности суммарного излучения.

Модель зонной структуры белого светодиода. Слои в исходной структуре расположены последовательно следующем образом: эмиттер E1, «красная» яма W1 толщиной 6 нм, барьер B1 толщиной 9 нм, «зеленая» яма W2 толщиной 9 нм, барьер B2 толщиной 5 нм, «синяя» яма W3 толщиной 2 нм, эмиттер E2. Барьеры и эмиттеры состоят из чистого GaN. Квантовые ямы состоят из твердого раствора $In_xGa_{1-x}N$, где x-содержание In в твердом растворе. Мы рассчитали составы InGaN в квантовых ямах. При изменение концентрации индия в твердом растворе меняется значение ширины запрещенной зоны, что в свою очередь, изменяет цвет оптического излучения. Толщины слоев были подобраны в зависимости от требуемого расположения энергетических уровней и волновых функций электронов.

Полученные значения запрещенных зон сведены в таблице 1

Таблица 1. Значения длин волн и запрещенных зон

Заданная длина волны (нм)	700	540	450
Значение запрещенной зоны (эВ)	1,8	2,3	2,7

«Эффективная» запрещенная зона $\mathcal{E}_{gi}$ отличается от номинальной запрещенной зоны $\mathcal{E}_{g0i}$ на сумму энергий уровней размерного квантования электронов $\mathcal{E}_{en}$ и дырок $\mathcal{E}_{hn}$ в квантовых ямах,

$$\mathcal{E}_{gi} = \mathcal{E}_{g0i} + \mathcal{E}_{en} + \mathcal{E}_{hn} \tag{2}$$

Каждое из трех слагаемых зависит о состава соответствующей ямы x_i

$$\mathcal{E}_{gi} = \mathcal{E}_{gInN} \cdot x_i + \mathcal{E}_{gGaN} \cdot (1 - x_i) - B \cdot x_i \cdot (1 - x_i) + \\ + \frac{\mathcal{E}_0}{M_{nInN} \cdot x_i + M_{nGaN} \cdot (1 - x_i)} + \frac{\mathcal{E}_0}{M_{pInN} \cdot x_i + M_{pGaN} \cdot (1 - x_i)} \tag{3}$$

где M_{nGaN} -эффективная масса электрона в GaN, M_{nInN} -эффективная масса электрона в InN, M_{pGaN} - эффективная масса дырки в GaN, M_{pInN} - эффективная масса дырки в InN, B -параметр провисания, $\mathcal{E}_{gGaN}$ - запрещенная зона GaN, $\mathcal{E}_{gInN}$ -запрещенная зона InN, $\mathcal{E}_0$ - параметр с размерностью энергии.

$$\mathcal{E}_0 = \frac{\pi^2 \cdot \hbar^2}{2 \cdot m_0 \cdot d^2 \cdot q} \tag{4}$$

Значения содержания InN в ямах и энергии эффективных запрещенных зон, рассчитанные по уравнению (3), приведены в таблице 2

Таблица 2Значения процента индия в составе и энергии запрещенной зоны

Значение энергии эффективной запрещенной зоны (эВ)	2,7	2,3	1,77
Содержание In в твердом растворе, %	15	28	45

При моделировании важно было учесть пьезо- и спонтанную поляризации. Характерными особенностями III-нитридов являются высокая степень ионности связей, вследствие чего в них возникает спонтанная поляризация. В многослойных структурах деформации, вызванные несоответствием решеток, обусловливают возникновение пьезополяризации. В эмиттерах и барьерах, состоящих из GaN, пьезополяризация отсутствует. Электрическое поле, обусловленное

суммарным действием обеих поляризаций, в каждом из пяти слоев (ямы и барьеры) может быть вычислено по формуле [2]

$$E_j = \frac{\sum_k l_k P_k / \varepsilon_k - P_j \sum_k l_k / \varepsilon_k}{\varepsilon_j \sum_k l_k / \varepsilon_k} \qquad (5)$$

где j, k -номер слоя, l_k-толщина k– го слоя, P_k- полная суммарная поляризация в k– м слое, ε_k - диэлектрическая проницаемость k– го слоя, j-номер слоя, P_j-полная суммарная поляризация в j– м слое, ε_j - диэлектрическая проницаемостьj-го слоя.

Значения полей, рассчитанные по формуле (5) с использованием поляризационных параметров из [3], приведены в таблице 3. Они искривляют энергетические зоны, в результате чего зонная диаграмма структуры принимает вид (рис.1)

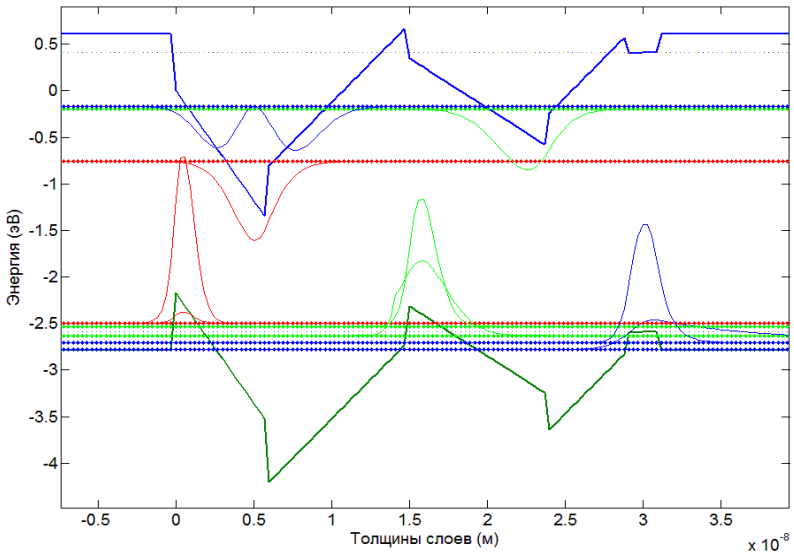


Рис.1. Волновые функции и уровни энергии электронов, легких и тяжелых дырок

Таблица 3. Значения электрических полей в слоях

	Красная яма	Барьер	Зелёная яма	Барьер	Синяя яма
E (В/м)	$2{,}4*10^8$	$1{,}7*10^8$	$1{,}1*10^8$	$1{,}7*10^8$	$5{,}1*10^6$

Энергетические уровни электронов ε_{en} и дырок ε_{hn} в структуре и их волновые функции Ψ_{en}, Ψ_{hn} находили численно из уравнения Шредингера

$$-\frac{\hbar^2}{2\cdot m}\cdot\frac{d^2\Psi_n(x)}{dx^2}+V(x)\Psi_n(x)=\mathcal{E}\Psi_n(x) \tag{6}$$

где m — масса частицы, $V(x)$ — потенциальная энергия, $\mathcal{E}$ — полная энергия, $\Psi_n(x)$ — волновая функция.

Полученные волновые функции и уровни энергии изображены на рис. 1. Вверху показаны энергетические уровни электронов и волновые функции для каждого уровня. Внизу показаны энергетические уровни и волновые функции тяжелых и легких дырок. Оптическое излучение генерируется при переходах электронов из состояния зоны проводимости в состояния тяжелых и легких дырок в валентной зоне.

Важным параметром при подсчете спектра является положение квазиуровней Ферми в структуре. Изменение положения этих уровней зависит от приложенного смещения к структуре. Спектр излучения рассчитывали для каждой ямы по формулам (7,8,9). [3]

$$r_{sp}(h\nu)=\frac{q^2h}{2m_0\varepsilon\varepsilon_0}\frac{1}{h\nu}D_{opt}D_r\left|M\right|^2 f_C(1-f_V) \tag{7}$$

$$D_{opt}(h\nu)=\frac{\varepsilon n_r}{\pi^2\hbar^3c^3}(h\nu)^2 \tag{8}$$

$$D_r=\frac{m_r}{\pi\hbar^2 d_z} \tag{9}$$

где q-заряд электрона, m_0- масса свободного электрона, ε-относительная диэлектрическая проницаемость, ν-частота, $\left|M\right|^2$-матричный элемент перехода, f_C-функция распределения электронов в зоне проводимости, f_V-функция распределения дырок в валентной зоне, ε_0-диэлектрическая постоянная, h-постоянная Планка, D_r-плотность электронных мод, D_{opt}-плотность оптических мод, n_r-показатель преломления материала, d_z-толщина квантовой ямы, m_r-приведенная масса электрона и дырки.

По полученным данным была составлена таблица значений пиковых длин волн спектров излучения в трех ямах (Таблица 4).

Таблица 4. Таблица значений пиковых длин волн спектров излучения в трех ямах

	W1(красная яма)	W2(зеленая яма)	W3(синяя яма)
Длина волны (нм)	710	510	475

По суммарному спектру, соответствующему переходам $e1 \longrightarrow h1, e2 \longrightarrow h2, e3 \longrightarrow h3$, вычислялись координаты цветности для смещений в интервале $1B \le U \le 3B$. Полученные точки нанесены на плоскости цветности XY (рис.2).

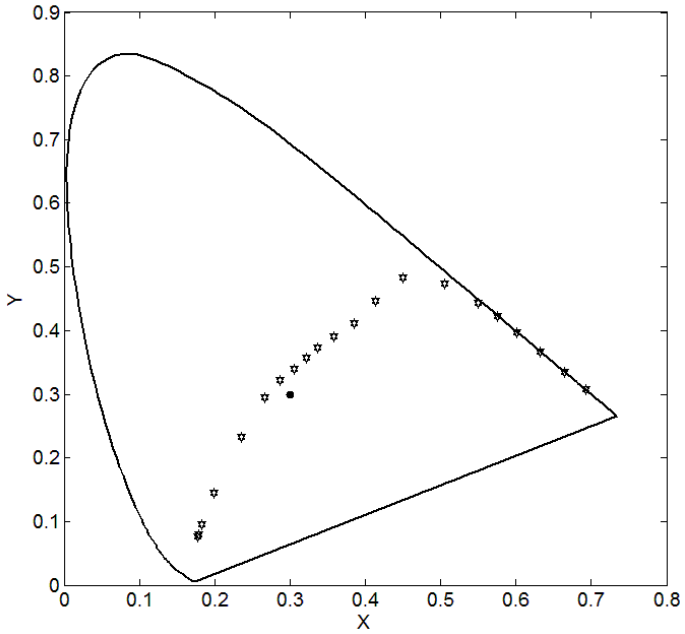


Рис.2. Зависимость цветности суммарного спектра от разности уровней Ферми на плоскости цветности

Выводы. В результате выполнения работы была построена физическая модель трехдиапазонного светодиода на основе квантовых ям в системе GaN/InGaN. Методом математического моделирования рассчитаны спектры спонтанного излучения в этой системе. Показано, что при разности квазиуровней Ферми в интервале от 2.3 В до 2.5 В цвет суммарного спектра близок к белому цвету. Таким образом, эта структура может оказаться перспективной для создания монолитного излучателя белого цвета.

Список литературы

[1]. Piprek J., Li S. Optoelectronic Devices: Advanced Simulation and Analysis// Springer; 2005 edition (December 7, 2004), pp. 1-5.

[2]. Bernardini F., Fiorentini V. Spontaneous vs. Piezoelectric polarization in III-V nitrides: conceptual aspects and practical consequences // Phys. Rev. B. 1997- V. 56. № 16. - P. R10024-R10027, pp. 2-3.

[3]. Bulashevich K.A., Mymrin V.F., Karpov S.Yu.. Simulation of Visible and Ultra-Violet Group-III Nitride Light Emitting Diodes / e.a.// J. Comput. Phys. 213, No 214-238 (2006) / DOI 10.1016/j.jcp.2005.08.011, pp. 4-10.

Головатый Юрий Павлович - канд. техн. наук, старший преподаватель КФ МГТУ им. Н.Э. Баумана. E-mail: yugolovatiy@mail.ru

Хахаев Николай Алексеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: xoxbmx123@gmail.com

Д.А. Романов, И.А. Прохоров, С.С. Стрельченко,
А.П. Большаков, А.А. Хомич, В.Г. Ральченко

РЕНТГЕНОДИФРАКЦИОННЫЕ ИССЛЕДОВАНИЯ ЭПИТАКСИАЛЬНЫХ CVD ПЛЕНОК АЛМАЗА С МОДИФИЦИРОВАННЫМ ИЗОТОПИЧЕСКИМ СОСТАВОМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

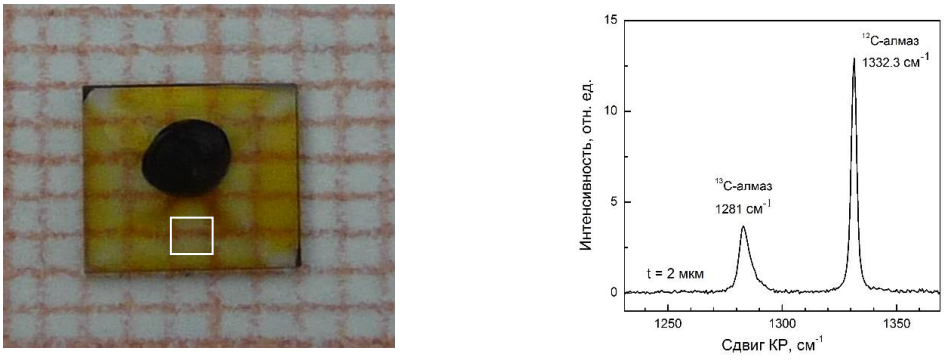
Введение. Монокристаллы синтетического алмаза благодаря уникальным свойствам этого материала – высокой твёрдости, химической и радиационной стойкости, малому коэффициенту теплового расширения и высокой теплопроводности (особенно изотопически модифицированных кристаллов) и т.д., находят всё более широкое применение в различных областях науки и техники. Технологические применения алмаза возрастают не только в традиционных областях, связанных с изготовлением обрабатывающих инструментов, но и в высокотехнологичных приложениях, таких как создание электронных приборов, детекторов излучений, рентгенооптических элементов для синхротронных источников с исключительно высокими потоками излучения [1]. При этом особенно многообещающими являются кристаллы, получаемые методом осаждения из газовой фазы (chemical vapor deposition – CVD) [2], так как этот ростовой процесс позволяет получать не только наиболее чистые кристаллы, но и прецизионно управлять содержанием примеси, что особенно важно в электронных и некоторых оптических применениях. Алмаз, как и любой углерод природного состава (^{nat}C), содержит два стабильных изотопа 98.93% ^{12}C и 1.07% ^{13}C. Целенаправленное изменение изотопного состава позволяет улучшать уникальные свойства этого материала, включая твердость и теплопроводность[3]. В частности, обогащение до 99.93% по изотопу ^{12}C увеличило его теплопроводность почти на 50% до величины 33.2 Вт/см·К при комнатной температуре [4]. Изменение изотопного состава безазотного IIa алмаза от естественного (концентрация ^{13}C 1.07%) до почти чистого (> 99%) ^{13}C приводит к уменьшению периода кристаллической решетки, которое по данным [5] составляет $\Delta a/a \sim -1.5\cdot10^{-4}$. Изучение влияния изотопного состава алмаза на свойства кристаллов имеет большое значение, т.к. на его основе можно реализовывать новые свойства, превосходящие свойства естественных кристаллов.

В настоящей работе проведены прецизионные измерения величины несоответствия периодов кристаллических решеток подложки Ib алмаза и выращенной на ней эпитаксиальной ^{13}C пленки толщиной 2 мкм, обогащенной по изотопу ^{13}C до 99,96%.

Методика эксперимента. Синтез изотопически модифицированной эпитаксиальной пленки алмаза ^{13}C толщиной около 2 мкм проводили методом химического газофазного осаждения в метан-водородной ($^{13}CH_4/H_2$) газовой смеси с использованием обогащенного по изотопу ^{13}C до 99,96% метана ($^{13}CH_4$) на специализированном реакторе ARDIS-100 [2] в плазме СВЧ разряда (частота 2.45 ГГц). В качестве подложки для эпитаксии использовали монокристаллическую алмазную пластину ориентации (001) размером 5×5 мм^2 и толщиной 0,5 мм, изготовленную из монокристалла алмаза типа Ib, выращенного в аппарате высокого давления (метод HPHT - high pressure, high temperature). Из-за присутствия примеси азота в состоянии замещения кристалл имел желтый оттенок. Условия осаждения были следующие: содержание метана в смеси - 6%, давление в камере реактора 130 Торр, СВЧ мощность 2,2 кВт. Скорость роста составляла около 9 мкм/час.

Исследования методами двухкристальной рентгеновской дифрактометрии проводили на двухкристальном рентгеновском дифрактометре в $CuK_{\alpha 1}$ излучении (длина волны характеристического излучения λ = 1.54 Å). Известно, что эффективность этого метода существенно возрастает при использовании бездисперсионной (n, -n) установки кристаллов. Однако высокая твердость алмаза затрудняет изготовление из этого материала прецизионно ориентированных сильно асимметричных кристаллов-монохроматоров. Кроме того, кристаллы алмаза по структурному совершенству, как правило, пока уступают элементарным полупроводникам Ge и Si. В этой связи в настоящей работе для расширения пучка и формирования почти плоской волны использовали сильно асимметричное отражение 511 от монохроматора из высокосовершенного бездислокационного германия марки ГДГ-3 (угол Брэгга θ~ 45.0°, фактор асимметрии отражения b ~0.01, расходимость пучка после монохроматора составляет ~ 0.5"). Исследования пластин алмаза проводили в отражении 113 (угол Брэгга θ~ 46.0°), хорошо согласующемся по межплоскостному расстоянию с отражением 511 от германия.

Результаты и их обсуждение. Ниже приведены предварительные результаты определения несоответствия периодов кристаллических решеток подложки Ib алмаза и выращенной на ней эпитаксиальной ^{13}C пленки толщиной 2 мкм, обогащенной по изотопу ^{13}C до 99,96% (Рис. 1а). Спектры комбинационного рассеяния света (КР) двуслойного алмаза $^{13}C/^{nat}C$ регистрировали спектрометром LabRam HR840в конфокальной схеме при возбуждении КР излучением полупроводникового лазера с длиной волны 473 нм со стороны слоя алмаза ^{13}C, на которую лазерный луч фокусировался в пятно диаметром около 1 мкм. В спектре КР наряду с более сильной линией на 1332,3 см$^{-1}$ от подложки присутствует также сдвинутая линия КР на 1381 см$^{-1}$ от пленки (Рис. 1б).



(а) (б)

Рис. 1. (а) Фотография образца ТШ-3 (CVD13C/ HPHTIb) со стороны пленки. Ориентация (001), боковые стороны соответствуют направлениям типа <110>. Темное пятно – фломастерная метка со стороны подложки. Белым квадратом отмечена область размером ~ 1 × 1 мм2, в которой проводились дифрактометрические измерения, остальная часть кристалла закрывалась свинцовой фольгой. (б) Спектр КР двуслойного синтетического алмаза 13C/natC со слоем изотопно-обогащенного алмаза 13C толщиной 2 мкм на подложке из HPHT алмаза natC.

По результатам исследований в асимметричном отражении 113 с использованием двух геометрий дифракции [6] с углами падения излучения на образец $\omega A = \theta + \varphi$ и $\omega B = \theta - \varphi$, ($\theta$ – угол Брэгга, φ – угол выхода отражающих плоскостей к поверхности образца) были получены следующие результаты. Кривые качания, полученные в отражении 113 с полным омыванием образца пучком, были уширены и содержали два доминирующих пика, сформированных отражениями от подложки и пленки. Кроме того, выявлялись дополнительные пики, связанные с отражением от различных слегка разориентированных секторов роста в подложке.

Ограничение области отражение на образце (белый квадрат на Рис. 1а) позволило значительно улучшить параметры кривых качания. Для ωA геометрии дифракции полуширины кривых качания для подложки и пленки составили $\Delta\omega SA1/2 \sim 2.9"$ и $\Delta\omega LB1/2 \sim 4.0"$, соответственно (Рис. 2 а). Для ωB геометрии полуширины кривых качания для подложки и пленки составили $\Delta\omega SA1/2 \sim 5.3"$ и $\Delta\omega LB1/2 \sim 10.6"$, соответственно (Рис. 2 б). Отражение от пленки расположено со стороны больших углов (что соответствует меньшим значениям межплоскостного расстояния) и характеризуется большим значением полуширины кривой качания. Искажение формы кривых качания и появление дополнительных пиков обусловлено, очевидно, неоднородностью подложек Ib алмаза [7].

Угловые расстояния между пиками отражения от подложки и пленки, полученными в двух геометриях дифракции, составляют $\Delta\omega A = 12.3"$ и $\Delta\omega B = 38.4"$. Известно [6], что полусумма этих расстояний дает изменение брэгговского угла $\Delta\theta = (\Delta\omega A + \Delta\omega B)/2 \sim 25.4"$, а полуразность равна взаимной разориентации отражающих плоскостей $\Delta\varphi = (\Delta\omega A - \Delta\omega B)/2 \sim 13.1"$.

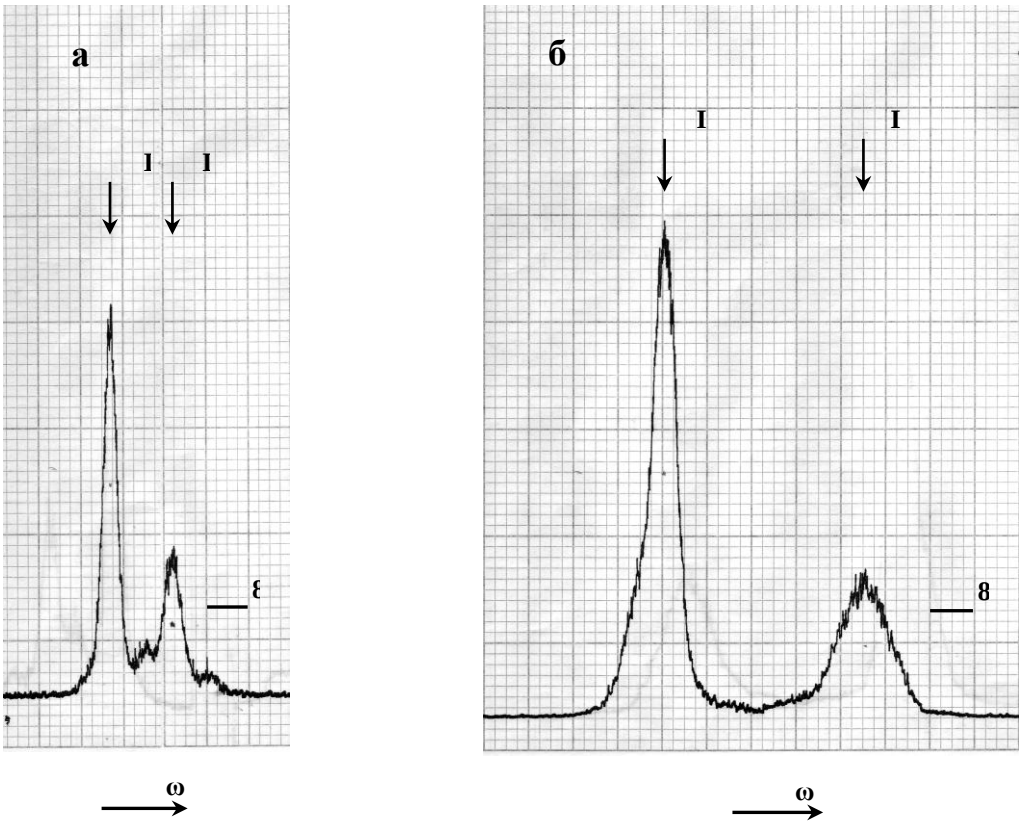


Рис. 2. Кривые качания, полученные в двух геометриях дифракции от области образца, отмеченной белым квадратом на Рис. 1. CuKα1 излучение, отражение 113.
I– пик отражения от подложки, II – пик отражения от пленки.

Таким образом, для относительного изменения межплоскостного расстояния (113) получаем $(\Delta d/d)_{113}= -ctg\ \theta \cdot \Delta\theta \sim 1.19\cdot 10^{-4}$. Используя известное соотношение [6] $\Delta d/d = (\Delta d/d)_{\perp}\cdot \cos^2\varphi$, где $(\Delta d/d)_{\perp}$ - изменение межплоскостных расстояний перпендикулярно поверхности пленки, находим, что $(\Delta d/d)_{\perp}\sim 1.45\cdot 10^{-4}$. Изменение релаксированного (в свободном, недеформированном состоянии) периода решетки равно $(\Delta a/a)_{relax} = \gamma\cdot (\Delta d/d)_{\perp}$, где $\gamma\cdot$– корректировочный фактор [8]. Для ориентации подложки (001) $\gamma_{001} = C_{11}/(C_{11}+ 2C_{12})$, где C_{11} и C_{12} упругие постоянные. Используя значения упругих постоянных для алмаза ^{13}C [9] находим, что $\gamma_{001}\sim 0.81$. И для несоответствия периодов кристаллических решеток получаем $(\Delta a/a)_{relax}\sim 1.2\cdot 10^{-4}$.

Использование симметричного отражения 004 позволяет непосредственно из одного измерения определить $(\Delta d/d)_{\perp}$. Однако, из-за дисперсионного уширения кривых качания (угол Брэгга для отражения 004 составляет $\theta \sim 59.75°$, что значительно отличается от брэгговского угла

отражения от монохроматора) пики отражения от подложки и пленки разделяются хуже, чем в отражении 113 (Рис. 3).

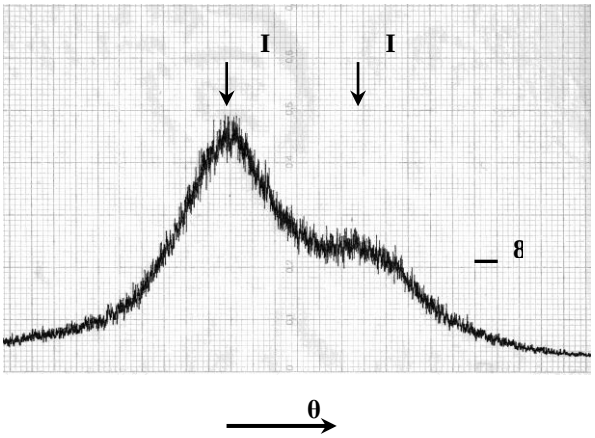


Рис. 3. Кривая качания, полученная в симметричном отражении 004. **I**– пик отражения от подложки, **II** – пик отражения от пленки. Угловое расстояние между пиками составляет $\Delta\theta \sim 50''$.

Для относительного изменения межплоскостных расстояний перпендикулярно поверхности пленки получаем $(\Delta d/d)_{\perp} = -\,\mathrm{ctg}\,\theta \cdot \Delta\theta \sim 1.4\cdot10^{-4}$. Изменение релаксированного периода решетки равно $(\Delta a/a)_{relax} = \gamma\cdot\,(\Delta d/d)_{\perp} \sim 1.14\cdot10^{-4}$, что, практически, совпадает с результатами, полученными с использованием асимметричного отражения 113.

Таким образом, результаты измерений с использованием симметричного и асимметричного отражений дают примерно одинаковое значение для величины несоответствия в периодах кристаллических решеток Ib подложки и ^{13}C CVD пленки $(\Delta a/a)_{relax} \sim (1.1\div1.2)\cdot10^{-4}$. Это несколько отличается от результатов [5], полученных при исследовании изотопически модифицировнных кристаллов IIa алмаза с низким содержанием азота, $(\Delta a/a)_{relax}\sim1.5\ \cdot10^{-4}$. Основная причина наблюдаемого расхождения обусловлена, прежде всего, относительно низким структурным совершенством и достаточно высокой степенью неоднородности подложек из Ib алмаза [7], что снижает точность измерений.

Выводы. Проведенные методами двухкристальной рентгеновской дифрактометрии исследования показали, что в изотопически модифицированных пленках алмаза ^{13}C, выращенных на подложках Ib алмаза наблюдается уменьшение периода кристаллической решетки $(\Delta a/a)_{relax} \sim (1.1\div1.2)\cdot10^{-4}$. Результаты, в целом, согласуются с результатами прецизионных измерений периода решетки в изотопически модифицированных кристаллах алмаза группы IIас низким содержанием азота. Наблюдаемое различие обусловлено, главным образом, неоднородностью подложек Ib алмаза, что затрудняет проведение измерений и снижает их точность. Использование при получении эпитаксиальных слоев безазотных подложек алмаза группы IIa позволило бы проводить более точные дифрактометрические исследования по

влиянию изотопного состава на период кристаллической решетки и реальную структуру кристаллов алмаза.

Работа по синтезу алмаза выполнена при поддержке гранта РНФ №14-12-01403.

Списоклитературы.

[1]. Shvyd'ko Yu., Stoupin S., Blank V., Terentyev S.Near-100% Bragg reflectivity of X-rays // Nature Photonics. 2011. V. 5. P. 539-542.

[2]. БольшаковА.П.,РальченкоВ.Г., ПольскийА.В., КоновВ.И., АшкиназиЕ.Е., ХомичА.А., ШароновГ.В., ХмельницкийР.А., ЗаведеевЕ.В., ХомичА.В., СовыкД.Н.СинтезмонокристалловалмазавСВЧплазме. // Прикладнаяфизика. 2011. Т. 6. С. 104-110.

[3]. Anthony T.R. and Banholzer W.F. Properties of diamond with varying isotopic composition // Diamond and Related Materials. 1992. V.1. P. 717-726.

[4]. Wei L., Kuo P.K., Thomas R.L., Anthony T.R., Banholzer W. F. Thermal conductivity of isotopically modified single crystal diamond// Phys. Rev. Lett. 1993. V. 70. № 24. P. 3764–3767.

[5]. Holloway H.A., Hess R.A., Tamor M.K., Anthony T.A. and. Banholzer W. F.Isotopic dependence of the lattice constant of diamond. // Phys. Rev. B, V. 44 (1991) P. 7123-7126.

[6]. Bartels W.J., Nijman W. X-Ray double-crystal diffractometry of $Ga_{1-x}Al_xAs$ epitaxial layers// J. Cryst. Growth. 1978. V. 44. P. 518-525.

[7]. Prokhorov I.A., Ralchenko V.G., Bolshakov A.P., Polskiy A.V., Vlasov A.V., Subbotin I.A., Podurets K.M., Pashaev E.M., Sozontov E.A. Analysis of Synthetic Diamond Single Crystals by X-Ray Topography and Double-Crystal Diffractometry // Crystallogr. Rep. 2013. V. 58. № 7. P. 1010-1016.

[8]. Hornstra J., Bartels W.J. Determination of the lattice constant of epitaxial layers of III– V compounds // J. Cryst. Growth. 1978. V. 44. P. 513-517.

[9]. Каминский А. А., Ральченко В. Г., Большаков А. П., Хомич А. А. CVD – алмаз ^{13}C – новый ВКР–активный кристалл // ДАН. 2015. Т. 465. № 6. С. 1-4.

Романов Даниил Алексеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: Oxly12@yandex.ru

Прохоров Игорь Алексеевич - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: igor.prokhorov@mail.ru

Стрельченко Станислав Сергеевич - д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана, Калуга. E-mail: stas40@kaluga.ru

Большаков А.П. – сотрудник ФГБУН Институт общей физики им. А.М. Прохорова РАН. E-mail: bolshak@ran.gpi.ru

Хомич А.А. – сотрудник ФГБУН Институт общей физики им. А.М. Прохорова РАН. E-mail: antares-610@yandex.ru

Ральченко В.Г. - сотрудник ФГБУН Институт общей физики им. А.М. Прохорова РАН. E-mail: ralchenko@nsc.gpi.ru

С.С. Стрельченко, Н.Ю. Козлов

ТЕРМОДИНАМИЧЕСКАЯ МОДЕЛЬ ЛЕГИРОВАНИЯ АРСЕНИДА ГАЛЛИЯ БЕРИЛЛИЕМ В ХЛОРИДНО-ГИДРИДНОЙ ГАЗОФАЗНОЙ ЭПИТАКСИИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Введение.В последние два десятилетия огромное внимание уделяется эпитаксиальному выращиванию структур соединений A3B5 в виде квантовых ям и сверхрешеток [1]. Одной из важных научных и прикладных проблем при этом стала задача выбора оптимального типа легирующей примеси p-типа проводимости.

Наиболее широко используемой примесью для получения p-типа проводимости до последнего времени являлся цинк. Однако его высокое давление паров и большой коэффициент диффузии потребовали поиска более подходящих примесей, как для новых композиций соединений A3B5, так и для уже хорошо освоенных соединений A3B5, в частности арсенида галлия.

Одной из таких перспективных примесей является бериллий [2-4]. Этот элемент уже нашел применение для легирования посредством ионной имплантации и молекулярно-лучевой эпитаксии. Однако, возможности его применения в хлоридно-гидридном методе эпитаксии до настоящего времени исследованы крайне мало. Цель настоящей работы состояла в получении детальных физико-химических данных о поведении бериллия в этой системе методом термодинамического анализа с учетом возможности протекания реакции взаимодействия основных компонентов с конструкционным материалов реактора – кварцем и образующимися при этом промежуточными соединениями. На важность такого учета указывалось в ранних работах по исследованию систем Ga-As-H-Cl и Si-H-Cl[5-7].

Процедура вычисления. Хорошо известно, что определение равновесного состава газовой и конденсированных фаз таких сложных систем при использовании стандартного метода констант равновесия встречает значительные трудности. Поэтому был использован универсальный метод решения этой задачи, основанный на фундаментальном принципе условий равновесия Гиббса [8].

При постоянных значениях давления и температуры равновесный состав изолированной системы определяется путем поиска минимального значения функционала энергии Гиббса вида[9]:

$$G(n_i, n_s, n_k) = \sum_{i=1}^{I} n_i \left[c_i + \ln\left(\frac{n_i}{\sum_{i=1}^{I} n_i} \right) + \ln \varphi_i \right] + \sum_{l=1}^{L} \sum_{s=1}^{S} n_s^l \left[c_s^l + \ln\left(\frac{n_s^l}{\sum_{s=1}^{S} n_s^l} \right) + \ln \gamma_s^l \right] + \sum_{k=1}^{K} n_k c_k \quad (1)$$

при наличии ограничений в виде уравнений материального баланса:

$$\sum_{i=1}^{I} a_{ij} n_i + \sum_{l=1}^{L} \sum_{s=1}^{S} a_{js}^{l} n_s^{l} + \sum_{k=1}^{K} a_{jk} n_k = b_j \text{ (j = 1 ... J)} \quad . \qquad (2)$$

и неравенств:

$$n_i \geq 0 \text{ (i = 1 ... I)}, \; n_s^{l} \geq 0 \text{ (s = 1 ... S; l = 1 ... L)}, \; n_k \geq 0 \text{ (k = 1 ... K)}, \qquad (3)$$

где: i, s, k - нижние индексы относятся к газовой фазе, конденсированным растворам и индивидуальным веществам соответственно; ni,s,k - число молей i,s,k-го элемента системы; ci,s,k - безразмерная функция температуры и давления системы;φi, γsl, - мольная доля вещества в газовом и жидком состоянии соответственно; aij- число атомов j-го элемента в молекуле i-го вещества в системе;bj- количество j-го элемента в системе.

Значения ci,s,k рассчитывают при помощи следующих выражений:

$$c_i = \frac{\Delta_f H_{298}^{0}(i)}{RT} - \frac{\Phi_i}{R} + \ln(p), \qquad c_{s,k} = \frac{\Delta_f H_{298}^{0}(s,k)}{RT} - \frac{\Phi_{s,k}}{R} \quad , \qquad (4)$$

где: ΔfHo298- энтальпия образования из простых веществ в стандартном состоянии; $\Phi_{i,s,k} = -\frac{\Delta_f G_T^{0}(i,s,k) - \Delta_f H_{298}^{0}(i,s,k)}{T}$ - приведенная энергия Гиббса (функция Массье - Планка) составляющей системы; $\Delta H_T = \Delta_f H_{298}^{0} + \int_{298}^{T} \Delta C_p(T) dT$ - энтальпия образования из простых веществ при температуре T; ΔCp - теплоемкость вещества при постоянном давлении; R - универсальна газовая постоянная;T - абсолютная температура; p - относительное значение общего давления системы к давлению в стандартном состоянии (т.е. к 1 атм).

Из-за сложности системы Si-O-H-Cl-Ga-As-Be, определяющей процессы роста арсенида галлия и его легирования бериллием с учетом возможности «паразитных реакций», расчет проводился в несколько этапов. На первом этапе для выбора наиболее значимых химических форм были проведены расчеты вспомогательных систем (H-Cl-Be, Si-O-H-Cl, Si-O-H-Cl-Be, H-Cl-Ga-As, Si-O-H-Cl-Ga-As) часть из которых была ранее исследована американскими и японскими учеными [6,7,10-14].

После проведения таких предварительных расчетов, результаты которых в соответствующей части подтвердили данныепредыдущих работ, были выбраны следующие компоненты для учета в газовой фазе: As2, As4, AsH3, AsO, Be, BeCl, BeCl2, BeClOH, BeH2, Ga, GaCl, GaCl2,GaCl3,GaH, GaO, GaOH, H2, HCl, H2O, SiCl2, SiCl3, SiCl4, SiH4, SiHCl3, SiH2Cl2,

SiH3Cl, SiO; и в твердой фазе: Be, BeO, Si, SiO2, GaAs.Все расчеты проводились в соответствии со схемой хлоридно-гидридной эпитаксии при стандартном давлении.

Метод хлоридно-гидридной эпитаксии имеет две особенности, отличающие его от других используемых методов эпитаксии из газовой фазы – металлоорганической газофазной эпитаксии и молекулярно-лучевой эпитаксии из химических пучков. Во-первых, в отличие от последних, стенки реактора в этом методе имеют температуру соответствующих зон. Во-вторых, в составе исходных и промежуточных продуктов имеются хлорсодержащие вещества, которые могут активно вступать в реакции с основным конструкционным материалом реактора – кварцем, а также с промежуточными веществами, образующимися в результате взаимодействия с кварцем. Как показывают результаты исследований этих процессов в системах Ga-As-H-Cl и Si-O-H-Cl, количество образующихся при этом веществ достигает многих десятков, и состав из них может оказывать определяющее влияние на параметры осаждаемых эпитаксиальных слоев. В частности, достаточно упомянуть о существенном снижении фазового легирования примесями n-типа при увеличении отношения Cl/H [7,10].

Результаты и обсуждение. В работе были получены зависимости состава газовой и конденсированной фаз в широком диапазоне используемых в хлоридно-гидридном методе эпитаксии параметров: температуры в диапазоне 600-900 ˚С и отношения Cl/Нот 10-3 до 100.

Полученные данныесвидетельствуют о значительном образовании твердой фазы кремния на всем диапазоне исследованных параметров.В тоже время наличие образующегося элементарного бериллия ничтожно мало.

В предположении, что образующиеся твердые фазы кремния и бериллия входят в состав арсенида галлия, образуя идеальный раствор, из полученных выше данных можно построить теоретические зависимости «уровня легирования» бериллием и кремнием. Данные такого рода представлены на рис. 1.

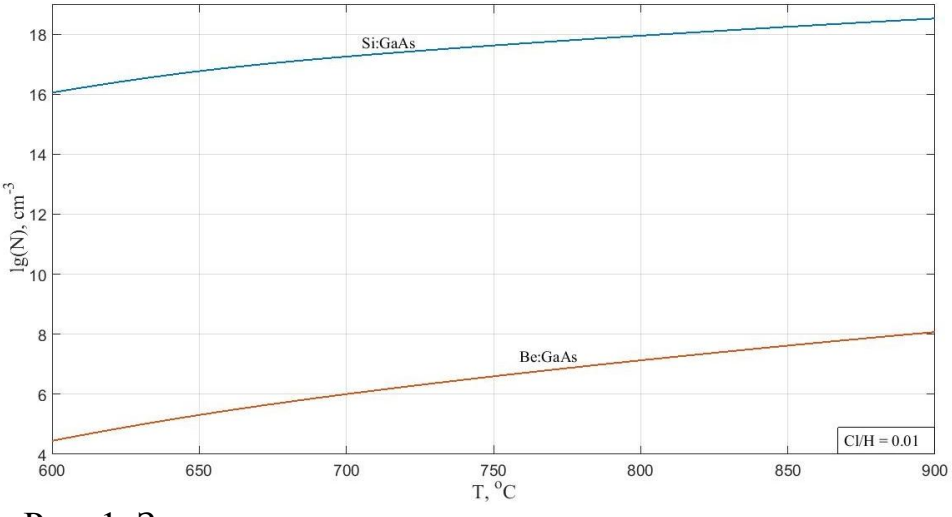


Рис. 1. Зависимость уровня легирования от температуры

Очевидно, что эти данные должны рассматриваться как некоторая исходная точка для сопоставления с экспериментальными данными, так как они абсолютно не учитывают кинетики как процесса роста арсенида галлия, так и процесса вхождения примеси. Однако, колоссальный разрыв в «уровне легирования» кремнием и бериллием, полученный в равновесном приближении позволяет подтвердить вывод экспериментальной работы [5]о том, что наличие кварцевой оснастки эпитаксиального реактора не позволяет рассчитывать на получение p-типа проводимости арсенида галлия за счет примеси бериллия. Изучение возможных условий решения этой задачи является предметом нашей дальнейшей работы.

Выводы.Из полученных данных следует, что достичь высокий уровень легирования (>1015 cm-3) арсенида галлия бериллием в хлоридно-гидридном методе эпитаксиального наращивания не возможно из-за протекания побочных реакций взаимодействия транспортных соединений бериллия с кварцевыми стенками реактора и парами воды в системе. В результате протекания таких реакций основная доля транспортных соединений бериллия расходуется на образование твердой фазы оксида бериллия. При этом в системе из-за разложения силанов образуется твердая фаза кремния, которая может осуществлять вторичное легирование с n-типом проводимости, что приводит к компенсации примеси p-типа.

ЛИТЕРАТУРА

[1]. Келсалл Р., Хэмли А., Геогеган М. *Научные основы нанотехнологий и новые приборы*. Учебник – монография, Долгопрудный, Издательский Дом «Интеллект», 2011, 528 с.

[2]. Ohtsuka N.,Kodama K., Ozeki M., Sakuma Y. ExtremelyhighBedopingofInGaAsbylow-temperatureatomiclayerepitaxy.*JournalofCrystalGrowth*,1991, vol. 115, pp. 460-463.

[3]. Shigeo F.,Bedair S.M., Littlejohn M.A., Hauser J.R.Doping characteristics and electrical properties of Be-doped p-type AlxGa1−xAs by liquid phase epitaxy.*Journal of Applied Physics*, 1980, vol.51, pp. 5438-5444.

[4]. Parsons J.D.,Lichtmann L.S., Krajenbrink F.G., Brown D.W. MOVPE growth of beryllium-doped gallium arsenide using diethylberyllium.*Journal of Crystal Growth*,1986, vol. 77, pp. 32-36.

[5]. ПашинкинА.С., МалковаА.С., ШубинаВ.В., СтрельченкоС.С., МатяшА.А. Легирование эпитаксиальных слоев арсенида галлия бериллием в хлоридном методе.*Электроннаятехника*, 1978, №3, с.55–59.

[6]. Sirtl E., Hunt L.P.,Sawer D.H. High temperature reactions in the Silicon-Hydrogen-Chlorine system. *Journal of the Electrochemical Society*, 1974, vol. 121, pp. 919 – 925.

[7]. Dilorenzo J.V. Vapor growth of epitaxial GaAs: a summary of parameters which influence the purity and morphology of epitaxial layers. *Journalof-CrystalGrowth*, 1972, vol. 17, pp. 189-206.

[8]. Snider J., Griva I., Sun X., Emelianenko M.Set based framework for Gibbs energy minimization.*CALPHAD*, 2015, vol. 48, pp. 18-26.

[9]. ГлазовВ.М., Павлова Л.М.*Химическая термодинамика и фазовые равновесия.*Москва, Металлургия, 1988, 560 с.

[10]. Dilorenzo J.V., Moare J.E. Effects of the $AsCl_3$ mole fraction on the incorporation of germanium, silicon, selenium, and sulfur into vapor grown epitaxial layers of GaAs. *Journal of the Electrochemical Society*, 1971, vol. 11, pp. 1823 – 1830.

[11]. Rai-Choudhury P. Thermodynamic of Ga-$AsCl_3$-H_2 system and dopant incorporation. *Journal of Crystal Growth*, 1971, vol. 11, pp. 113-120.

[12]. Herrick C.S., Sanchez-Martinez R.A. Equilibrium Calculations for the Si-H-Cl system from 300 to 3000 K. *Journal of the Electrochemical Society*, 1984,vol. 131, pp. 455-458.

[13]. Hunt, L.P. Thermodynamic equilibria in the Si-H-Cl and Si-H-Br systems. *Journal of the Electrochemical Society*, 1988, vol. 135, pp. 206 – 209.

[14]. Gao Y.Edgar J.H. Selective epitaxial growth of SiC: Thermodynamic analysis of the Si-C-Cl-H and Si-C-Cl-H-O systems. *JournaloftheElectrochemicalSociety*, 1997, vol. 144, pp. 1875-1880.

Стрельченко Станислав Сергеевич - д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана, Калуга. E-mail: stas40@kaluga.ru

Козлов Николай Юрьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: kozlov-nik@rambler.ru

Д.П. Островский, С.А. Адарчин, В.Г. Косушкин

ТОЛСТОПЛЕНОЧНАЯ ТЕХНОЛОГИЯ В ПРОИЗВОДСТВЕ ПОДЛОЖЕК СИЛОВОЙ ЭЛЕКТРОНИКИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время на рынкепрактически отсутствуют подложки для изделий силовой электроники Российского производства. Поэтому необходимаразработка конкурентоспособных способов производства подложек, получивших название DirectCupperBonding(DCB)в условиях отечественных производств. Применение толстопленочной технологии, стандартной для целого ряда отечественных предприятий позволит достигнуть технических параметров, соизмеримых с параметрами подложек, предлагаемых сегодня на международном рынке и значительно снизить цену[1]. Не мало важным при этом остается и вопрос обеспечения импортозамещения, который одновременно решается.

Силовая электроника широко распространена в различных областях народного хозяйства. От бытовой и автомобильной техники до авионики необходимы высокоэффективные интеллектуальные системы энергообеспечения, показывающие высокую экономическую эффективность. Целью нашей работы была разработка технологии производства подложек для силовой электроники с параметрами, сравнимыми с DCB на базе толстопленочной технологии.

Для достижения поставленных результатов было необходимо подобрать дешевый толстопленочный материал, способный обеспечить высокую электропроводность и надежность при условии низкой цены, разработать технологию его применения и определить параметры получаемых подложек. Перспективы этого метода обусловлены наличием в России производственного оборудования и специалистов, способных обеспечить весь комплекс требований, предъявляемых к таким изделиям.

В качестве материалов для подложек силовой электроники была выбрана алюмонитридная керамика и толстопленочная проводниковая паста на базе меди. Выбор этих материалов обусловлен тем, что алюмонитридная керамика обладает высокой теплопроводностью и сравнительно хорошими механическими свойствами по сравнению с другими керамиками [2].

В классической толстопленочной технологии применяются проводниковые пасты на базе драгоценных металлов. Этот факт обуславливает и основные параметры получаемых отпечатков по классической технологии. Основными требованиями к проводникам, получаемым по классической технологии была величина адгезии отпечатка и минимальная толщина, что обусловлено высокой стоимостью исходных материалов. Предложенный в ходе выполнения работы вариант толстопленочной пасты на базе меди позволит решить проблему обеспечения

высокой электропроводности за счет использования отпечатков большой толщины. Вместе с тем, применение такого материала может внести ряд затруднений в классическую толстопленочную технологию. Медь в отличии от драгоценных металлов подвержена окислению при температурах вжигания паст, которые могут достигать 900 ^{0}C. Решение проблемы окисления так же стало одной из задач настоящей работы.

Разработка технологии изготовления подложек.В качестве базовой технологии была взята классическая толстопленочная технология, приведенная в работе [3]. Для устранения эффекта окисления было предложено в лабораторных условиях проводить вжигание толстопленочной пасты в кварцевой капсуле, заполненной инертным газом. В настоящее время за счет дешевых способов получения азота этот газ стал применяться во многих технологических процессах. По этой причине в качестве инертного газа был выбран азот.

Предварительная подготовкаалюмонитридных подложек включала в себя очистку поверхности от загрязнений и термообработку.

Качество подготовленной поверхности контролировалось визуально с помощью микроскопа. Толстопленочная технологияпозволяет многократное нанесение отпечатков для получения необходимых толщин проводников, обеспечивающих требуемую теплопроводность. Кроме того, нанесение слоев допускается с двух сторон подложки, что позволит изготавливать теплоотводящие слои.

Классические толстопленочные пасты имеют незначительную вязкость, что обеспечивает малую толщину отпечатков [3]. В случае силовой электроники это требование является противоречивым. Было предложено применение паст с высокой вязкостью [1].

По методике, приведенной в нашей предыдущей работе [4] была изготовлена партия подложек. Электрофизические свойства полученных отпечатков соответствовали свойствам металлической меди.

Таблица 1. Электрофизические свойства

Свойство	Металлическая медь	Медный отпечаток
Теплопроводность, Вт/(м ·)	401	320.8
Электропроводность, МСм,	59,5	47,6
Плотность, кг/	8,9* 1	7,1* 1

На рисунке 1 приведены результаты измерения адгезии отпечатков к поверхности керамики. Необходимо отметить, что полученные результаты полностью соответствуют требованиям к адгезии проводниковых слоев как в классической технологии, так и в DCB.

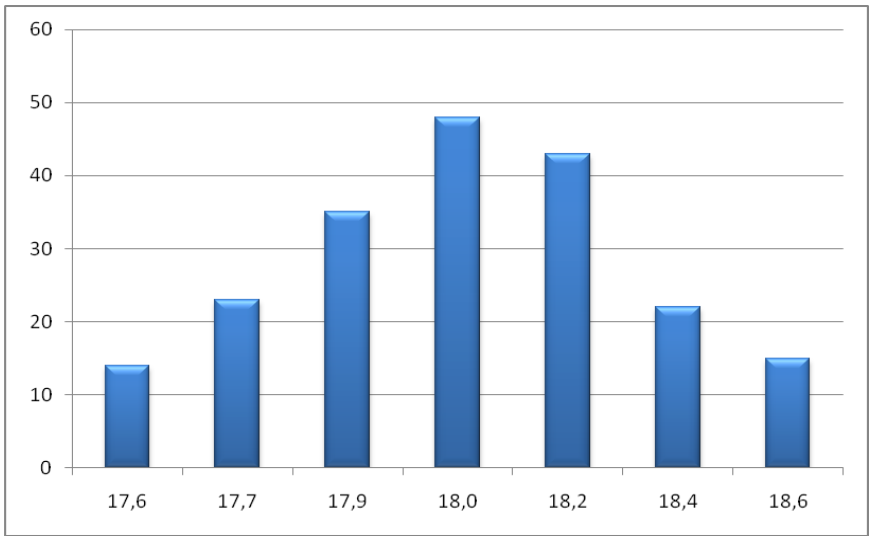


Рис. 1. Гистограмма распределения значений адгезии медной пасты к подложке, Н

Вывод.Была изготовлена опытная партия изделий для которой получен уровень адгезии, составивший 18Н, удовлетворяющий предъявляемым требованиям.

Список литературы

[1]. Разработка способа получения металлокерамических подложек для приборов силовой электроники. Молодёжная конференция ИННОСТАРТ - 2014. Тезисы итогового мероприятия по Программе "Участник молодежного научно - инновационного конкурса 2014". Обнинск, 13 - 14 ноября 2014 г., 80 с.

[2]. Медведев А. М. Печатные платы. Конструкции и материалы. Москва, Техносфера, 2005, 304 с.

[3]. Коледов Л. А. Технология и конструкции микросхем, микропроцессоров и микросборок: Учебник для вузов. Москва, Радио и связь, 1989. 400 с.

[4]. Толстопленочная технология, как инструмент создания силовой электроники. Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе: материалы Региональной научно-технической конференции. 22-25 апреля 2014 г. Т. 2. М.: Издательство МГТУ им. Н.Э. Баумана, 2014 г., 254 с.

Островский Дмитрий Петрович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: blackswan.94.klg@gmail.com

Адарчин Сергей Александрович - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: adarchin@rambler.ru

Косушкин Виктор Григорьевич - д-р техн. наук, зав. каф. КФ МГТУ им. Н.Э. Баумана. E-mail: kosushkin@gmail.com

СЕКЦИЯ 12.

СОВРЕМЕННЫЕ ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ И МЕТОДЫ КОНТРОЛЯ В ЭЛЕКТРОНИКЕ И МИКРОЭЛЕКТРОНИКЕ

С.А. Лоскутов, Д.И. Терещенко

АНАЛИЗ ВОЗМОЖНОСТЕЙ САПР PULSONIX В СРАВНЕНИИ С ПАКЕТОМ PCAD

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время, несмотря на достаточно широкий спектр различных САПР для проектирования печатных плат, стандартом де-факто для проектирования в нашей стране остается PCAD различных версий. Это связано со многими причинами: парк отечественных ПЭВМ в основной своей массе представлен всевозможными IBM-совместимыми машинами; сама программа прошла длинный путь от версии 4.5 до версии 2006 (для IBM-платформ) [1]; также далеко не последней причиной является широкое распространение различных версий пакета PCAD на территории нашей страны.

Однако если посмотреть на проблему проектирования печатных плат более широко, то выясняется, что выбор отечественных специалистов в сторону PCAD далеко не оптимален. Во-первых, пакет PCAD ориентирован исключительно на проектирование печатных плат, он не является САПР, предлагающей сквозное проектирование от создания схемы, ее электрического моделирования и заканчивая трехмерным представлением готовой несущей конструкции. Во-вторых, интерфейс пользователя PCAD весьма путанный и тяжел для первоначального освоения. В-третьих, PCAD снят с производства и более не поддерживается. В-четвертых, для полноценной работы даже непосредственно с проектированием печатных плат, пакета PCAD не достаточно, требуется (желательно) наличие внешнего трассировщика от сторонних фирм (чаще всего Specctra от Cadence), также желательна пост-обработка Gerber-файлов опять-таки во внешней САПР (CAM-350). За последние годы появилось достаточное количество САПР, предлагающих сквозное проектирование, но либо переход на них достаточно сложен, либо цена их весьма высока.

Целью данной статьи является краткое знакомство-анализ САПР Pulsonix – системы проектирования печатных плат, выпускаемой английской компанией Westdev Ltd [2].

Данный продукт рекомендуется для плат среднего уровня сложности и включает редактор схем многолистовых проектов, редактор печатных плат, средства автоматической и полуавтоматической трассировки, смешанного аналого-цифрового моделирования. Позиционируется как наиболее простая замена снятому с производства несколько лет назад продукту P-CAD 2006 компании Altium.

Начиная с версии 6.0, продукт обеспечивает следующие функции:

— полностью поддерживает работу под управлением Microsoft Windows 7/8;
— поддерживает два монитора, что позволяет просматривать схему на одном экране, а топологию на другом;
— в редактор плат добавлена функция Rules By Area, позволяющая задавать специфические правила для конкретных областей платы;
— в редактор компонентов введена новая функция документирования библиотек, позволяющая включать в отчеты графическое изображение символов и топологических посадочных мест компонентов;
— добавлена функция Embedded Views, позволяющая добавлять в проект рисунки с масштабированными видами отдельных участков топологии;
— введена возможность задавать область, определяющую зазоры между компонентами;
— введена возможность назначения одному выводу схемотехнического символа нескольких выводов на топологическом посадочном месте;
— добавлена возможность задавать разные стили отображения текста и атрибутов для разных вариантов в многовариантном проекте.

Программа имеет мощный набор трансляторов файлов данных из различных популярных систем проектирования, благодаря чему позволяет сохранить все сделанные ранее наработки. Имеются интерфейсы связи с программами трассировки Specctra и Electra.

Начиная с версии 7.0, поддерживает формат STEP, который де-факто стал промышленным стандартом обмена данными между 3D механических систем проектирования (MCAD). Интерфейс Pulsonix STEP был разработан для импорта проектных данных из таких систем как SolidWorks и Autodesk Inventor, например, контура печатной платы и контуров запрещенных зон (cutout), а также трехмерных моделей компонентов.

Также с версии 7.0 поддерживаются следующие функции:
— масштабирование символов на схемах;
— отображение допусков в обозначениях размеров;
— добавление интерактивных меандровых объектов для выравнивания длин пар проводников;
— отображение имен контактных площадок на них;
— отображение кодовой маркировки резисторов на 3D виде;
— измерительный инструмент во всех графических редакторах;
— импорт PCB-файлов в формате Cadence Allegro.

Программа доступна для свободного скачивания с сайта компании-производителя [3] в Light-версии или с ограниченной работоспособностью (отсутствует интегрированный автоматический трассировщик и возможность сохранять проект), однако эти ограничения не мешают ознакомиться с возможностями программы.

Можно выделить следующие отличия Pulsonix от P-CAD 200x:
— продукт не снят с производства, вследствие этого регулярно обновляется, поддерживает современные технологии разработки печатных плат и т.д;

— поддержка Windows 7, 8, 10;
— имеется пакет моделирования схем на основе SPICE;
— интегрируемость – поддерживает огромный набор трансляторов файлов данных в том числе из Altium, Protel, Accel, P-CAD, CadStar, Visula, PCB, PADS, DxDesigner, ViewLogic, Eagle, Integra, OrCAD, Cadence, Allegro, Zuken, CR5000, System Designer, Ultiboard, EdWin. Транслировать можно как схемы, библиотеки, проекты плат, так и контуры печатных плат или контуры запрещенных зон (CutOut) из AutoCad, а также трехмерные модели компонентов;
— поддержка правил проектирования высокоскоростных плат. Для пользователей опции Interactive High Speed Routing, обеспечивающей возможность проектирования высокоскоростных плат, реализован ряд полезных функций. В частности, теперь можно оперативно отслеживать длину прокладываемого сегмента и всей цепи. При прокладке дифференциальных пар на экране отображается разница между длинами проводников в паре. Кроме того, имеется возможность добавить к дифференциальной паре меандр, увеличивающий длину проводников;
— поддержка скриптов Active-X. В P-CAD 200x была только поддержка макросов для упрощения однотипной работы. Программа Pulsonix поддерживает обработку скриптов, написанных на языках VBscript, JavaScript, PythonScript или любом другом языке, который может быть инсталлирован в систему, как поддерживающий технологию Active-X. Скрипт может быть запущен непосредственно из среды проектирования Pulsonix и извне из командной строки. Поддержка скриптов в Pulsonix реализована в виде простого в использовании диалогового интерфейса редактирования и отладки. Язык команд оформлен в структурированном стиле с HTML ссылками, облегчающем его понимание и использование. Скрипты могут использоваться, например, для написания процедуры генерации списков соединений пользовательских форматов или управляющих файлов для аппаратуры расстановки компонентов с добавлением в них специфической информации о компонентах в зависимости от их типов;
— поддержка технологии лазерных микропереходов Micro Via. При определении типа переходного отверстия, некоторые из них могут быть обозначены, как Micro Via, изготавливаемые лазерным прожиганием. Обработка таких отверстий в программе будет выполняться особым образом. В программу введены специальные стили контактных площадок Micro-via Entry Pad и Micro-via Stop Pad, описывающие размеры начальной и конечной площадок микроперехода. Каждый набор типов переходов может быть записан в отдельный файл для соответствующей технологической обработки. Данная функция доступна пользователям опции Advanced Technology. Модули трехмерного просмотра платы и просмотра стека слоев позволяют отображать все заданные в проекте типы переходных отверстий и выполнять их визуальную верификацию;

— кроме поддержки современных автотрассировщиков, таких как Spectra и Electra, продукт имеет свой собственный встроенный автотрассировщик. Программа использует численно стабильный математический алгоритм, что означает возможность трассировать топологии с компонентами, имеющими очень плотное расположение выводов. Автотрассировщик имеет преобладающий диагональный режим со скосами под углом 45 градусов и демонстрирует результат, более похожий на результат ручной трассировки;
— новая функция редактора плат позволяет размещать объекты на топологии на сетке с полярными координатами, что упрощает проектирование плат с закругленными или криволинейными краями. Функция работает и для заимствованных блоков, в этом случае копирование в полярных координатах будет применено как для компонентов, так и для проводников. При размножении блоков в качестве шага может задаваться угловой шаг;
— данный продукт поддерживает создание групповых заготовок для выпуска печатных плат, причём при изменении в трассировки групповая заготовка будет автоматически перерисована в рамках проекта;
— поддерживает Gerber X2, IPC-2581 Netlist Export. Гибкий инструмент разводки проводников поддерживает такие функции как: каплевидные контактные площадки, нестандартная форма дорожек, нестандартная форма контактных площадок (в соответствии с контуром из AutoCAD например), добавление переходных отверстий вдоль проводника. Продукт содержит в себе встроенные средства для вывода и просмотра 3D вида печатной платы с возможностью экспорта в SolidWorks.

К сожалению, пока в русскоязычной литературе и интернет-пространстве программа сквозного проектирования РЭС Pulsonix почти не представлена, но, судя по отдельным отзывам, завоевывает все большую популярность. Надеемся, что этот краткий обзор заинтересует всех, кто работает в области проектирования РЭС.

Список литературы

[1=. От P-CAD 4.5 к P-CAD 2002: взаимодействие и совместное применение при проектировании печатных плат.
http://www.chipinfo.ru/literature/chipnews/200306/14.html
[2]. Pulsonix: http://www.pulsonix.com/
[3]. Download Pulsonix: http://www.pulsonix.com/softwaredownload request.asp

Лоскутов Сергей Александрович - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: SergeL-75@yandex.ru

Терещенко Дмитрий Иванович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: vitamin937@rambler.ru

А.О. Корякин, В.В. Сорочан

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ АВТОМАТИЗАЦИИ В ПОДБОРЕ ТЕХНОЛОГИЧЕСКИХ ПАРАМЕТРОВ ПРОИЗВОДСТВА СОЛНЕЧНЫХ ЭЛЕМЕНТОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Основным направлением альтернативной энергетики является поиск и использование нетрадиционных источников энергии. Причина поиска альтернативных источников энергии — ограниченность традиционных источников, а также глобальные экологические проблемы из–за их использования.

Солнечная энергетика — направление альтернативной энергетики, основанное на непосредственном использовании солнечного излучения для получения энергии в каком-либо виде. Солнечная энергетика использует неисчерпаемый источник энергии и является экологически чистой, то есть не производящей вредных отходов во время активной фазы использования. Производство энергии с помощью солнечных электростанций хорошо согласовывается с концепцией распределённого производства энергии[1].

К основным достоинствам солнечных элементов можно отнести:

— общедоступность и неисчерпаемость источника энергии;
— теоретически признанная экологическая безопасность солнечных батарей;
— солнечные батареи практически не изнашиваются, поскольку не содержат движущихся частей и крайне редко выходят из строя;
— длительный срок службы без ухудшения эксплуатационных характеристик - 25 лет и более, что подтверждено многолетней практикой использования;
— функционирование солнечных батарей не зависит от технических неполадок энергопоставщиков;
— солнечным батареям не нужно топливо, что дает возможность не зависеть ни от цен на него, не от проблем с транспортировкой;
— солнечные батареи бесшумны, чем выгодно отличаются от ветровых систем;
— при увеличении энергопотребления и/или финансовых возможностей домовладелец, использующий солнечные батареи в качестве источника электроснабжения, может увеличивать мощность системы за счет добавления дополнительных фотоэлектрических модулей.

Солнечный элемент представляет собой фотоэлектрический генератор постоянного тока. Преобразование энергии основано на фотоэлектрическом эффекте, который возникает в неоднородных полупроводниковых структурах при воздействии на них солнечного излучения [2].

Так как один солнечный элемент не производит достаточного количества электроэнергии для большинства применений, солнечные элементы со-

бирают в солнечные модули для получения требуемой мощности. Фотоэлементы представляют собой пластину, размеры которой по технологическим особенностям производства не могут превышать определенного значения. Для их производства применяются различные полупроводниковые материалы. В настоящее время наибольшее распространение получили монокристаллические кремниевые фотоэлементы. Это связано с тем что технология получения монокристаллического кремния хорошо отработана в производстве интегральных микросхем.

Для получения необходимой мощности и выходного напряжения комбинируют последовательное и параллельное соединении этих элементов между собой, набирая фотоэлектрические модули. Их объединяют в фотоэлектрические системы. Мощность кремниевых фотоэлектрических модулей составляет от 40 до 260 Wp (пиковый ватт, т.е. мощностью максимум в 40-260 Вт при ярком солнце). Они имеют размеры от 0,4 до 2,5 м²[4].

Учитывая довольно широкое распространение солнечных батарей будет актуальным создание автоматизированной системы расчета технологических параметров их изготовления, обеспечивающих требуемые выходные характеристики.

Список литературы

[1]. Альтернативная энергетика, энергосбережение, экология: Ветроэнергетика. [Электронный ресурс]. Режим доступа:http://altenergetics.ru

[2]. Виссарионов В.И., Дерюгина Г.В., Кузнецова В.А., Малинин Н.К.; под ред. В.И. Виссарионова. — Солнечная энергетика: учеб. пособие для вузов. — М.: Издательский дом МЭИ, 2008. — 276 с.

[3]. Солнечные батареи [Электронный ресурс]. Режим доступа:http://solbat.ru/

[4]. А.В. Левшов , А.Ю. Фёдоров. Электроника и энергетика. Издательство: Наукові праці ДонНТУ. – Д., 2013. –158 с

Корякин Александр Олегович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: nautamdb9@gmail.com

Сорочан Виталий Викторович - канд. физ.-мат. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: vsorochan@mail.ru

В.В. Кузнецов, А.А. Корнеев, А.В. Иванов

МОДЕЛИРОВАНИЕ СРЕДСТВ КОНТРОЛЯ ИНДУКТИВНЫХ ДАТЧИКОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Индуктивный датчик — бесконтактный датчик, предназначенный для контроля положения объектов из металла (к другим материалам не чувствителен). Индуктивные датчики широко используются для решения задачАСУ ТП. Выполняются с нормально разомкнутым или нормально замкнутым контактом.

Принцип действия основан на изменении параметров магнитного поля, создаваемогокатушкой индуктивностивнутри датчика.

Объектом исследований является стенд для контроля индуктивных датчиков. С его помощью можно проверять обмотки индуктивных датчиков как отдельно, так и внутри схемы. Возможно определить не только целостность обмотки, но и наличие в ней короткозамкнутых (КЗ) витков.

Прибор выполнен на основе микросхем средней степени интеграции: компараторов, логических элементов КМОП и триггеров Шмитта. Стенд обеспечивает проверку датчика и световую индикацию его исправности.

Цель данной работы – создать модель стенда и объекта контроля (датчики). На текущем этапе производится подбор и тестирование ПО для моделирования объекта и создание библиотеки компонентов. Для моделирования данной схемы планируется использовать симулятор электронных схем Qucs-S.

Qucs [1-4]— это симулятор электронных схем с открытым кодом. Qucs использует ядро моделирования Qucsator, разработанное с нуля. Это ядро имеет много преимуществ (моделирование S-параметров [4], расширенный постпроцесоор), но также имеет многочисленные баги, связанные с моделированием во временной области (Transient analysis). Для преодоления этого недостатка был разработан набор патчей spice4qucs, позволяющий моделировать схемы при помощи SPICE-совместимых движков (Ngspice или XYCE), и подготовлен специальный выпуск с интегрированным набором патчей: Qucs-0.0.19S (Qucs-S) [5-8].

Формат схемного файла Qucs основан на XML и к нему поставляется документация. Поэтому схема Qucs может быть легко сгенерирована сторонними программами. Это позволяет создавать ПО для синтеза схем, которое является расширением Qucs. Проприетарное ПО как правило использует бинарные форматы.

Библиотека компонентов использует собственный формат, основанный на XML. Но можно импортировать существующие

библиотеки компонентов, основанные на SPICE (приводятся в даташитах на электронные компоненты).

Возможности версии Qucs-S [5]:

— Большинство компонентов Qucs совместимо со SPICE. Поддерживаются подсхемы, библиотечные компоненты. О несовместимых компонентах во время моделирования выдаётся сообщение об ошибке: These components are SPICE-incompatible… Система уравнений (Equations) Qucs частично совместима со SPICE. об ограничениях читать документацию [8].

— Добавлены виды моделирования совместимые со SPICE: .FOURIER, .NOISE и .DISTORTION Моделирование S-параметров не работает с Qucs-S.

— Qucs-S позволяет моделировать схемы, недоступные симулятору Qucsator. Прежде всего это силовая электроника, ключевые схемы, схемы на полупроводниковых приборах, работающих с заходом в режим отсечки, и схемы с большим количеством компонентов.

Пример схемы, собранной в данном симуляторе:

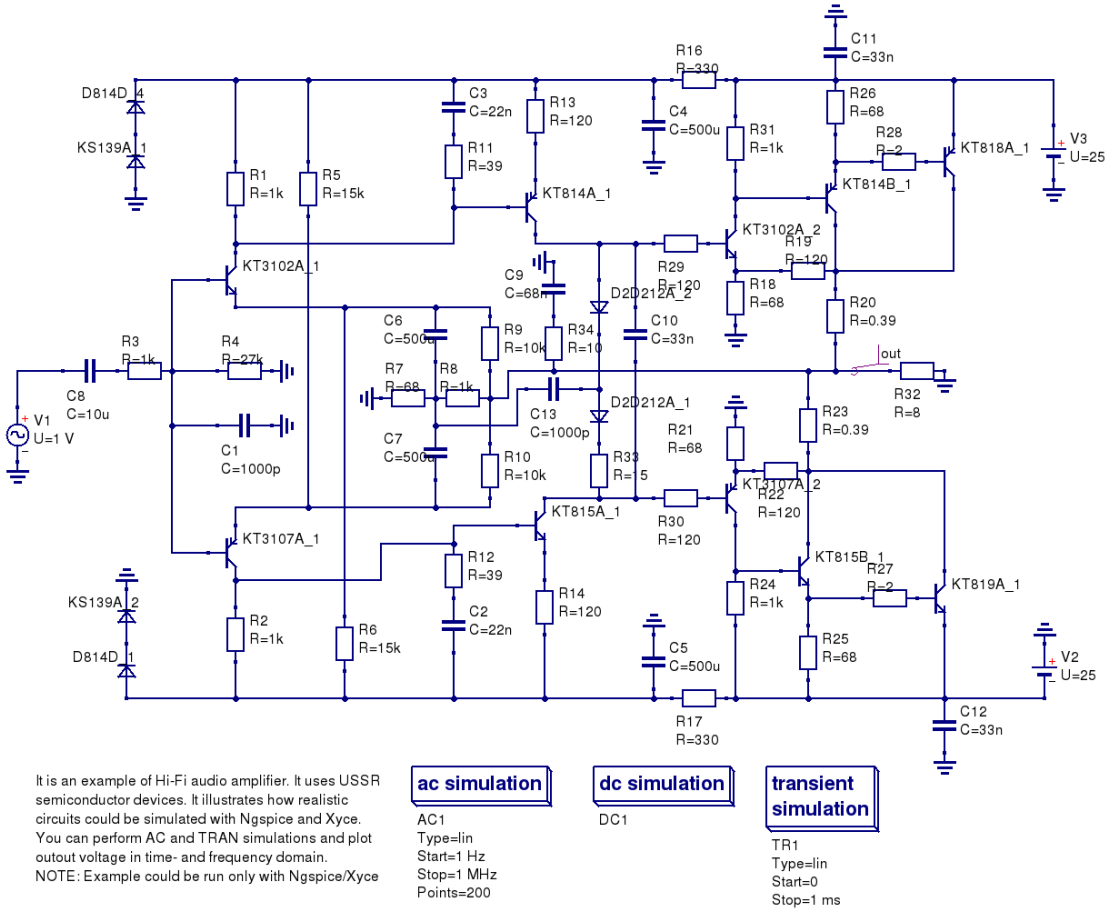


Рис.1. Высококачественный усилитель звука на транзисторах

Таким образом Qucs-S является расширенной версией Qucs, которая позволяет применять его не только для анализа высокочастотных схем, но и для решения задач разработки широкого спектра электронных средств, в

том числе и рассмотренного стенда для контроля индуктивных датчиков. Qucs-S свободно доступен для загрузки [6].

В настоящее время планируется получить результаты анализов таких, как моделирование переходного процесса, моделирование по постоянному и переменному току и построить модель индуктивного датчика на основе компактных моделей [7].

Литература

[1]. Qucs: Quite Universal Circuit Simulator. http://qucs.sourceforge.net.

[2]. Brinson M. E., Jahn S. Qucs: A GPL software package for circuit simulation, compact device modelling and circuit macromodelling from DC to RF and beyond // International Journal of Numerical Modelling (IJNM): Electronic Net-works, Devices and Fields. — 2008. — September. — Vol. 22, no. 4. — Pp. 297 – 319.

[3]. Кузнецов В.В., Симулятор электронных схем с открытым исходным кодом Qucs: основные возможности и основы моделирования. — Компоненты и технологии.- 2015. - №3. - С.114-120.

[4]. Кузнецов В.В. Моделирование высокочастотных схем в частотной области при помощи САПР Qucs. Компоненты и технологии. 2015. № 8 (169). С. 120-127

[5]. M. Brinson, R. Crozier, V. Kuznetsov, C. Novak, B. Roucaries, F. Schreuder, and G. B. Torri. Qucs: An introduction to the new simulation and compact device modelling features implemented in release 0.0.19/0.0.19Src2 of the popular GPL circuit simulator. MOS-AK Workshop, Graz. http://www.mos-ak.org/graz2015/presentations/T_5_Brinson_MOS-AK_Graz_2015.pdf

[6]. V. Kuznetsov. Unofficial build with spice4qucs features enabled. release candidate 3. https://github.com/ra3xdh/qucs/releases/tag/0.0.19S-rc3

[7]. M. Brinson and V. Kuznetsov, “Qucs equation-defined and Verilog-A RF device models for harmonic balance circuit simulation,” in Mixed Design of Integrated Circuits Systems (MIXDES), 2015 22nd International Conference, June 2015, pp. 192–197.

[8]. M. Brinson and V. Kuznetsov. Spice4qucs help documentation. User manual and reference material. https://qucs-help.readthedocs.org/en/spice4qucs/

Кузнецов Вадим Вадимович - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: ra3xdh@gmail.com

Корнеев Александр Анатольевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: sas825@yandex.ru

Иванов Андрей Витальевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: ivanovav@yandex.ru

С.А. Лоскутов, Р.О. Бут

ПОВЫШЕНИЕ ТОЧНОСТИ АМПЛИФАЗОМЕТРИЧЕСКОГО МЕТОДА АНТЕННЫХ ИЗМЕРЕНИЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Наиболее часто измерение параметров антенных устройств проводится в дальней зоне.При этом необходимое расстояние между испытуемой антенной и вспомогательным источником определяется рабочей длиной волны и размерами их апертур и составляет несколько километров.

Однако традиционные методы дальней зоны имеют ряд существенных недостатков и ограничений. Эти недостатки прежде всего обусловлены влиянием различных предметов на подстилающей поверхности полигона и влиянием помех на измерительную аппаратуру [1].

Решением этих проблем является использование методов измерений в ближней зоне. В настоящее время наиболее распространенными являются коллиматорный и амплифазометрический (голографический) методы.

Амплифазометрический метод дает очень хорошие результаты но требует решения широкого круга научных и технических задач в области электродинамики и вычислительной техники, голографии и оптики, математической физики и вычислительной математики, автоматизации измерений и оптимальной обработки информации [2].

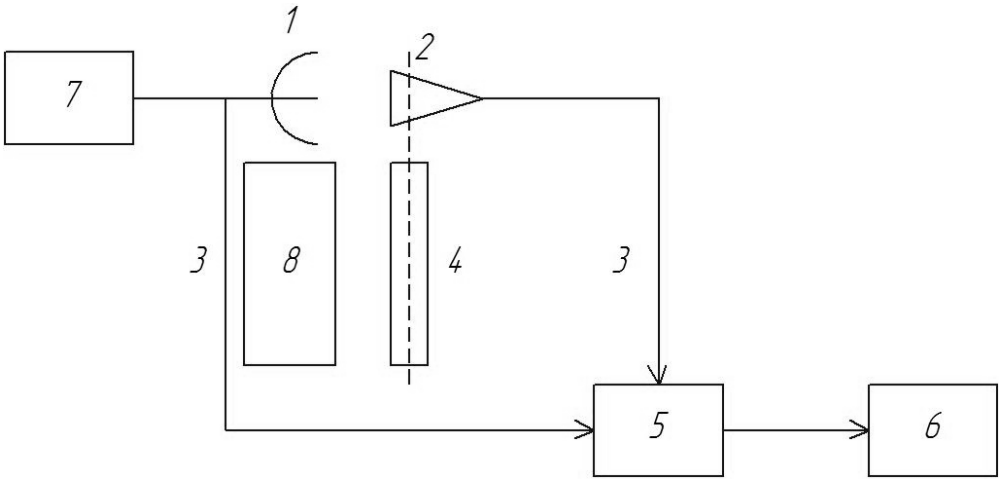


Рис. 1. Структурная схема голографической измерительной установки
1 – испытуемая антенна, 2- измерительный зонд, 3 – линия передачи,
4 – механизм перемещения зонда, 5 – амплифазометр, 6 – устройство регистрации,

С метрологической точки зрения, этот метод так же более сложен, чем метод дальней зоны. В методе дальней зоны отклик испытуемой антенны на плоскую волну получается непосредственно в процессе измерения. В случае

же амплифазометрического метода сначала необходимо определить векторное поле на поверхности вблизи антенны, а затем по дифракционным формулам пересчитать его в диаграмму направленности [3].

Типичная схема амплифазометрической измерительной установки представлена на рисунке 1.

Амплифазометрический метод в первом приближении заключается вследующем. Небольшая слабонаправленная измерительная антенна – зонд – механически перемещается вблизи испытуемой антенны. Для каждого пространственного положения зонда измеряются и запоминаются амплитуда и фаза сигнала на выходе испытуемой антенны. После окончания этой процедуры набор измеренных данных – массив комплексных чисел {En} (индекс n соответствует n-му пространственному положению измерительной антенны) – подвергается обработке. В общем случае обработка сводится к суммированию на ЭВМ комплексных чисел с некоторыми весовыми коэффициентами Dni [1]:

$$F_i = \sum_n D_{ni} \cdot E_n$$

где Fi – массив значений диаграммы направленности для i-ых угловых ориентаций;

Dni – весовые коэффициенты, определяющие связь параметров в ближней и дальней зонах антенны;

En – массив значений амплитудно-фазового распределения в ближней зоне антенны.

При реализации амплифазометрических измерений приходится решать следующие основные задачи: выполнение сканирования ближнего поля антенного устройства, передача СВЧ-сигнала от неподвижного генератора к движущейся измерительной антенне, организация измерительно-вычислительного комплекса и разработка программного обеспечения. Решение каждой из представленных задач накладывает определенные условия и ограничения на техническую и программную реализацию амплифазометрического метода.

Одна из трудностей создания механических сканеров состоит в обеспечении высокой точности механического перемещения. Например, для планарных измерений отклонение измерительной антенны от плоскости сканирования не должно превышать (0,003...0,015)λ, т. е. десятых долей единиц миллиметров в дециметровом и сантиметровом диапазонах длин волн [5]. Такие жесткие требования к точности лимитируют размеры сканирующего устройства.

Решение этой задачи с применением современной элементной базы, высокопроизводительных микроконтроллеров и методов аналого-

цифровой обработки сигналов позволило увеличить разрешающую способность описываемого метода.

Для реализации столь точных механических перемещений кроме совершенствования механической части сканера потребовалась схема контроллера перемещений для управления двигателями с прецизионными параметрами. Для управления перемещением используется современный высокопроизводительный контроллер семейства ATMEGA 64. Большое набор периферии и ресурсов позволяет обойтись высокоуровневым программированием, что значительно облегчило и ускорило решение задачи. Высокие требования к цифро-аналоговому преобразованию (ЦАП) кода, выставляемого микроконтроллером, в аналоговый сигнал управления двигателем потребовали кардинальной переработки узла ЦАП.

Для уменьшения влияния цифровой части устройства использованы современные высокоскоростные изолирующие усилители от ф. «AnalogDevices», в качестве ЦАП выбран сдвоенный преобразователь той же фирмы. Конечное формирование аналогового сигнала управления выполняется по сложной композитной схеме на двух операционных усилителях, что позволяет получить высокую линейность преобразования, требуюемую помехозащищенность и выдержать временную и температурную стабильность параметров сигнала.

Список литературы

[1]. Бахрах Л. Д., Каменский С. Д., Курочкин А. П. Методы измерений параметров излучающих систем в ближней зоне. – Л.: Наука, 1985. – 272 с.

[2]. Марков В. И., Усин В. А., Помазанов С. В., Усина В. А. Измерительно-моделирующие комплексы для настройки и измерения параметров антенн. // Каталог «Крымской конференции «СВЧ и телекоммуникационной техники 2008», 2008, Т. 1, с. 726.

[3]. Воронин Е. Н., Нечаев Е. Е., Шашенков В. Ф. Реконструктивные антенные измерения. – М.: Наука. Физматлит, 1995. – 352 с.

[4]. Бузов А. Л., Тимашков В. А. Опытно-расчетная методика определения пространственных характеристик антенн по результатам измерений амплитудно-фазового распределения ближнего поля. // Электроника и техника СВЧ, КВЧ и оптических частот. 2003. Т. 11, №1(37), с. 34 - 42.

[5]. Захарьев Л. Н., Леманский А. А., Турчин В. И. и др. Методы измерения характеристик антенн СВЧ . Радио и связь, 1985. – 368 с.

Лоскутов Сергей Александрович - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: SergeL-75@yandex.ru

Бут Роман Олегович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: madara_40_rus@mail.ru

Е.Н. Дрожжова, А.Н. Мозохин

ПРОЕКТИРОВАНИЕ СТЕНДА ПРОВЕРКИ БЛОКА ЭЛЕКТРОННОГО СТАБИЛИЗАЦИИ ПЛАТФОРМЫ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Стенд проверки предназначен для формирования управляющих кодовых комбинаций, необходимых для оценки правильного функционирования блока электронного стабилизации платформы. Данный стенд проверки используется для блока электронного стабилизации платформы транспортных средств, перевозящих взрывоопасные и сыпучие грузы, а так же ряд изделий, которые могут доставляться к месту монтажа только в полностью готовом виде.

Целью работы является разработка конструкции стенда проверки блока электронного на базе производства АО «Калужского завода телеграфной аппаратуры (КЗТА)», обеспечивающего контроль важнейших параметров работы блока электронного.

Стенд проверки состоит из модуля управления и коммутатора. Модуль управления выполнен на печатной плате, на которой установлены микропроцессор (микроконтроллер) 1886ВЕ4У, внешний кварцевый генератор и периферийное обрамление, обеспечивающие необходимые режимы работы контроллера.

1886ВЕ4У - высокопроизводительный 8-ми разрядный RISC микроконтроллер. Он предназначен для однокристальной реализации систем передачи, обработки и хранения данных, в том числе с применением внешней энергонезависимой памяти типа NAND Flash, использующих USB интерфейс. Может использоваться для организации малопроизводительных вычислительных систем и в качестве устройства совмещения различных типов интерфейсов. [1]

Так как схемное решение платы позволяет защитить микроконтроллер от выхода из строя, то нет необходимости в использовании такого дорогого микроконтроллера, поэтому возможно рассмотреть замену его на аналог К1886ВЕ4у. По характеристикам они отличия не имеют, есть значительные различия по цене: микроконтроллер 1886ВЕ4У стоит 7250 руб., а цена К1886ВЕ4у – 3100 руб.

Коммутатор получает сигналы с модуля управления, обрабатывает их и передает в блок электронный. Рассмотрим схему коммутатора и уделим внимание некоторым элементам, а именно полевому транзистору 2П7210Б9.

Рассмотрим характеристики полевого транзистора (таблица1):

Таблица 1. Параметры полевого транзистора 2П7210Б9

Параметры	Значения
Ток стока	8 А
Ток стока /начальный ток стока	0,01 мА
Максимально допустимое постоянное напряжение сток-исток	100 В
Максимально допустимое постоянное напряжение сток-исток	±20 В
Допустимое постоянное напряжение затвор-исток	±20 В
Сопротивление сток-исток в открытом состоянии	0,25 Ом
Пороговое напряжение	4,0 В

Как правило, полевой транзистор чувствителен к выбросам напряжения, т.е его вывести из строя не составляет особого труда, и в данном схемном решении используется транзистор стоимостью 1500руб., поэтому я предлагаю заменить этот транзистор на микросхему 142ЕН9В, стоимостью 28 руб.

Трёхвыводной стабилизатор с фиксированным выходным напряжением 27 вольт могут найти применение в широком спектре радиоэлектронных устройств в качестве источниках питания логических систем, измерительной технике, устройств высококачественного воспроизведения и других радиоэлектронных устройств. Внешние компоненты могут быть использованы для ускорения переходных процессов. Входной конденсатор необходим только в том случае, если регулятор находиться на расстоянии более 5 см от фильтрующего конденсатора источника питания. [2]

Рассмотрим микросхемы К142ЕН9В и КР142ЕН9В. Параметры микросхем приведены в таблице 2.

Таблица 2. Параметры микросхем К142ЕН9В (КР142ЕН9В)

Uвых, В	Imax, А	Ku, %/В	Ki, %	TKU, %/К	Uвх max, В	Uвх min, В	Uвых-Uвх min, В	P max, Вт	Т, ^{0}С
27 ±0,54	1,5	0,05	1	0,02	40	23	2,5	6	-45 …+70

Убедимся в правильности выбора микросхемы для платы. Рассчитаем мощность рассеивания и сравним с максимальной мощностью рассеивания микросхемы. Ток потребления (согласно ТЗ) по цепи напряжения 27 В, не более 0,4 А, тогда:

Из расчета следует, что 5,2 Вт < 6 Вт , значит микросхема выбрана верно. В качестве теплоотвода используем алюминиевую пластину с дополнительным чернением.

Эти микросхемы различаются корпусом. Тип корпуса микросхемы К142ЕН9В - 4116.4-2, а КР142ЕН9В - КТ-28-2. В данной схеме нам больше подходит корпус КТ-28-2, т.к он значительно меньше корпуса 4116.4-2, не требует большей затраты места на плате. (рис.1)

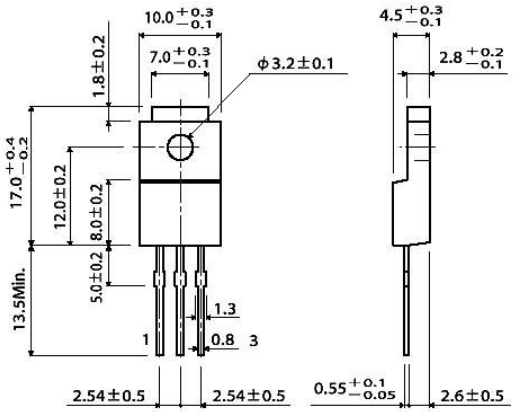


Рис. 1 Корпус микросхемы КР142ЕН9В

Для микросхемы КР142ЕН9В емкость входного конденсатора С2 должна быть не менее 2,2 мкф для керамических или оксидных танталовых и не менее 10 мкФ - для алюминиевых оксидных конденсаторов, а выходного конденсатора С1 - не менее 1 и 10 мкФ соответственно. Роль входного может исполнять конденсатор сглаживающего фильтра, если он расположен не далее 70 мм от микросхемы.[3] (рис.2)

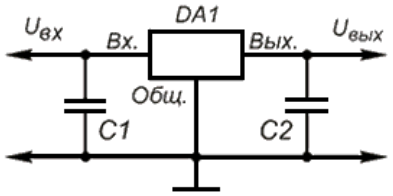


Рис. 2 Типовая схема включения микросхемы КР142ЕН9В

На основание вышесказанного, предлагается замена микроконтроллера на более удешевленный, с теми же характеристиками, а так же рассмотрена замена полевого транзистора 2П7210Б9 на микросхему КР142ЕН9В

В результате выполнения работы предлагается новое схемотехническое решение, которое позволит уменьшить экономические затраты на стенд проверки блока электронного, а так же улучшить надежность данного изделия.

Литература:

[1]. ЗАО «ПКК Миландр». Спецификация 1886ВЕ4У, К1886ВЕ4У., ТКСЯ.431295.004 СП, версия 2.4 от 27.04.2010. С.1-3.

[2]. П.Хоровиц, У.Хилл. Искусство схемотехники: Пер. с англ.- Изд.2-е.- М.:БИНОМ.- 2014. С.360-362.

[3]. А.И. Аксенов, А.В. Нефедов. Микросхемы для бытовой радиоэлектронной аппаратуры. Изд.2-е, дополненное и исправленное – М.:СОЛОН-Пресс, 2009.С.180.

Дрожжова Елена Николаевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: drozhzhova92@yandex.ru

Мозохин Алексей Николаевич – канд. техн. наук, старший преподаватель КФ МГТУ им. Н.Э. Баумана. E-mail: mozohin_an@mail.ru

И.А. Рытиков, В.В. Андреев, А.А. Столяров

РАЗРАБОТКА ИЗМЕРИТЕЛЬНОГО БЛОКА ДЛЯ КОНТРОЛЯ ПАРАМЕТРОВ МИКРОСХЕМЫ 526ПС1СМК

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Данная работа посвящена разработке специального измерительного блока для контроля параметров микросхемы 526ПС1СМК с помощью стенда NIPXIEXPRESS, который работает под управлением программного обеспечения NI LabVIEW. Микросхема 526ПС1СМК представляет собой двойной балансный смеситель электрических сигналов и выпускается на АО «ОКБ Микроэлектроники».

Структурная схема измерительной установки для контроля параметров микросхемы 526ПС1СМК приведена на рис. 1.

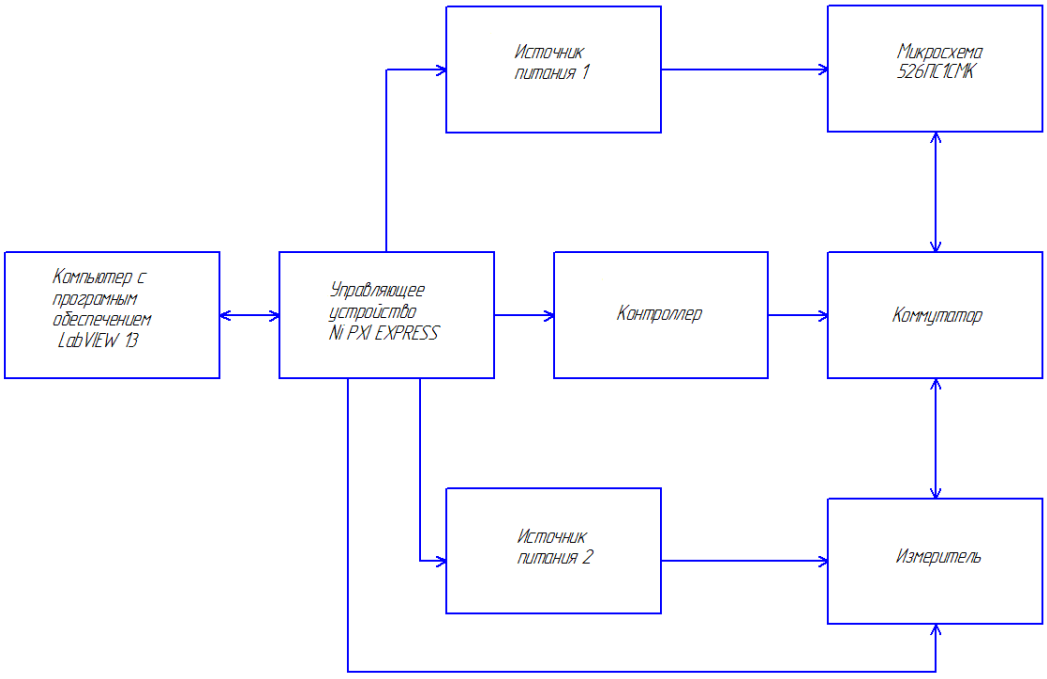


Рис. 1. Структурная схема измерительной установки

Управление установкой осуществляется с использованием управляющего устройства NIPXIEXPRESS, работающего на программном обеспечении LabVIEW. Контроллер необходим для преобразования кода с управляющего устройства в сигнал, подаваемый на коммутатор. Напряжения питания, подаваемые на микросхему и измеритель, формируются с использованием источников питания 1 и 2, соответственно.

Для проведения измерений используются приборы: высокоточный измеритель NI PXI-4132. Программируемый источник постоянного тока NI PXI-4110, цифровой мультиметр NI PXI-4071, вектор анализаторов сигнала NI PXI-5661.

С использованием данной измерительной установки контролируются следующие параметры микросхемы: ток потребления, коэффициенты ослабления входного напряжения, коэффициенты ослабления опорного напряжения, крутизна преобразования. Электрические параметры микросхемы приведены в таблице 1.

Таблица 1. Электрические параметры микросхемы 526ПС1СМК

Наименование параметра, единица измерения	Буквенное обозначение	Норма		Температура, °С
		Не менее	Не более	
1	2	3	4	5
Ток потребления, мА	I_{cc}	-	5,0 6,0 6,0	25 минус 60 125
Коэффициент ослабления входного напряжения, дБ	α_{UI}	8	-	25
Коэффициент ослабления опорного напряжения, дБ	α_{Uref}	65	-	25
Крутизна преобразования, мА/В	S_{con1} S_{con2} S_{con2}	- - -	5 3,5 3,5	25 минус 60 125

Основные характеристики режимов измерения при контроле параметров микросхемы приведены в таблице 2.

Схема измерения тока потребления (I_{cc}) и крутизны преобразования (S_{con})перед испытаниями и после испытаний на воздействие пониженной и повышенной рабочей температуры среды, повышенной влажности воздуха, на безотказность, долговечность, на стойкость к воздействию спецфакторов, представлена на рис. 2. На рис. 2: G1,G2 – генераторы сигналов; G3 – источник питания; DA1 – микросхема; PV1 – вольтметр цифровой универсальный; PV2 – селективный милливольтметр; конденсаторы (C1÷C8 – 1,0 мкФ); резисторы (R1,R2 – 49,9 Ом; R3 – 1 Ом; R4,R5 – 1 кОм).

Таблица 2. Основные технические характеристики режимов измерения

Наименование параметра, единица измерения	Буквенное обозначение	Норма				Время воздействия
		Предельно допустимый режим		Предельный режим		
		не менее	не более	не менее	не более	не более
Напряжение питания, В	U_{cc}	5,4	6,6	5,4	10,5	30 мин.
Входное напряжение по выводам 4,6,10,11, В	U_I	-	0,005	-	1,0	-
Выходной ток, мА	I_0	-	1	-	2	-

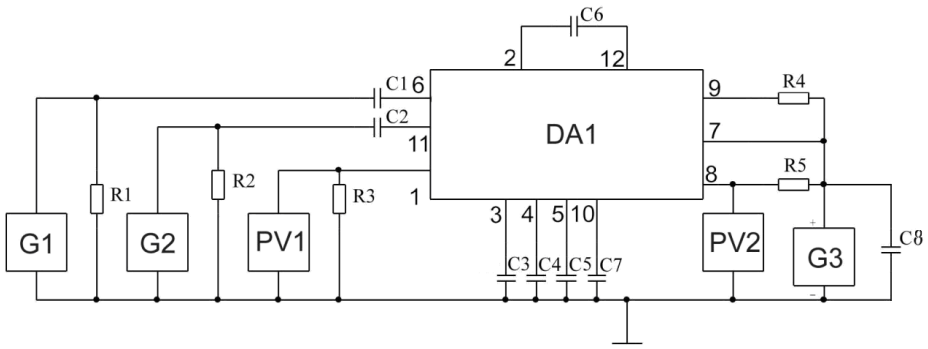


Рис. 2. Схема измерения тока потребления и крутизны преобразования микросхемы 526ПС1СМК

Разработанный измерительный блок позволяет реализовать схему измерения, изображенную на рис. 2, в составе измерительной установки для контроля параметров микросхемы 526ПС1СМК. Использование данного блока позволило уменьшить время измерения параметров микросхемы и упростить сам процесс измерения.

ЛИТЕРАТУРА:

[1]. National Instruments Corporation. All rights reserved.- LabVIEW/ Изданиеоктябрь 2009.- 432с.

Рытиков Илья Алексеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: doktorwww@gmail.com

Андреев Владимир Викторович – д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

Столяров Александр Алексеевич – д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана. E-mail: alalstol@mail.ru

В.В. Кузнецов, Т.С. Моисеев

РАЗРАБОТКА РАСШИРЕННОЙ БИБЛИОТЕКИ КОМПОНЕНТОВ ДЛЯ СИМУЛЯТОРА ЭЛЕКТРОННЫХ СХЕМ QUCS

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Традиционно при подготовке студентов специальностей, связанных с электроникой и радиотехникой используется моделирование электронных схем на ПК. Это позволяет наглядно продемонстрировать работу электронного устройства и провести измерения без физического измерительного оборудования.

Qucs [1-6] – это система автоматизированного проектирования, предназначенная для моделирования аналоговых и цифровых схем электроники на постоянном и переменном токах. Qucs или Quite Universal Circuit Simulatior относится к классу свободного программного обеспечения, и поддерживается системами Windows и системами на базе ядра Linux.

Программа имеет встроенную библиотеку компонентов, однако в ней присутствуют только самые распространенные электронные компоненты в основном зарубежного производства. Поэтому, актуальна задача создания собственных библиотек компонентов.

Производители электронных компонентов в справочной документации на выпускаемую продукцию размещают электронные модели в виде списка цепей PSPICE, чья структура поддерживается библиотеками большинства симуляторов схем. Структура библиотеки Qucs некоторым образом отличается от структуры формата PSPICE.

<Component [имя компонента библиотеки]> – первая строка описания компонента библиотеки;

<Description></Description> – между данными тегами заключается описание компонента;

<Spice></Spice> – между данными тегами заключается отредактированная для Qucs SPICE модель. Секция введена в версии 0.0.19S;

Библиотеки компонентов программы Quite Universal Circuit Simulatior основаны на формате XML, представлены в текстовом формате и имеют возможность редактирования в обычном текстовом редакторе.

Библиотека содержит следующие строки:

<Qucs Library [версия Qucs] «[имя библиотеки]»> - первая строка библиотеки;

<Model></Model> - между данными тегами заключается описание модели компонента

<Symbol></Symbol> - между данными тегами заключается описание символа условного графического обозначения;

</Component> - последняя строка описания компонента библиотеки.

В одну библиотеку может входить довольно много различных компонентов, поэтому получившийся файл может быть довольно длинным.

Возможно два способа создания элементов библиотек Qucs. Первым способом является использование команды qucsconv в командной строке.

$ qucsconv -i [входной файл] -o [выходной файл] - if [формат входных данных] -of [формат выходных данных] -d [имя переменных]

Данная команда выполняет не только преобразование списка цепей, но и экспорт данных из диаграмм qucs для последующей обработки данных моделирования в сторонних программах.

В качестве форматов входных данных могут быть использованы touchstone, citi, qucsdata, spice, zvr, mdl и другие, в качестве форматорв выходных данных - matlab, qucs, csv, qucsdata или qucslib.

Второй способ создания библиотек заключается в создании каждого компонента библиотеки в отдельности с помощью подсхем. В зависимости от сложности этого компонента используют либо эквивалентную схему, состоящую из резисторов, конденсаторов и индуктивностей, либо файловый компонент схема SPICE. В последний загружается отредактированная для Qucs SPICE модель и выбираются необходимые узлы цепей SPICE.

После создания электрической схемы можно перейти к редактированию условного графического обозначения (УГО) компонента.

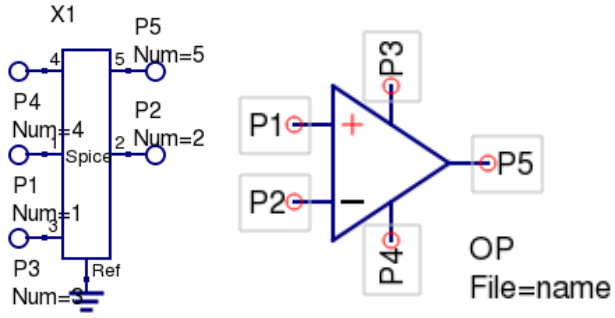


Рис. 1. Схема SPICE для операционного усилителя К140УД6А и его УГО

В одну библиотеку могут входить компоненты собранные с помощью схемы SPICE, а так же с использованием эквивалентных схем. Использование проекта для создание библиотеки имеющей большое число компонентов позволяет хранить схемы компонентов в одном месте и знать какой компонент был создан. Важной особенностью является совпадение имени файла схемы с наименованием создаваемого компонента.

После создания всех элементов библиотеки можно переходить к ее сборке выбрав *Проект -> Создать библиотеку.* Указав имя библиотеки и выбрав ее компоненты, переходим к описанию каждого компонента. После завершения сборки, пользовательские библиотеки станут доступны для использования.

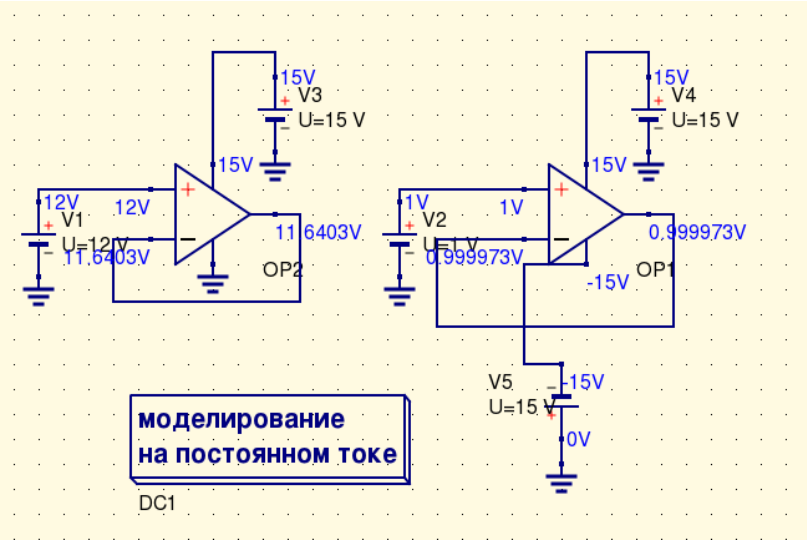


Рис. 2. Моделирование элемента пользовательской библиотеки операционного усилителя К140УД6А на постоянном токе с использованием схем повторителей напряжения при однополярном и двухполярном питании

Возможность создавать пользовательские библиотеки позволяет добавить новые компоненты, в некоторых случаях дает представление о структуре элемента. Разработанные в данной работе библиотеки доступны в репозитории на Github [6]

Литература

[1]. Qucs: Quite Universal Circuit Simulator. http://qucs.sourceforge.net.

[2]. Brinson M. E., Jahn S. Qucs: A GPL software package for circuit simulation, compact device modelling and circuit macromodelling from DC to RF and beyond // International Journal of Numerical Modelling (IJNM): Electronic Net-works, Devices and Fields. — 2008. — September. — Vol. 22, no. 4. — Pp. 297 – 319.

[3]. Кузнецов В.В., Симулятор электронных схем с открытым исходным кодом Qucs: основные возможности и основы моделирования. — Компоненты и технологии.- 2015. - №3. - С.114-120.

[4]. Кузнецов В.В. Моделирование высокочастотных схем в частотной области при помощи САПР Qucs. Компоненты и технологии. 2015. № 8 (169). С. 120-127

[5]. M. Brinson, R. Crozier, V. Kuznetsov, C. Novak, B. Roucaries, F. Schreuder, G. B. Torri. Qucs: improvements and new directions in the GPL compact device modelling and circuit simulation tool., MOS-AK Workshop, Grenoble, March, 2015 http://www.mos-ak.org/grenoble_2015/presentations/T4_Brinson_MOS-AK_Grenoble_2015.pdf

[6]. Qucs extended components library https://github.com/ra3xdh/qucs-rus-complib

Кузнецов Вадим Вадимович - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: ra3xdh@gmail.com

Моисеев Тимофей Сергеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: voig1396@gmail.com

С.А. Лоскутов

СИСТЕМА УПРАВЛЕНИЯ АВТОМАТИЧЕСКИМ КОМПЛЕКСОМ РЕМОНТА КОРРОЗИОННЫХ ДЕФЕКТОВ ТРУБ МАГИСТРАЛЬНЫХ ГАЗОПРОВОДОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В рамках НИОКР, выполняемых Калужским филиалом МГТУ им. Н.Э. Баумана, была поставлена задача разработать систему управления автоматическим комплексом для ремонта коррозионных дефектов труб магистральных газопроводов. Данный комплекс должен обеспечивать ремонт коррозионных дефектов путем фрезерования и последующей наплавки на подготовленный участок. Использование такого комплекса позволит увеличить срок службы труб магистральных газопроводов, имеющих высокую стоимость, что даст существенную экономию средств при их эксплуатации.

В целом комплекс представляет собой станок с ЧПУ портального типа, устанавливаемый на ремонтируемую трубу диаметром 1420 мм или 1200 мм; модуль управления подогревом (установлен на боковой стенке станка); шкаф (стойка) управления, соединенный гибкими кабелями длиной 20 м со станком; сварочный аппарат производства НПП «Технотрон» ДС400.33М [1]; газовый баллон с пропаном 40 л. Станок устанавливается на трубу с предварительно удаленной изоляцией и размеченными дефектами. Максимальный размер обрабатываемого дефекта 900х350х9 мм, максимальное время восстановления дефекта 135 мин.

Структурная схема комплекса приведена на рис.1.

Система управления установкой представляет собой шкаф управления, соединенный с установкой гибкими кабелями. В шкафу управления смонтированы: устройство ЧПУ «Балтсистем» NC-210 [2], пять модулей частотного управления асинхронными двигателями [3], блок релейной низковольтной автоматики, модули питания. Контуры управления двигателями построены по закрытому векторному типу. В качестве датчиков обратной связи используются энкодеры, установленные на валы электродвигателей. Обратные связи замкнуты непосредственно на модули частотного управления двигателями. Такое построение позволяет обеспечить очень высокую точность перемещения и высокий момент. Питание шкафа управления осуществляется от трехфазной сети переменного тока 380 В.

Непосредственно на установке смонтирован блок контроля температуры. Его алгоритм работы следующий: по команде «Начало работы» от ЧПУ производится подогрев поверхности до 70 °С, далее управление передается ЧПУ для выполнения операций фрезерования.

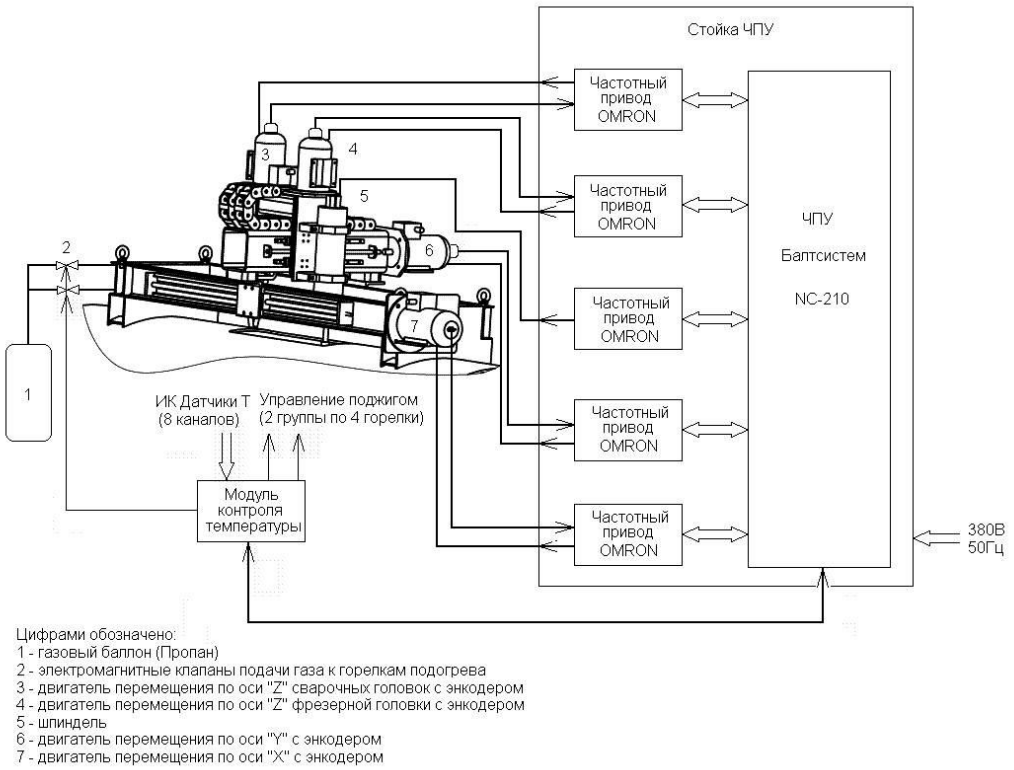


Рис.1. Структурная схема автоматизированного комплекса

После получения от ЧПУ сигнала «Окончание фрезерования», устройство производит нагрев дефектной области до 150 – 180 °С, после чего управление передается ЧПУ для выполнения операции наплавки. Во время наплавки контролируется температура обрабатываемой зоны, при необходимости производится дополнительный подогрев.

Структурная схема блока контроля температуры приведена на рис.2.

Для предварительной сушки и подогрева обрабатываемой поверхности служит функциональный блок контроля температуры. В его состав входят:

— газовый баллон;
— два электромагнитных клапана, каждый на группу из четырех горелок;
— восемь газовоздушных пропановых горелок, объединенные в две группы по четыре;
— свечи электроискрового поджига газовоздушной смеси (по одной на каждую горелку);
— восемь цифровых инфракрасных датчиков температуры (пирометров) [4];
— модуль контроля температуры, представляющий собой микроконтроллерный блок, осуществляющий обмен данными с ЧПУ и управление функциональными узлами блока.

Нагрев дефектной области производится в старт-стопном режиме, т.е. открывается электромагнитный клапан, газовоздушная смесь подается в горелки, формируется электрическая искра, воспламеняющая смесь.

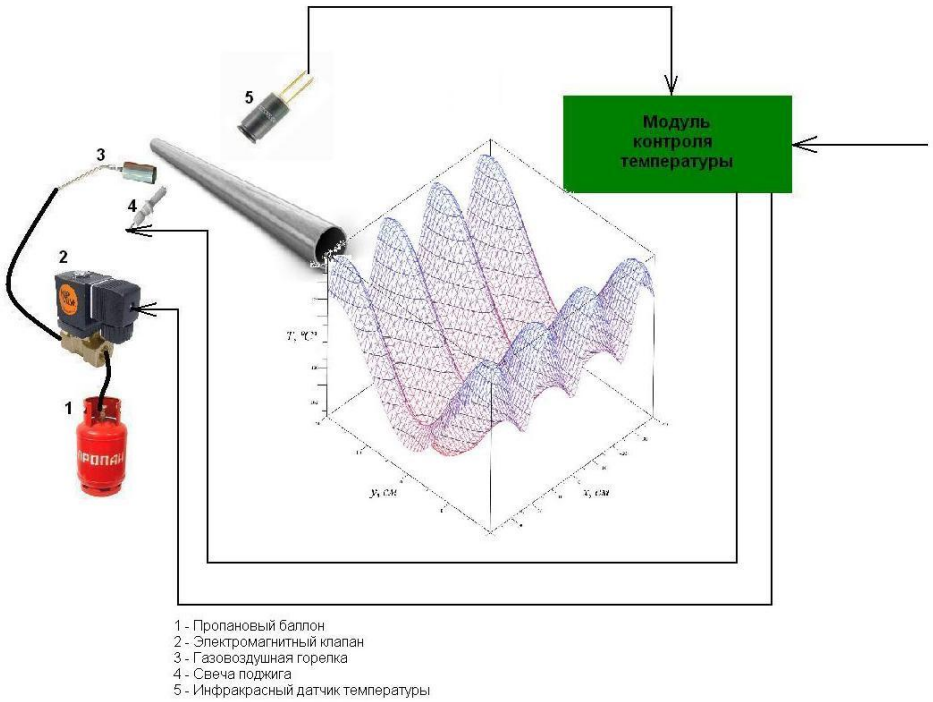


Рис.2. Структурная схема блока контроля температуры

После расчетного времени (определяемого начальной температурой) производится перекрытие газа, измерение температуры и модуль принимает решение о необходимости дальнейшего подогрева. Т.к. нагрев дает неоднородное тепловое поле, то нагрев ведется до температуры, превышающей требуемую, а затем, в процессе остывания, происходит размытие тепловых полей и выравнивание температуры по всей обрабатываемой зоне. В процессе горения производится формирование искры каждые 30 с, что исключает накопление газовоздушной смеси вследствие угасания одной из горелок (например, из-за сильного ветра).

Список литературы

[1]. Сварочный аппарат ДС400.33М производства НПП «Технотрон»: http://xn--e1aqadalkdy.xn--p1ai/product/ds40033m/

[2]. Компактное модульное устройство ЧПУ NC-210: http://www.bsystem.ru/Default.aspx?tabid=82

[3]. Преобразователи частоты/инвертеры общего назначения ф. «Omron»: https://industrial.omron.ru/ru/products/catalogue/motion_and_drives/frequency_inverters/general_purpose/rx/default.html

[4]. ИК-пирометры ф. «Melexis»: http://www.melexis.com/Infrared-Thermometer-Sensors/Infrared-Thermometer-Sensors/MLX90614-615.aspx

Лоскутов Сергей Александрович - канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана.E-mail: SergeL-75@yandex.ru

СЕКЦИЯ 13.

ЗАЩИТА ИНФОРМАЦИИ

Р.Р. Ахтямов, М.К. Савкин

SQL-ИНЪЕКЦИИ И УТИЛИТЫ ДЛЯ ИХ ПОИСКА И ЭКСПЛУАТАЦИИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Многие веб-разработчики не догадываются, что SQL-запросы, которыми они пользуются, могут быть подделаны, и считают, что SQL-запросы всегда достоверны. На самом деле поддельные запросы могут обойти ограничения доступа, стандартную проверку авторизации, а некоторые виды запросов могут дать возможность выполнять команды операционной системы.

Прямое внедрение вредоносных инструкций в SQL-запросы – это методика, в которой взломщик создает или изменяет текущие SQL-запросы для отображения скрытых данных, их изменения или даже выполнения опасных команд операционной системы на сервере базы данных. Атака выполняется на базе приложения, строящего SQL-запросы из пользовательского ввода и статических параметров [1].

Благодаря отсутствию проверки пользовательского ввода и соединению с базой данных под учетной записью суперпользователя (или любого другого пользователя, наделенного соответствующими привилегиями), взломщик может создать еще одного пользователя БД с правами суперпользователя и получить неограниченный доступ к базе данных.

SQL-инъекция – это атака, направленная на веб-приложение, в ходе которой конструируется SQL-выражение из пользовательского ввода путем простой конкантенации (например,$query="SELECT * FROM users WHERE id=".$_REQUEST["id"]). В случае успеха атакующий может изменить логику выполнения SQL-запроса так, как это ему нужно. Чаще всего он выполняет просмотр или редактирование СУБД, а также извлекает таблицы с наиболее «интересными» именами (например «users»). После этого, в зависимости от привилегий, с которыми запущено уязвимое приложение, он может обратиться к защищенным частям веб-приложения (например, прочитать файлы на стороне хоста или выполнить произвольные команды).

Существует несколько основных классов SQL-инъекций:

1. Union SQL-инъекция. Использование данной техники основано на применении оператора UNION, который позволяет объединить результаты выполнения двух или более запросов SELECT. Для корректности результирующего запроса, полученного при помощи оператора UNION, необходимо, чтобы у двух выражений SELECT совпадало количество и тип колонок результата. В противном случае СУБД сгенерирует исключение. В зависимости от логики работы приложения либо будет выведено сообщение о возникшем при работе с СУБД исключением, либо страница отобразится пользователю некорректно.

2. Error-based SQL-инъекция. Данная техника используется, когда приложение некорректно обрабатывает исключения, возникающие при

работе с СУБД, и сообщение о возникшем исключении отображается пользователю. В СУБД Oracle есть уязвимые функции, которые отображают в сообщении о возникшем исключении часть входных параметров. Используя данные функции, злоумышленник может построчно считывать информацию из таблицы БД [2].

3. Blind SQL-инъекция. Не всегда можно использовать Union и Error-based SQL-инъекцию: результат выполнения запроса может не отображаться пользователю либо приложение может корректно обрабатывать исключения. В этом случае составляется SQL-выражение, которое при истинном значении не нарушает логику работы приложения. При ложном же значении возникает аномальное поведение в работе web-приложения: страницы неправильно отображаются либо возвращается только часть данных.

Рассмотрим некоторые популярные утилиты для поиска и эксплуатации SQL-инъекций:

1. SQLmap

Рис. 1. Интерфейс программы SQLmap

Одна из мощных открытых утилит, которая автоматизирует процесс поиска и эксплуатации SQL-инъекций с целью извлечения данных или захвата удаленного хоста. sqlmap отличается от других утилит для обнаружения SQL-инъекций тем, что позвляет эксплуатировать каждую найденную уязвимость. Это означает, что sqlmap способен не только находить уязвимость, но также и использовать её множеством различных способов. В качестве задачи ставится именно эксплуатация уязвимости, сканеру приходится быть особенно внимательным к деталям: он не будет выдавать миллион ложных срабатываний «на всякий случай» (как это мы видим во многих других приложениях). Любая потенциальная уязвимость дополнительно проверяется на возможность эксплуатации. Сканер обладает довольно широкой функциональностью, начиная от возможности определения системы управления базой данных (далее DBMS), создания дампа (копии) данных и заканчивая получением доступа к системе с возможностью обращаться к произвольным файлам на хосте и выполнять на сервере произвольные команды. И главное – это обнаружение возможности сделать инъекцию SQL-кода.

Ядро для определения SQL-уязвимостей – самая важная, но не единственная часть функционала sqlmap. Bsqlmap реализовано:

— Извлечение имен пользователей, хешей их паролей, а также привилегий и полей.
— Автоматическое распознавание типа используемого хеша и возможность взлома его с помощью брутфорса по словарю.
— Получение списка баз данных, таблиц и столбцов.
— Возможность сделать полный или частичный дамп базы данных.
— Продвинутый механизм поиска баз, таблиц или даже столбцов (по всем базам сразу), что может быть полезно для определения таблиц с «интересными» данными вроде имен пользователей (users) или паролей (pass).
— Загрузка или, наоборот, закачка произвольных файлов на сервер, если уязвимое веб-приложение использует MySQL, PostreSQL или Microsoft SQL Server.

2. Havij

Havij представляет собой автоматизированное средство для использования SQL-инъекций, которое помогает тестеровщикамнайти и использовать уязвимость SQLInjection на веб-странице.

С его помощью можно воспользоваться уязвимостями веб-приложения. С помощью Havij пользователь может выполнять слепок базы данных, извлекать пользователей СУБД и хэши паролей, таблицы и столбцы дампа, выборки данных из базы данных, запускать запросы SQL и даже обращаться к основной файловой системе и выполнять команды операционной системы.

Основным достоинством Havij, которое делает его отличным от аналогичных инструментов, являются его методы инъекций. Более чем 95% инъекций, проведенных с помощью Havij, являются успешными.

3. Acunetix Web VulnerabilityScanner

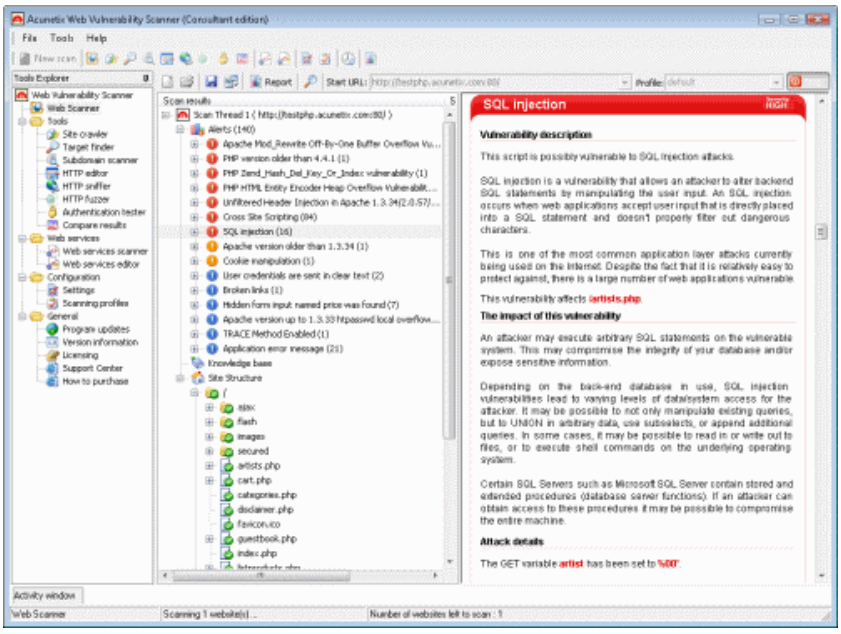


Рис. 2. ИнтерфейспрограммыAcunetixWebVulnerabilityScanner

Acunetix Web VulnerabilityScanner автоматизирует задачу контроля безопасности Web-приложений и позволяет выявить уязвимые места в защите web-сайта до того, как их обнаружит и использует злоумышленник. Данный инструмент работает следующим образом:

— Acunetix WVS исследует и формирует структуру сайта, обрабатывая все найденные ссылки и собирая информацию обо всех обнаруженных файлах;
— Затем программа тестирует все web-страницы с элементами для ввода данных, моделируя ввод данных с использованием всех возможных комбинаций и анализируя полученные результаты;
— Обнаружив уязвимость, Acunetix WVS выдает соответствующее предупреждение, которое содержит описание уязвимости и рекомендации по ее устранению;
— Итоговый отчет WVS может быть записан в файл для дальнейшего анализа и сравнения с результатами предыдущих проверок.
— Могут быть обнаружены следующие уязвимости:
— crosssitescripting (выполнение вредоносного сценария в браузере пользователя при обращении и в контексте безопасности доверенного сайта);
— SQL injection (выполнение SQL-запросов из браузера для получения несанкционированного доступа к данным);
— обращение к базе данных GHDB (Googlehackingdatabase);
— выполнение кода;
— обход каталога;
— вставка файлов (Fileinclusion);
— раскрытие исходного текста сценария.

Работая с базами данных, очень важно понимать, что представляют из себя SQL-инъекции, и как предотвратить их использование злоумышленником; или даже обернуть их себе на пользу и научиться работать с ними.

Литература

[1]. Поляков А. М. Безопасность глазами аудитора: нападение и защита. // М.: ДМК Пресс, 2013.

[2]. Евтеев Д. Учимся на ошибках. Error-basedSQL-Injection // Хакер. 2014, № 135.

[3]. Марков А. С., Миронов С. В., Цирлов В. Л. Выявление уязвимостей в программном коде // Открытые системы. 2013, № 12.

[4]. Фленов М.Е. SQL-инъекции глазами хакера. 2 изд. // БХВ-Петербург, 2011. - 336 с.

Ахтямов Ренат Рашидович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: doktorwww@gmail.com

Савкин Михаил Константинович – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

Д.А. Мельников, И.В. Садиков, А.Н. Молчанов

АНАЛИЗ ФУНКЦИИ ПРОЗРАЧНОГО ШИФРОВАНИЯ ДАННЫХ (TRANSPARENT DATA ENCRYPTION) В MICROSOFT SQL SERVER 2008

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Шифрование - это способ сокрытия информации от злоумышленника, использующий в качестве одного из инструментов ключ. В результате информация теряет свою ценность для злоумышленника, если у того отсутствуют инструменты, необходимые для расшифровки. Таким образом, даже если неавторизованное лицо сумеет получить доступ к базе данных, содержащей в себе защищенную информацию, воспользоваться ею оно не сможет[1].

Целью данной работы является анализ функции прозрачного шифрования данных (TransparentDataEncryption),применяемой для криптографической защиты баз данных вMicrosoft SQL Server 2008.

Описание функции прозрачного шифрования данных. Прозрачное шифрование баз данных (TransparentDataEncryption) реализовано в Microsoft SQL Server 2008 (и более поздних версиях). Базы данных кодируются целиком с помощью функции прозрачного шифрования. Страница данных зашифровывается, в момент, когда происходит запись информации из оперативной памяти компьютера на жёсткий диск. Процесс расшифровывания происходит, когда страница выгружается обратно с жёсткого диска в оперативную память. В результате на жёстком диске база данных становится зашифрованной, тогда как в оперативной памяти она остаётся незашифрованной. Главным преимуществом TDE является то, что шифрование и дешифрование выполняются абсолютно прозрачно для приложений[2].

Как правило, процесс шифрования данных является достаточно простым. Для того чтобы зашифровать данные необходимо использовать один из существующих алгоритмов шифрования. Алгоритмы шифрования хорошо известны, тем более что большинство из них реализованы в операционной системе (такие как AES и 3DES). Намного сложнее придумать защиту для ключа, при помощи которого эти данные были зашифрованы. Ведь если «положить» этот ключ рядом с зашифрованными данными, то о надёжной защите данных не может идти и речи. Решить данную задачу помогает специальная иерархия ключей.

В TransparentDataEncryption (TDE) построение иерархии ключей начинается с того, что для каждой базы данных, которая шифруется с помощью TDE, будет создан специальный ключ, называющийся DatabaseEncryptionKey (DEK). Ключ DEK будет использоваться для непосредственного шифрования данных. Затем этот ключ шифруется

сертификатом, который создаётся в базе данных Master. Этот сертификат шифруется главным ключом базы данных Master. После этого главный ключ базы данных Master шифруется главным ключом службы (ServiceMasterKey или SMK). И, наконец, главный ключ службы (SMK) шифруется с помощью DPAPI. Преимущество такой схемы очевидно: она позволяет SQL Serverполучить доступ как к ключу, так и к зашифрованным данным в любой момент времени.При этом никто другой доступа к этим данным не имеет[3].

Однако,при использовании функции прозрачного шифрования данных (TDE) необходимо учитывать следующие особенности: создание резервных копий сертификата и ключа должно осуществляться сразу после включения функции шифрования(TDE);сертификат шифрования должен быть сохранён даже в случае отключения TDE; должны быть созданы учётные данные для доступа к базе, а также должна быть создана резервная копия ассиметричного ключа.

Возможности функции прозрачного шифрования данных. В случае получения злоумышленником доступа к защищаемым данным через SQL Server, TransparentDataEncryption (TDE) оказывается абсолютно бесполезным, поскольку в оперативной памяти данные остаются незашифрованными. TransparentDataEncryption (TDE) так же не способно защитить данные от администраторов, поскольку администратор SQL Server может просто отключить шифрование, и вся защита сойдёт на нет.

Что действительно может сделать TransparentDataEncryption (TDE), так это защитить файлы баз данных и резервные копии на случай их похищения. Если снять копию с файлов активной БД – задача непростая, то похищение резервной копии при наличии к ним доступа не представляет никаких проблем. Однако и здесь есть свои ограничения. Файлы базы данных и соответствующие резервные копии будут надежно защищены, только если злоумышленнику не удастся вместе с данными заполучить и ключ. Разумеется, если злоумышленник получит ключ, то он без проблем расшифрует секретные данные. Самым слабым звеном в этой системе является главный ключ службы (SMK), который находится на вершине иерархии ключей и защищается с помощью DPAPI[3].

В том случае, когда для базы данных включено TransparentDataEncryption (TDE), шифруются как ее файлы данных, так и ее журнал транзакций. Кроме того, как только на экземпляре SQL Server включается шифрование хотя бы одной базы данных, остальные базы данных также начинают шифроваться. Предположим, что среди этих баз находится некоторая база данных под названием tempdb. Почему была зашифрована база данных tempdb, понятно, – она может содержать куски секретной информации из шифруемых баз. А вот почему должны шифроваться приложения, работающие с другими, не зашифрованными базами данных? Ведь в результате шифрования их запросы, выполнение которых требует

участия базы данных tempdb (большие сортировки, например), очевидно, станут выполняться медленнее. А дело, видимо, в том, что не всегда возможно однозначно определить источник данных, попадающих в tempdb. Поэтому для гарантии безопасности она шифруется целиком.

Во время включения TransparentDataEncryption (TDE) SQL Server, как уже упоминалось выше, в отдельном потоке выполняет шифрование всех файлов данных этой базы данных. Однако есть области, которые даже после завершения процесса остаются незашифрованными. К этим областям относятся:FileHeaderPage (первая страница файла данных), BootPage (страница для хранения DEK), заголовки страниц[4].

В отличие от файлов данных, для журналов транзакций операция первоначальной шифровки выполняться не будет. Это означает, что информация о транзакциях, находящаяся в журналах транзакций на момент включения шифрования, по-прежнему остается незащищенной. Шифроваться будет только информация о новых транзакциях. Как следствие, если есть полная резервная копия базы данных до того как она была зашифрована, то даже после включения шифрования, можно сделать резервную копию журнала транзакций уже зашифрованной базы данных, а затем восстановить ее на момент, предшествующий шифрованию, и, соответственно, получить доступ к секретным данным. Для восстановления такого архива наличие ключа необязательно (например, это можно сделать на другом сервере)[5].

Какой вывод можно из этого сделать? Если мы шифруем базу данных, которая на момент шифрования уже содержит секретную информацию, то необходимо либо пересоздать журнал транзакций, либо сделать так, чтобы незашифрованные транзакции в журнале транзакций были заменены новыми зашифрованными транзакциями.

Достоинства и недостатки TDE. К положительным особенностям TransparentDataEncryption (TDE) можно отнести следующие:

— TDE позволяет защитить базу данных прозрачно, не внося изменений в интерфейсные приложения.
— За счет использования правильных индексов не требуется дополнительное пространство дляхранение данных.
— К отрицательным особенностям TransparentDataEncryption (TDE) относятся следующие:
— Загрузка процессора и памяти.
— Ресурсоемкое шифрование базы данных tempdb.
— Для эффективной работы TDEтребуются дополнительные накладные расходы системных ресурсов.
— Затрудняется оптимизация запросов[6].

Выводы. Основной вывод, который следует сделать, заключается в том, что использование прозрачного шифрования баз данных в приложениях может повлиять как на работу самой базы данных, так и на

производительность системы в целом, поэтому использование прозрачного шифрования нужно планировать заранее. После включения TDE нагрузка на сервер увеличится, поэтому необходимо убедиться в том, что свободных ресурсов (в первую очередь речь идет о CPU) сервера хватит, чтобы справится с возросшими потребностями после включения TDE. В этом случае если уменьшение производительности произойдёт, то оно будет незначительным.

Библиографический список

[1]. Айтхожаева Е.Ж. CryptoAPI и шифрование БД // *Международная научная конференция: Высокие технологии – залог устойчивого развития.* – Алматы, 2011.- С. 275-278.

[2]. Нанда Арап. Прозрачное шифрование данных. - М.: *OracleMagazine /*Русское издание. - 2005.- Сентябрь-Октябрь.

[3]. Ян Либерман. Прозрачное шифрование баз данных в Microsoft SQL Server 2008 - *RSDNMagazine #2-2008*.

[4]. *Прозрачное шифрование данных (TDE).*URL: https://msdn.microsoft.com/ru-ru/library/bb934049(v=sql.120).aspx(дата обращения 25.09.2015).

[5]. John Magnabosco. *Transparent Data Encryption*. URL: https://www.simple-talk.com/sql/database-administration/transparent-data-encryption/(дата обращения 12.10.15).

[6]. *Шифрование данных средствами MicrosoftSQL Server*.URL: http://efsol.ru/articles/encryption-means-microsoft-sql-server.html(дата обращения 17.10.15).

Мельников Дмитрий Алексеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: dmitriymelnikov1407@gmail.com

Садиков Игорь Владимирович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: sadikov-igor@list.ru

Молчанов Алексей Николаевич – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

А.С. Макаров, А.Б. Лачихина, С.А. Кирдяшкин

АППАРАТНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ С ПОМОЩЬЮ РЕКОНФИГУРИРУЕМЫХ ВЫЧИСЛИТЕЛЬНЫХ СТРУКТУР

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Развитие современных программируемых логических интегральных схем (ПЛИС) класса FPGA (Field-ProgrammableGateArray) открывают новые возможности в аппаратной реализации широкого класса вычислительно трудоемких задач [1]. К решению задач подобного рода всегда можно отнести разработку программно-аппаратных методов и средств, направленных, в свою очередь, на повышение информационной безопасности автоматизированных систем (АС) самого различного назначения, без которых на сегодняшний день не обходится ни одна сфера жизнедеятельности человека. При этом данная задача на практике в большинстве случаев реализуется чисто программными средствами [2], аппаратная часть которых представляет собой унифицированные микропроцессорные системы.

В работах [3, 4, 5] были рассмотрены способы организации контрольно-диагностического обеспечения бортовых систем управления современных космических аппаратов (КА) с помощью реконфигурируемых вычислительных структур (РВС), построенных на основе ПЛИС класса FPGA.

Целью данной работы является разработка алгоритмов повышения информационной безопасности в АС посредством РВС.

Решение задач повышения информационной безопасности в АС посредством РВС. Самые распространенные типы РВС строятся на базе ПЛИС, которые, в свою очередь, являются сложной высокоинтегрированной микросхемой, способной многократно менять свою внутреннюю конфигурацию в зависимости от управляющей программы. Используемые в РВС ПЛИС, как правило, представляют собой матричной структуры, элементами которой являются коммутируемые логические блоки (КЛБ) (Рис. 1). Матричная организация КЛБ обеспечивает возможность последовательно-параллельного распределения вычислений в виде графа, структура которого соответствует информационной иерархии решаемой задачи. Возможность топологической адаптации архитектуры РВС к информационной структуре вычислительной задачи наделяет свойством «гибкости» алгоритмы информационной безопасности [1], что предлагается использовать в информационном обеспечении АС при необходимости глубокого перестроения алгоритмов аутентификации, идентификации и многих других.

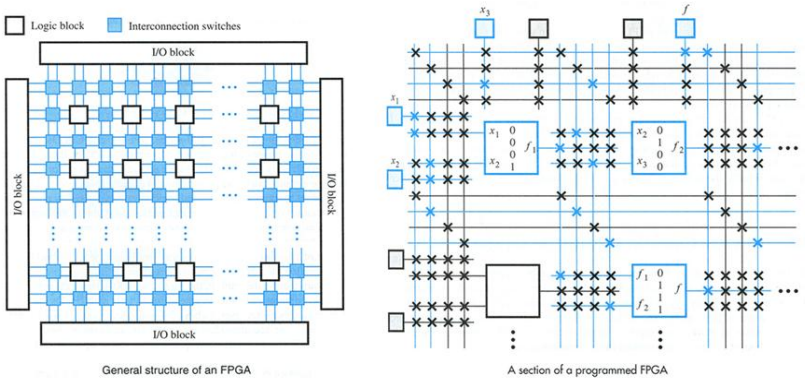


Рис. 1. Архитектура ПЛИС класса FPGA

Таким образом, РВС предоставляют возможность аппаратной реализации алгоритмов повышения информационной безопасности АС с динамически корректируемой архитектурой. При этом сами возможности динамической реконфигурации будут полностью определяться характеристиками выбранной для построения РВС ПЛИС.

Описание аппаратных архитектур РВС, реализующих алгоритмы информационной безопасности в различных типах АС. Любую архитектуру РВС, реализующую алгоритм информационной безопасности АС можно описать в пределах матрицы $\mathbf{L}_d^{\text{РВС}}$, где $d = \overline{1,k}$ – условный порядковый номер матричного набора КЛБ в РВС. Аппаратную архитектуру любого из функциональных фрагментов РВС можно представить в виде следующей зависимости

$$K_h^{\text{РВС}} = F(\mathbf{L}_h, G(\mathbf{L}_h)) \tag{1}$$

где $\mathbf{L}_h$ – матричный набор КЛБ, реализующий *h*-й функциональный модуль информационной безопасности АС, который, в свою очередь, можно записать как

$$\mathbf{L}_h = \mathbf{L}^{(q)} = \mathbf{L}^{(1)} = \begin{Vmatrix} \gamma_{11}L_{11}^{(1)} & \gamma_{12}L_{12}^{(1)} & \cdots & \gamma_{1k}L_{1k}^{(1)} \\ \gamma_{21}L_{21}^{(1)} & \gamma_{22}L_{22}^{(1)} & \cdots & \gamma_{2k}L_{2k}^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{m1}L_{m1}^{(1)} & \gamma_{m2}L_{m2}^{(1)} & \cdots & \gamma_{mk}L_{mk}^{(1)} \end{Vmatrix}, \tag{2}$$

где *q* – условный аппаратный уровень модуля информационной безопасности АС (в данном случае *q* = 1), $L_{ij}^{(1)}$ – логико-арифметическая функция, реализуемая посредством КЛБ, расположенного в *i*-ой строке и *j*-ом столбце матрицы $\mathbf{L}_h$ ($i = \overline{1,m}$, $j = \overline{1,k}$), γ_{ij} – функция включения (задействования) КЛБ в вычислительной операции и описываемая выражением

$$\gamma_{ij} = \begin{cases} 1, \textit{если } КЛБ\, L_{ij}^{(1)} \textit{ включен } (\textit{задействован}), \\ 0, \textit{если } КЛБ\, L_{ij}^{(1)} \textit{ выключен } (\textit{незадействован}). \end{cases}, \tag{3}$$

Орграф $G(\mathbf{L}_h)$ описывает топологию логико-арифметических связей между КЛБ-вершинами в матрице $\mathbf{L}_h$, задавая тем самым строгую аппаратную конфигурацию (архитектуру), реализующую рассматриваемый алгоритм информационной безопасности АС.

Выводы. В настоящее время исследуются способы аппаратной реализации алгоритмов информационной безопасности в АС на базе РВС, которые в отличии от классических программных методов позволяют:

— обеспечить высокую гибкость алгоритмов информационной безопасности АС на низком аппаратном уровне путем адаптации РВС к иерархической структуре широкого спектра задач информационной безопасности;

— снабдить АС возможностью пополнения новыми алгоритмами информационной безопасности в пределах предварительно рассчитанного вычислительного ресурса РВС.

Проводится анализ доступной номенклатуры ПЛИС класса FPGA, способной максимально эффективно реализовать большой набор алгоритмов информационной безопасности АС различного назначения.

Библиографический список

[1]. Каляев И.А., Левин И.И., Семерников Е.А., Шмойлов В.И. Реконфигурируемые мультиконвейерные вычислительные структуры /Изд. 2-е, перераб. и доп. / Под общ. Ред. И.А. Каляева.Ростов-на-Дону, Изд-во ЮНЦ РАН, 2009, 344 с.

[2]. Варфоломеев А.А. Основы информационной безопасности: Учеб. Пособие. Москва, РУДН, 2008, 412 с.

[3]. Savkin L.V., Makarov A.S. About diagnostic support of onboard equipment of aircraft on the basis of reconfigurable computing systems.Global Science and Innovation: materials of the III International Scientific Conference, Chicago, October 23-24th, 2014 / publishing office Accent Graphics communications – Chicago – USA, 2014, pp. 357-361.

[4]. Ширшаков А.Е., Новичков В.М., Савкин Л.В., Макаров А.С. Расширение функциональных возможностей системы контроля и диагностики бортового комплекса управления космического аппарата за счет встроенных реконфигурируемых вычислительных структур. Вестник НПО им. С.А. Лавочкина, 2015, №2, с. 45-51.

[5]. Савкин Л.В., Клочко О.С., Макаров А.С. О возможности восстановления вышедших из строя дискретных элементов бортовых систем управления космических аппаратов, контролируемых с помощью внешних реконфигурируемых вычислительных структур. Технические науки — от теории к практике / Сб. ст. по материалам XL междунар. науч.-практ. конф. № 11 (36), Новосибирск: Изд-во «СибАК», 2014, с. 96-103.

Макаров Антон Сергеевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: makarov.bas@gmail.com

Лачихина Анастасия Борисовна – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

Кирдяшкин Сергей Анатольевич - преподаватель КФ МГТУ им. Н.Э. Баумана. E-mail: rbhlzirby@mail.ru

Е.Е. Хмельницкая, А.Б. Лачихина

БЛОКИРОВКА ПОСТОРОННЕГО ДОСТУПА К ДАННЫМ В ПРОЦЕССЕ ИХ ОБРАБОТКИ КАК ОДИН ИЗ СПОСОБОВ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ В СУБД MS SQL SERVER

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Под целостностью данных понимается взаимная корректность и согласованность отдельных фрагментов данных. Согласованность, в свою очередь, - это единообразное моделирование всего количества запросов и данных в базе данных и их включение в систему.

Как известно, СУБД, имеющие клиент-серверную архитектуру, работают в многопользовательском режиме. Пользователи запускают транзакции, и часто происходит, что несколько транзакций обращается к одним и тем же данным одновременно. При этом возможны конфликтные ситуации, результатом которых является появление в информационной системе ложных данных или даже частичная потеря данных, что может привести к существенному урону организации, в которой зарегистрирована информационная система. Общеизвестными являются следующие типы конфликтов:

1. Последнее изменение.

Первая транзакция произвела запись в таблицу. Не дожидаясь ее завершения, другая транзакция перезаписала те же самые данные, поставив другие значения. В результате верные значения в таблицах могут быть потеряны, а неверные значения приняты и являются в дальнейшем источниками вычислительных ошибок или вывода некорректных данных.

2. Чтение после записи («грязное» чтение)

В то время как одна транзакция выполняет модификацию данных, другая считает их же, не дожидаясь завершения первой транзакции, и использует их для своих вычислений. Во многих случаях нежелательно, чтобы транзакции «видели» неокончательные изменения, которые еще не зафиксированы в таблицах как результаты, так как «грязное» чтение может привести к получению ошибочной информации.

3. Запись после чтения

Первая транзакция считывает данные, а вторая, не дожидаясь завершения первой, модифицирует их. Получается, что первая транзакция выполняет вычисления, используя устаревшие исходные данные, что может привести к нарушению целостности информации, поскольку результат выполненных вычислений не будет соответствовать новому состоянию исходных данных.

Зарубежными специалистами выделено два отдельных случая данного конфликта. Первым случаем является проблема неповторяемого чтения. Этот случай возникает из-за многократного чтения данных одной и той же транзакцией. Между двумя считываниями другая транзакция может выполнить модификацию, и после повторного чтения первая транзакция получите измененные данные. Второй случай – «чтение фантомов» - возникает, когда транзакция несколько раз производит выборку строк, удовлетворяющий одному и тому же логическому условию. Если между считываниями другая транзакция вставит строки, удовлетворяющие этому же условию, первая транзакция при следующем считывании получит неверный набор данных.

Одним из способов обеспечения целостности данных, принятым в системах управления базами данных, является блокировка постороннего доступа к данным в процессе их обработки.

Механизм блокировок позволяет избежать перечисленных выше проблем. В основу принципов блокирования данных в СУБД Microsoft SQL Server положена концепция Американского национального института стандартов (ANSI), в которой выделено четыре уровня блокирования.

Уровень 0 – запрещение «загрязнения» данных.

На этом уровне запрещается одновременное изменение данных несколькими транзакциями: если транзакция начинает изменение данных, другие транзакции не могут модифицировать их до разблокирования, но считывание этих данных другими транзакциями разрешается.

Уровень 1 – запрещение «грязного» чтения.

На этом уровне при модификации данных транзакцией устанавливается блокировка, запрещающая сторонним транзакциям не только модифицировать, но и считывать эти данные до завершения первой транзакции.

Уровень 2 – запрещение неповторяемого чтения.

Если транзакция считывает данные, СУБД блокирует их так, что другие транзакции не могут изменять их до разблокирования.

Уровень 3 – Запрещение фантомов.

Если транзакция производит выборку по логическому условию, никакая другая транзакция до завершения первой транзакции не должна вставлять и удалять строки, этому условию удовлетворяющие.

Блокировки могут устанавливаться как на таблицу целиком, так и на строку в таблице. Блокировки чаще всего выставляются операторами UPDATE, INSERT. Существуют явные операторы задания блокировок, например, LOCK TABLE или SELECT: FOR UPDATE. Соответственно есть операторы и для снятия блокировок.

У многих SQL-серверов есть особые способы обнаружения и предотвращения взаимных блокировок. Они называются deadlocks. На практике их минусом является то, что они могут занимать ресурсы СУБД на неопределенное время, что может привести к временному замедлению или даже остановке работы СУБД.

СУБД SQL Server 2008 поддерживает все перечисленные уровни блокировки. Наложением и снятием блокировок управляет специальная подсистема в составе SQL Server – менеджер блокировок (Lock Manager). Процесс управления блокировками в значительной степени автоматизирован: менеджер блокировок сам выбирает нужный уровень блокирования, стараясь применять как можно менее жесткий режим.

Литература

[1]. *Архитектура современного SQL-сервера. Технология Клиент-Сервер* [Электронный ресурс] – М.: Изд-во АО Аудит-Оптим, 2011. URL: http://www.optim.ru/cs/2/Sql7Architecture (дата обращения 22.10.2015)

[2]. Мамаев Е.В. *Microsoft SQL Server 2008.* – Спб.: Изд-во БХВ-Петербург, 2004, 904 с.

[3]. Алекс Кригель, Борис Трухнов. *SQL. Библия пользователя. 2-е издание*: Изд-во Вильямс, 2010, 989 с.

[4]. Лачихина А.Б., Хмельницкая Е.Е. Поддержание целостности информации в базах данных на примере СУБД SQL Server. *Вопросы радиоэлектроники.* 2015, № 8 (8), С. 109-113.

Хмельницкая Екатерина Евгеньевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: ekaterina.hmel@yandex.ru

Лачихина Анастасия Борисовна – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

Ю.С. Ивченкова, М.К. Савкин

ИНСТРУМЕНТЫ ДЛЯ ПОИСКА И ЭКСПЛУАТАЦИИ XSS-УЯЗВИМОСТЕЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время веб-приложения получили широкое распространение, так как они обладают такими достоинствами как простота интерфейса, возможность удаленной работы через Интернет, предоставление доступа к единой информации одновременно большому числу пользователей и независимость от операционной системы, установленной на компьютере пользователя. Но вместе с этим веб-приложения создают большое число проблем, связанных с обеспечением информационной безопасности, так как приложение становится доступным через Интернет и для пользователей, и для злоумышленников. Уязвимости веб-приложений позволяют злоумышленникам похищать конфиденциальную информацию, изменять данные и нарушать доступность приложения.

Одной из самых распространенных атак на веб-приложения является межсайтовый скриптинг (третье место в рейтинге ключевых рисков веб-приложений согласно OWASP 2013). К данной атаке уязвимо примерно 70% веб-приложений [1]. В связи с этим актуальным вопросом является обнаружение XSS-уязвимостей.

Межсайтовый скриптинг (Cross-Site Scripting) или XSS – атака на веб-приложения, заключающаяся во внедрении вредоносного кода в веб-страницу и взаимодействии этого кода с веб-сервером злоумышленника, при этом вредоносный код будет выполнен на компьютере пользователя при открытии им этой страницы [2]. Суть атаки заключается в следующем: через необрабатываемые входные параметры передается некий код, который впоследствии встраивается в страницу и выполняется каждый раз при загрузке страницы или выполнении определенного действия. Когда пользователь заходит на зараженную страницу, в его браузере выполняется вредоносный код, который может читать, изменять или передавать любые данные, к которым есть доступ у браузера: cookies, идентификаторы сессий (session tokens) и т.д.

Наиболее популярными инструментами для нахождения и эксплуатации XSS-уязвимостей являются BeEF, OWASP Xenotix XSS Exploit Framework и XSSF.

OWASP Xenotix XSS Exploit Framework. Эта утилита включает в себя 3 браузерных движка: Trident, WebKit и Gecko, которые являются основой браузеров Internet Explorer, Google Chrome и Mozilla Firefox соответственно (рис. 1). Поскольку некоторые виды атак применимы только для отдельного движка, тестирование производится одновременно для всех представленных браузеров.

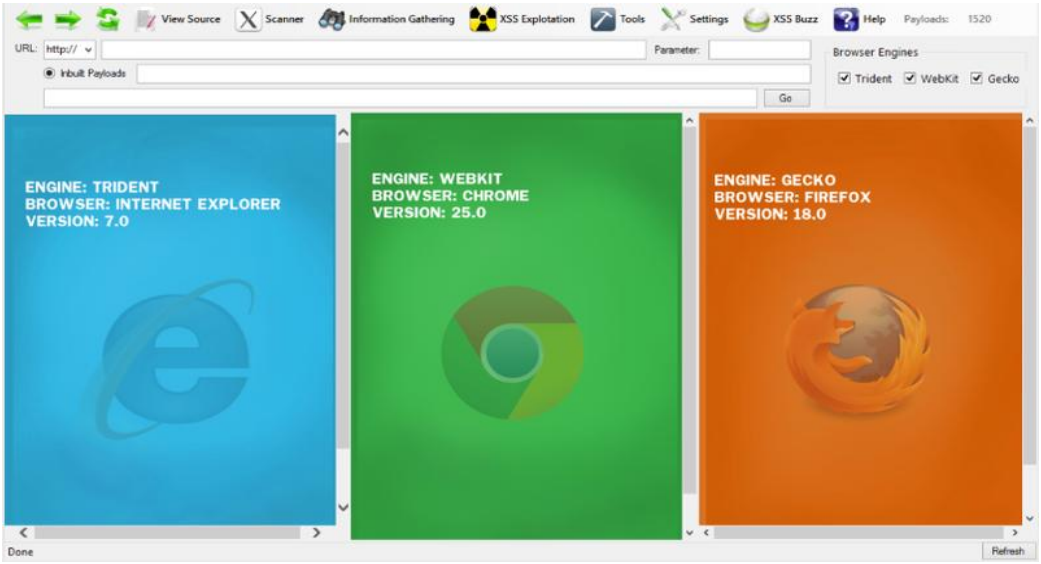


Рис. 1. Основной интерфейс OWASP Xenotix XSS Exploit Framework

Для использования программы необходимо запустить сервер. Для этого необходимо указать IP-адрес и порт. Сервер будет доступен по этому адресу до тех пор, пока вы окно с настройками не будет закрыто. Процесс работы с программой разбит на 3 части:

— процесс сканирования (Scanner);
— процесс сбора информации (Information Gathering);
— процесс эксплуатации найденных уязвимостей (XSS Explotation).

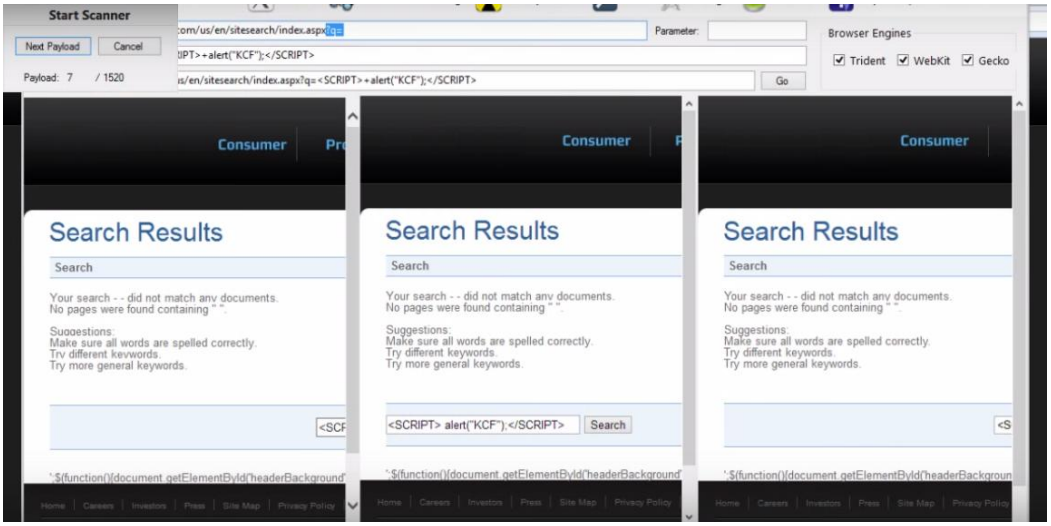


Рис. 2. Процесс сканирования

В базе Xenotix есть более 1500 полезных нагрузок [3], включая нагрузки, которые могут обойти основные XSS-фильтры, используемые для защиты веб-разработчиками. Полезные нагрузки могут быть использованы как в ручном, так и в автоматическом режиме. Например, есть возможность собирать данные, вводимые пользователем на инфицированной странице, или загружать вредоносные исполняемые файлы на компьютер жертвы без ее ведома.

BeEF. BeEF (Browser Exploitation Framework) – это утилита для выполнения различных атак, эксплуатирующих XSS-уязвимости (сбора информации о браузере, сбора информации о сети, сканирования портов и т.д.) и злоупотребления незащищенностью браузера жертвы в целом. В BeEF реализованы последние методы атак, которые используют специалисты в области тестов на проникновение с богатым практическим опытом атак на клиентские приложения.

Данный инструмент имеет модульную структуру, есть возможность разработки пользовательских модулей. Текущие модули включают Metasploit (инструмент для тестирования на проникновение), сканирование портов, кейлоггер, и многое другое.

Поскольку каждый браузер индивидуален (различаются тип и версия браузера, установленные плагины), BeEF позволяет выбирать конкретные модули для атаки на каждый браузер, поддерживает возможность одновременной работы с несколькими веб-браузерами, чтобы контролировать изменения на веб-сайте.

Вредоносный URL может быть сформирован с использованием значения Hook URL (рис. 3) и адреса уязвимого сайта: http://www.vulnerablesite.com/search.asp?keyword=<script type=text/javascript src = http://192.168.56.1:3000/hook.js></script>&x=0&y=0

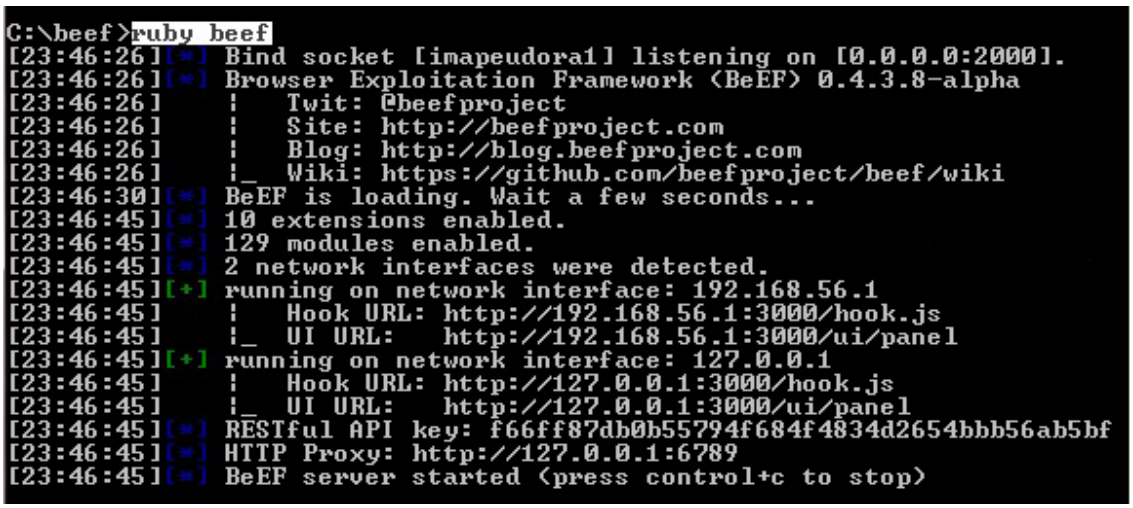


Рис. 3. Значение Hook URL

Информация о жертвах может быть просмотрена с помощью веб-интерфейса приложения. Он доступен по адресу http://your_ip_or_hostname:3000/ui/panel, где необходимо ввести логин и пароль [4]. Логин и пароль по умолчанию – beef, но они могут быть изменены.

После того, как жертва перейдет по сформированному URL, ее IP-адрес появится в списке, появится возможность просмотреть информацию о браузере (рис. 4) и будут указаны действия, которые могут быть произведены над жертвой (рис. 5).

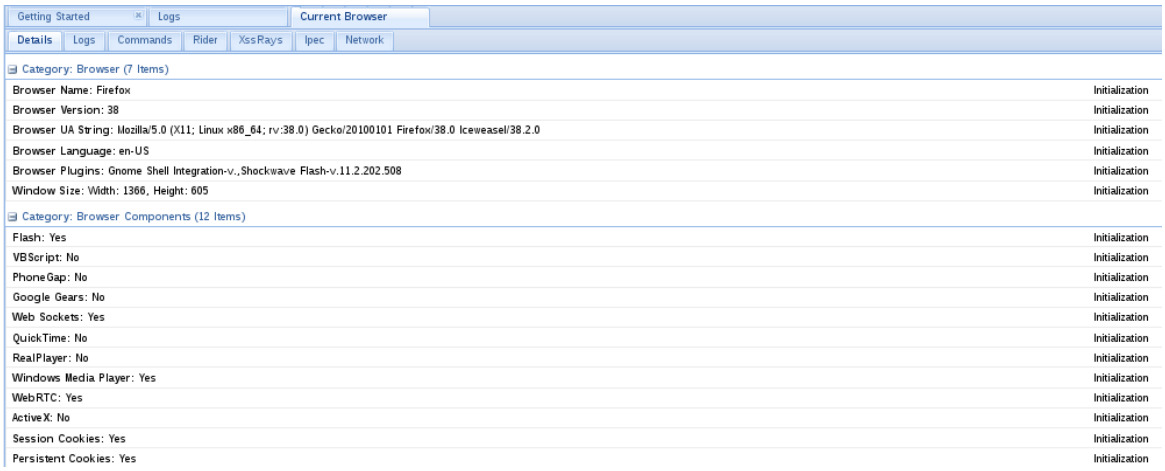


Рис. 4. Данные о браузере жертвы

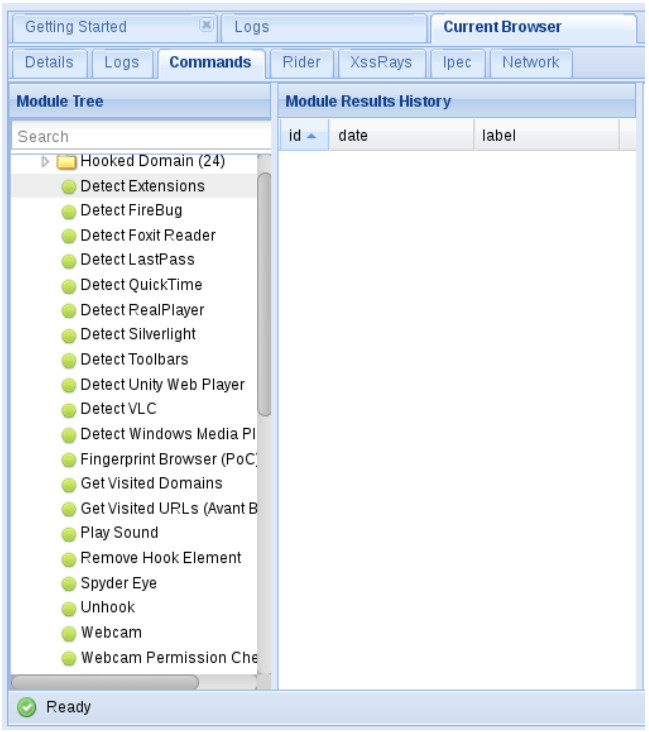


Рис. 5. Список возможных действий

XSSF. XSSF (The Cross-Site Scripting Framework) – инструмент для эксплуатации XSS-уязвимостей. Основная функция заключается в создании коммуникационного канала (XSSF-туннеля) с браузером жертвы для выполнения различных атак, каждая из которых оформлена отдельным модулем. Существует огромное количество модулей, например, для кражи файлов, сканирования сети и т.д.

Туннель создается, когда пользователь заходит на страницу с XSS-уязвимостью. Затем злоумышленник определяет браузер пользователя, ищет подходящий эксплойт и налаживает сеанс работы с жертвой.

Особенность XSSF – «атака на автомате», когда автоматически по очереди исполняются несколько эксплойтов после захода жертвы на уязвимую страницу.

Программа имеет собственный веб-интерфейс, где отображается следующая информация о проэксплуатированных целях: IP-адрес, название браузера, версия браузера, наличие cookie (рис. 6).

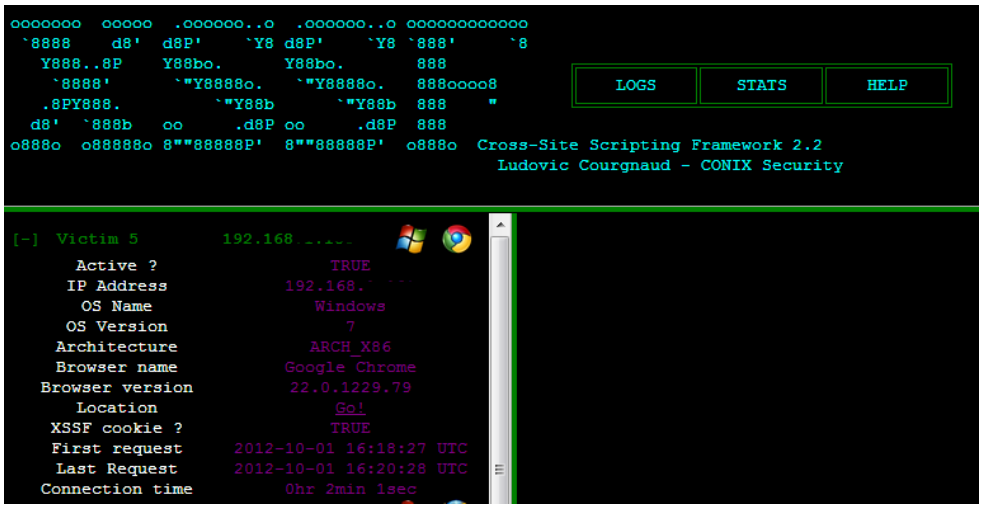


Рис 6. Данные о жертве атаки

Рассмотренные инструменты для поиска и эксплуатации XSS-уязвимостей позволяют существенно упростить работу по обнаружению уязвимостей в веб-приложениях.

Литература

[1]. Бреева А. Поцелуевская Е. Уязвимости веб-приложений: ситуация не улучшается. URL: http://www.ptsecurity.ru/download/PT_Positive_Research_2015_RU_web.pdf (дата обращения: 03.10.2015)

[2]. Межсайтовый скриптинг. URL: https://ru.wikipedia.org/wiki/Межсайтовый_скриптинг (дата обращения: 19.09.2015)

[3]. OWASP Xenotix XSS Exploit. URL: https://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework (дата обращения: 02.10.2015).

[4]. XSS Attack: Hacking Using BeeF XSS Framework. URL: http://www.hacking-tutorial.com/hacking-tutorial/xss-attack-hacking-using-beef-xssframework/#sthash.15g6TVbz.dpbs (дата обращения: 02.10.2015)

Ивченкова Юлия Сергеевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: Ivchenkova01@yandex.ru

Савкин Михаил Константинович – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

С.В. Лаптев, А.В. Мазин

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В НАВИГАЦИОННО-МОНИТОРИНГОВЫХ СИСТЕМАХ МВД РОССИИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Большое распространение в деятельности сотрудников органов внутренних дел Российской Федерации (далее – ОВД) и военнослужащих внутренних войск МВД России получили навигационно-мониторинговые системы (далее – НМС), выполняющие диспетчерские функции.

НМС - это комплекс технических и аппаратно-программных средств на основе аппаратуры спутниковой навигации, обеспечивающий возможность контроля в центре мониторинга состояния и местоположения транспортных средств и позволяющий принимать решения по их управлению в соответствии с полученной информацией.

Принцип работы НМС основан на получении от навигационной аппаратуры потребителей, которая установлена на подвижных объектах, данных об их местоположении. Информация с борта транспортного средства или от отдельных сотрудников (военнослужащих) передается по радиоканалу (УКВ или GSM), а между центрами по выделенному каналу связи. Информация о местоположении объекта отображается на фоне электронной карты местности, на мониторе. Кроме того на мониторе отображается состояние объекта (движение, стоянка, тревожные сообщения и т.д.).

Типовая структура НМС представлена на рисунке 1.

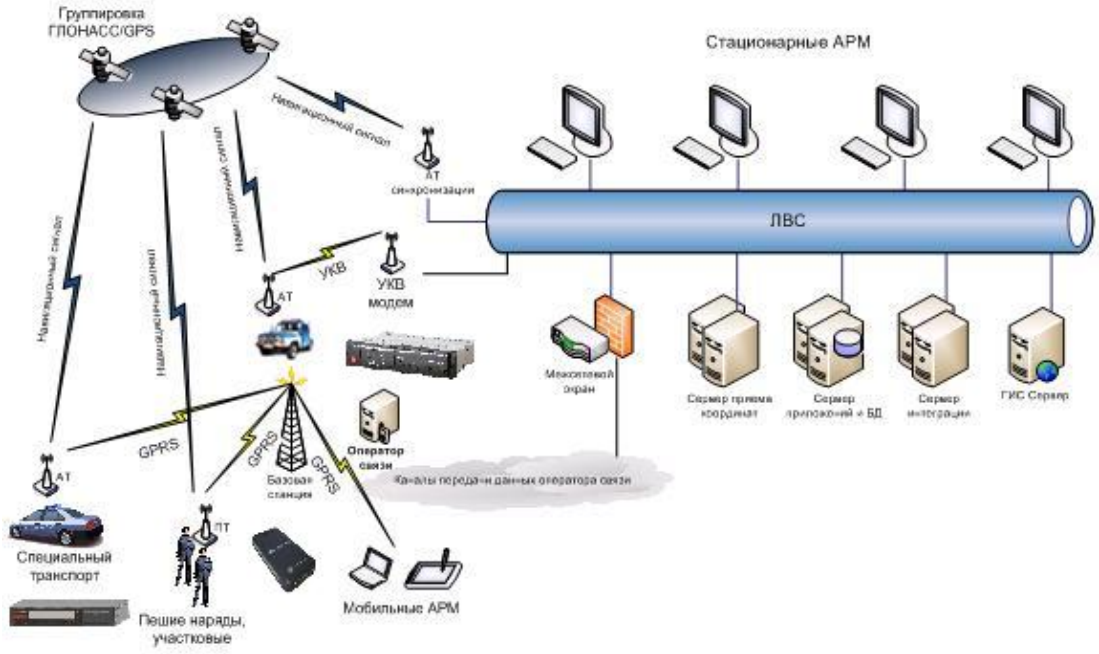


Рис. 1. Структура НМС

К элементам НМС, которые с позиции информационной безопасности, являются уязвимыми и требуют применения средств защиты информации, относятся следующие процессы:

— получение радионавигационной информации (сигналов) от космических аппаратов группировок ГЛОНАСС и GPS навигационной аппаратурой потребителей (далее – НАП), установленной на подвижных объектах;
— передача информации от мобильных объектов, на которых установлена НАП, в центр мониторинга (далее – ЦМ);
— обмен информацией между центрами мониторинга.

Рассмотрим более подробно каждый из процессов, применительно к указанным участкам передачи информации.

1. Каждый навигационный космический аппарат (далее – НКА) группировки ГЛОНАСС и GPS передает открытый сигнал (доступный любому потребителю) и «закрытый» сигнал, т.е. предназначенный для военных и специальных потребителей. В технической литературе он называется «сигнал санкционированного доступа», разрешение на его применение дает Минобороны России. Сигналы GPS, в отличие от ГЛОНАСС, могут загрубляться в пределах отдельных регионов по решению правительства США. Поэтому его исключительное использование в навигационной аппаратуре силовых структур Российской Федерации нецелесообразно.

Таким образом, для ограничения лиц к сигналам санкционированного доступа, требуется решение задачи избирательного доступа к передаваемой по радиоканалу навигационной информации. Избирательный доступ осуществляется как в отношении навигационной информации, так и со стороны различных категорий пользователей такой информацией (Минобороны России, МВД России, ФСБ России и др.). Для решения задач избирательного доступа необходимо обеспечить защиту информации от ее использования несанкционированным пользователем. Такая защита может выполняться различными методами и средствами. Для навигационной информации от несанкционированного доступа при ее перехвате на радиоканале применяется специальное кодирование. Специальное кодирование производится на основе алгоритма криптографического преобразования по общедоступному ГОСТ 28147-89, при этом структура протокола передачи информации остается неизменной. В НАП специальных потребителей производится декодирование принятой информации. Кроме того осуществляется защита информации от несанкционированного использования потребителями, имеющими уровень доступа ниже установленного. В качестве базовых элементов для технической реализации метода используются микропроцессоры (микроконтроллеры), имеющие защищенную область памяти для хранения ключа (параметра кодирования). Избирательный доступ с использованием этого метода реализован в НАП Минобороны России. В дальнейшем он будет использоваться в аппаратуре других силовых структур.

2. Передача информации от мобильных объектов, на которых установлена НАП, в ЦМ осуществляется по беспроводным каналам. В качестве канала передачи данных между мобильными терминалами и ЦМ могут быть использованы: сотовая связь, радиосвязь с использованием цифровых транков, УКВ конвенциальная радиосвязь, связь на основе широкополосного беспроводного доступа и спутниковая связь. Каналы сотовой и спутниковой связи предоставляются операторами на коммерческой основе и не обеспечивают закрытие передаваемой информации. УКВ связь организуется на штатных радиостанциях и не требует оплаты за трафик, но, как правило, передающих информацию также в открытом режиме. Для обеспечения защиты от несанкционированного доступа (далее – НСД) к этой информации применяются сертифицированные средства, в том числе средства криптографической защиты информации (далее – СКЗИ).В НМС гражданского назначения допускается использование в качестве канала связи Интернет.

3. Обмен информацией между ЦМ осуществляется по выделенным каналам связи.Выделенный канал - это канал с фиксированной полосой пропускания или фиксированной пропускной способностью, постоянно соединяющий двух абонентов. Абонентами могут быть как отдельные устройства (компьютеры или терминалы), так и целые сети. Для обеспечения защиты от НСД на этом участке применяется сертифицированное криптографическое оборудование.

В настоящее время наиболее полно удовлетворяет требованиям информационной безопасности автоматизированная система мониторинга местонахождения МВД России (далее – АСММ) (индекс 14Ц884) подвижных объектов с использованием спутниковых навигационных систем ГЛОНАСС/GPS, эксплуатируемая внутренними войсками МВД России (далее – ВВ). Данная система разработана по заказу Минобороны России и принята на снабжение Вооруженных Сил Российской Федерации и внутренних войск МВД России.

Кратко рассмотрим организационно-технические аспекты, реализованные в этой системе. Для того чтобы понять принципы обеспечения информационной безопасности, необходимо знать, какая информация циркулирует и обрабатывается в системе.

В системе 14Ц884 присутствует следующая информация:

— открытые данные;
— идентификационные данные объекта (для транспортных средств (далее – ТС): марка ТС, модель ТС, государственный номер);
— служебная информация ограниченного распространения (данные о местонахождении и дислокацииобъектов, их состояниях, маршрутах движения, связанных с ними событиях и т.д.);
— персональные данные сотрудников (военнослужащих), использующих возможности системы.

Система 14Ц884, как объект автоматизации, представляет собоймногоуровневую (4 уровня) иерархически структурированную систему, состоящую из НАП и центров мониторинга различных уровней, с возможностью организации вертикальных и горизонтальных связей между ЦМ. Структурная схема представлена на рисунке 2.

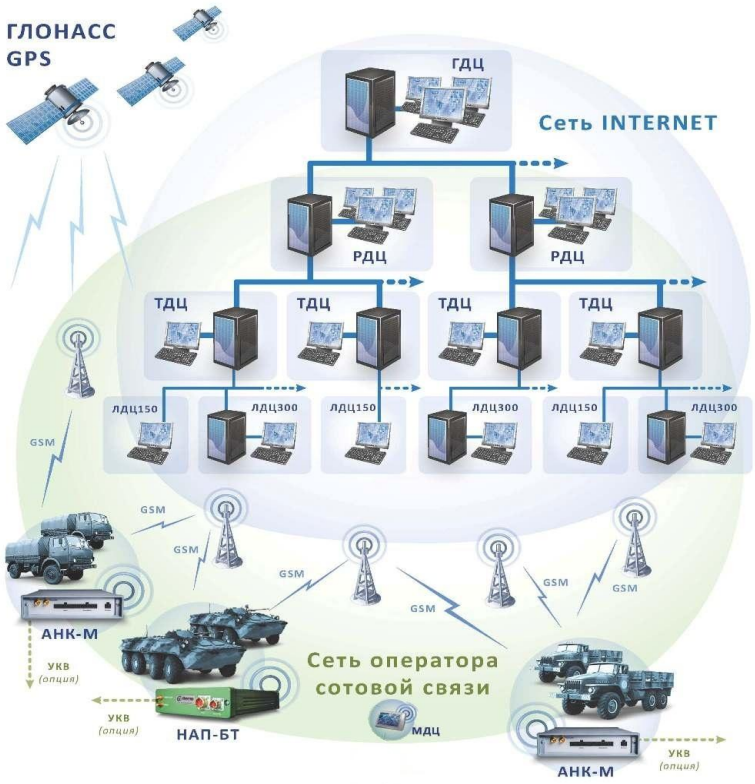


Рис. 2. Структурная схема системы 14Ц884

Все ЦМ, функционируя автономно или взаимосвязано в рамках иерархии и / или горизонтальных связей, учитывают, отображают и хранят информацию, поступающую в режиме реального времени от НАП. При этом каждый ЦМ аккумулирует информацию, поступающую только от зарегистрированныхНАП. Поступающая информация анализируется встроенными алгоритмами.

В качестве каналов передачи информации используются:

— открытые беспроводные каналы связи (сотовые сети связи стандарта GSM, УКВ);
— внутренние сети МВД России, не имеющие выхода во внешние сети.

При использовании открытых каналов связи элементы НМС передают незащищаемые сведения.При взаимодействии элементов системы между собой и с внешними информационными системами могут передаваться как открытые, так и конфиденциальные данные.

Доступ к информационным ресурсам осуществляется:

— элементами НМС по технологии «толстого», и «тонкого» клиента;
— пользователями взаимодействующих систем – только «тонкого» клиента.

Права элементов НМС и элементов иных взаимодействующих с ней систем на доступ к информационным ресурсам задаются средствами разграничения прав доступа.

В соответствии с требованиями статьи 5 Федерального закона от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании» и приказа ФСТЭК от 11 февраля 2013 года № 17 все применяемые в НМС средства защиты информации проходят оценку соответствия требованиям по безопасности информации (в форме обязательной сертификации). Согласно модели угроз безопасности информации МВД России система должна соответствовать 1-му классу защищенности информационных систем и обеспечивать 4-ый уровень защищенности персональных данных.

Технические средства, входящие в состав ЦМ НМС, должны соответствовать следующим требованиям:

— средства вычислительной техники – не ниже 5-го класса;
— системы обнаружения вторжений и средства антивирусной защиты – не ниже 4-го класса;
— межсетевые экраны – не ниже 3-го класса.

Меры, реализуемые системой защиты информации с учетом типа актуальных угроз (3-ий), уровня защищенности ПДн (4-ый), класса защищенности информационных систем (1-ый) и применяемых информационных технологий, включают:

— идентификацию и аутентификацию субъектов доступа и объектов доступа;
— управление доступом субъектов доступа к объектам доступа;
— ограничение программной среды;
— защиту машинных носителей информации;
— регистрацию событий безопасности;
— антивирусную защиту;
— обнаружение вторжений;
— контроль (анализ) защищенности информации;
— обеспечение целостности информационной системы и информации;
— обеспечение доступности информации;
— защиту среды виртуализации;
— защиту технических средств;
— защиту информационной системы, ее средств, систем связи и передачи данных;
— управление конфигурацией информационной системы и системы защиты персональных данных.

Для мобильных центров мониторинга информационная безопасность достигается применением:

— штатных средств информационно-телекоммуникационной сетиВВ МВД России;
— средств антивирусной защиты – не ниже 4-го класса;
— организационных мер.

Согласно модели угроз безопасности информации НМС имеет класс защищенности АС – 1Г.

Эффективное функционирование НМС возможно только при совместной обработке информационных баз данных, хранящихся на различных ЦМ. Необходимым условием организации такого взаимодействия по каналам связи общего пользования является применение средств криптографической защиты информации и шифрования конфиденциального трафика.

Используемые в системе средства криптографической защиты информациидолжны удовлетворять требованиям уровня криптографической защиты КС3. В системе применяются также средства межсетевого экранирования (далее – МЭ) и средств обнаружения вторжений (далее – СОВ).В целях экономии ресурсов используются комбинированные аппаратно-программные средства, объединяющие функционал СКЗИ, МЭ и СОВ, а именно: аппаратно-программный комплекс шифрования «Континент». Для мобильных центров мониторинга применяется СКЗИ «Континент-АП» в совокупности с комбинированным программным средством, включающим в себя СОВ и МЭ.

Телеметрическая информация, циркулирующая в НМС, не относится к информации ограниченного распространения, однако, высокая ценность актуальной информации о местонахождении (дислокации) мобильных объектов внутренних войск МВД России предполагает применение ряда дополнительных мер по обеспечению безопасности таких данных.

В качестве такой дополнительной меры обеспечения защиты информации используется техническое закрытие (скремблирование или специальное кодирование). В настоящее время сертифицированным решением, обеспечивающим такой механизм технического закрытия, разработчиками предложен унифицированный аппаратно-программный модуль избирательного доступа к информации для абонентских навигационных комплектов.Он может использоваться в навигационных системах класса защищенности до 1Г включительно.

Кроме описанных мер защиты информации для наиболее уязвимых элементов НМС, особое значение имеет помехозащищенность самой НАП. Используемая в МВД России НАП в настоящее время не обладает достаточной помехозащищенностью. Навигационные модули, устанавливаемые в НАП, не обеспечивают работу по высокоточному сигналу, обладающему повышенной помехозащищенностью, а алгоритмы, реализованные в навигационной аппаратуре, не позволяют полностью компенсировать влияние источников помех. Причем помехи могут быть как промышленными, так и организованными злоумышленниками. Учитывая, что система ГЛОНАСС является

стратегическим средством, обеспечивающим национальную безопасность, не исключается постановка преднамеренных помех со стороны потенциальных противников. А это уже не дворовые хулиганы, а хорошо организованная и технически оснащенная кооперация зарубежных стран, состоящих в блоке НАТО. Поэтому степень защищенности от подобного уровня помех должен быть соответствующим угрозам.

Помимо упомянутого способа защиты от помех (использование высокоточного сигнала) существуют и другие способы борьбы с помехами. К ним можно отнести использование двухчастотной НАП, принимающей навигационный сигнал в двух частотных диапазонах: L1 и L2, что позволяет повысить ее устойчивость к радиопомехам в диапазоне GPS (воспринимаемых как блокирующие помехи в приемном тракте аппаратуры), а также противостоять многократно переотраженным сигналам (многолучевости) и сводить к минимуму влияние ионосферных погрешностей навигационного сигнала.

Все эти риски необходимо оценить применительно к задачам, решаемым сотрудниками ОВД и военнослужащими ВВ МВД России, учесть при подготовке моделей угроз и использовать при создании перспективной НАП.

Заключение

Таким образом на примере автоматизированной системы мониторинга местоположения 14Ц884 рассмотрены принципы обеспечения информационной безопасности в навигационно-мониторинговых системах МВД России, которая в условиях обострения военно-политической обстановки приобретает для МВД России особое значение.

В настоящее время методы и способы защиты информации, используемые в навигационно-мониторинговых системах МВД России, можно рассматривать как соответствующие требованиям в мирное время. Для подготовки НМС к использованию в различные периоды военно-политической обстановки в рамках ФЦП «ГЛОНАСС-2020» будут разработаны технические средства, максимально удовлетворяющие требованиям информационной безопасности.

Единая техническая политика, проводимая Департаментом информационных технологий, связи и защиты информации МВД России направлена на проведение комплекса мероприятий (организационных, правовых, технических), который позволит предотвратить неправомерный доступ к информации ивозможный ущерб, а сотрудники Федерального казенного учреждения «Научно-производственного объединения «Специальная техника и связь» МВД России обеспечивают практическую реализацию этих мероприятий при разработке НМС.

Литература:

[1]. Приказ МВД России от 31.12.2008 №1197 «Об утверждении и использовании общих тактико-технических требований к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России».

[2]. «Тактико-технические требования к навигационно-мониторинговым системам ГЛОНАСС/GPS для легковых и грузовых автомобилей внутренних войск МВД России», утвержденные 8 октября 2012 г. начальником главного штаба внутренних войск МВД России С.В. Буниным.

[3]. Федеральный закон от 27.06.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

[4]. Приказ МВД России от 14.12.2013 г. №975 «О принятии на снабжение внутренних войск МВД России специальной техники.

[5]. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

[6]. Методические рекомендации по применению навигационной аппаратуры ГЛОНАСС сотрудниками ОВД и военнослужащими внутренних войск МВД России. – М.: ФКУ НПО «СТиС» МВД России, 2012.

[7]. Сазонов В.Е. Избирательный доступ к передаваемой навигационной информации. Сборник материалов научно-технических конференции 2009-2010. Издательство «Лика», г. Москва.

[8]. Поваров В.В. «Современные подходы к обеспечению информационной безопасности Министерства внутренних дел Российской Федерации с конкретным примером организации системы антивирусной защиты». Сборник докладов Международной научно-практической конференции «СПЕЦ-информационные технологии». Москва, 2015.

Лаптев Сергей Владимирович - начальник сектора КФ ФКУ НПО "СТиС" МВД России. E-mail: avreliimark@yandex.ru

Мазин Анатолий Викторович – д-р техн. наук, зав. каф. КФ МГТУ им. Н.Э. Баумана. E-mail: mazinav@yandex.ru

А.Н. Злыгостева, О.Ю. Жарова

МЕТОДЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ СОРТИРОВКИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В данной статье рассмотрена Корневая сортировка (Поразрядная сортировка, RadixSort) и ее сравнение с «Быстрой» сортировкой (QuickSort).

Целью данной работы является поиск методов повышения эффективности использования аппаратных ресурсов при решении задач связанных с сортировкой больших массивов данных.

RadixSort – алгоритм сортировки без сравнений. Является наиболее эффективным алгоритмом из всех существующих на сегодняшний день. Его сложность, как в наилучшем, так и в наихудшем случае равна O(N) (N – число элементов массива), то есть, сложность алгоритма линейна. Сортировка происходит по разрядам чисел входного массива, то естьпоочередно на каждом цикле числа проверяются по первому разряду, на следующем – по второму разряду и так далее, пока не будет полученотсортированныймассив чисел. Это первый тип корневой сортировки – LSD, с младших разрядов, до старших. Он используется для дальнейшей сравнительной характеристики, так как больше всего он подходит для сортировки чисел. Второй тип RadixSort – MSD. Он противоположен LSD – сортировка идет со старших разрядов к младшим. И этот тип используется для лексикографической сортировки строк. После каждого прохода по массиву получаются так называемые «стопки» элементов, которые представляют из себя массив чисел, выбранных из общего множества по принципу равенства цифр в определенном разряде.Из них в дальнейших проходах берутся числа, что в итоге приводит к тому, что в конце получается коллекция «стопок», при записи элементов которых по очереди получится готовый отсортированный массив. Поэтому этот алгоритм и не использует сравнений, так как происходят постепенные перекладывания элементов до достижения нужного результата. НедостатокRadixSort – большое потребление памяти, чему в данной статье тоже будет уделено внимание.

QuickSort – это алгоритм сортировки со сравнениями, который является одним из самых быстрых среди существующих алгоритмов.Его сложность O(N*log(N)) (N – число элементов массива). «Быстрая» сортировка рекурсивна. Каждый новый проход она делит массив еще на два массива, и для каждой части вызывает сама себя, таким образом постепенно отсортировывая весь массив. Существует множество видов «быстрой» сортировки, в основном они различаются выбором опорного

элемента – элемента, относительно которого сравниваются остальные числа. Для данной статьи использовался вариант QuickSort со средним в массиве опорным элементом. Сравниваются числа до среднего числа и после него с самим средним числом. Если левее него числа больше, они переносятся вправо, и, если правее него числа меньше, меняем их с неугодными числами в левой части. Потом делим массив относительно опорного элемента и повторяем для обеих частей. При самом худшем варианте QuickSort будет сравнима по скорости с BubbleSort, и разделения массива будут до одного элемента.

Теперь разберем вопрос о занимаемом объеме памяти при применении этих сортировок. Как уже было сказано выше, недостаток RadixSort – это большое потребление памяти, вследствие того, что нам на каждой итерации нужно хранить 10 списков, в которых хранятся «стопки» чисел. Чтобы оптимизировать этот процесс можно использовать динамические массивы, например, в языке программирования C++ это vector:

```
vector<int> *Temp = newvector<int>[10];
```

— Для данной задачи создается массив динамических массивов (векторов), так как количество цифр известно, а вот размер сортируемых данных – нет.
— Из полученных «стопок» копируются элементы в исходный массив, а динамические массивы, хранящие их, очищаем до следующей итерации, что дает нам дополнительный объем памяти.

```
for (size_t j = 0; j < 10; j++)
        {       Temp[j].resize(0);  }
```

После отработки алгоритма освобождается память, занятая под «стопки».

```
delete[] Temp;
```

BquickSort единственная проблема с занимаемой памятью – это переполнение стека в худшем случае, при большом количестве элементов, так как QuickSort, как было сказано выше – рекурсивный алгоритм сортировки. Чтобы уменьшить влияние этого недостатка на работу программы, в настоящее время придумано огромное количество оптимизаций, связанных или с выбором опорного элемента, или с разбиением не на две, а на три части исходного массива, а, так же, применением вместо QuickSort сортировки Introsort, базирующуюся на QuickSort.

Рассмотрим быстродействие данных сортировок на разных входных данных, а именно – размер массива и диапазон значений. Размер массива

будем брать довольно большой, так как разницы по времени при сортировке маленького массива данных видно не будет.

Входные параметры будут изменяться так: на вход даются случайные числа; отсортированный, или почти отсортированный массив; числа в обратном порядке следования (например 3, 2, 1, 0); массив с малым количеством уникальных элементов. По размерам возьмем массивы из 1000000: 200000; 3000000 и 4000000 элементов, чтобы проследить линейное увеличение времени работы RadixSort. Значения в таблицы будут записываться в миллисекундах. Замеры будут производиться 50 раз, в таблицу заносится среднее значение. Данные замеры нельзя считать точными, так как время отработки алгоритма зависит от состояния системы на данный момент, а оно имеет свойство изменяться.

Таблица 1. Корневая сортировка

		Размер входного массива			
		1000000	200000	3000000	4000000
Входные данные	Случайные	137,84	207,7	356,14	545,14
	Отсортированный	165,88	292,12	368,8	559,7
	Обратный	186,06	311,1	566,06	790,68
	Мало уникальных	75,3	125,3	192	289,12

Таблица 2. «Быстрая» сортировка:

		Размер входного массива			
		1000000	200000	3000000	4000000
Входные данные	Случайные	132,38	182,92	325,5	485,74
	Отсортированный	19,3	32,96	46,66	65,68
	Обратный	20,36	37,28	76,02	102,6
	Мало уникальных	63,4	124,06	183,9	277,84

Видно, что при случайных числах действительно видна линейная зависимость времени работы от количества сортируемых элементов в RadixSort. Время работы «быстрой» и корневой сортировок приблизительно равно.

При отсортированном массиве данных скорость «быстрой» сортировки резко возросла, в то время как корневая осталась стабильной. То же самое наблюдалось и про обратном порядке следования чисел. Хочется заметить, что если бы в «быстрой» сортировке за опорный элемент был выбран первый элемент в массиве, то при достаточно большом размере массива произошло бы переполнение стека. В общем случае она работала бы гораздо медленнее RadixSort, так как это был бы

худший вариант для данного алгоритма сортировки, в то время как у корневой сортировки нет худшего случая, как было сказано выше.

При малом количестве уникальных элементов, которые были выбраны от 0 до 9, у корневой сортировки заметно возрастание скорости, что говорит о ее зависимости от количества разрядов сортируемых чисел – чем их меньше, тем быстрее проходит сортировка.Процесс сортировки RadixSortзанимает то же время, что и «быстрая» сортировка.

В итоге можно сказать, что корневая сортировка хоть и может проигрывать в скорости при особых входных данных, но является более стабильной сортировкой, чем QuickSort, без худшего случая, а также может превосходить «быструю» сортировку при правильной оптимизации, а также на числах с малым количеством разрядов. Единственной проблемой является затрачиваемый объем памяти. Использование динамических массивов и своевременное освобождение памяти значительно улучшает эффективность работы алгоритма и значительно уменьшает объем памяти, потребляемый при работе сортировки.

Список литературы

[1]. *Вирт Н.* Алгоритмы и структуры данных. Новая версия для Оберона [Электронный ресурс]: учебное пособие. — Электрон. дан. — М.: ДМК Пресс, 2010.

[2]. *Павловская Т.А*. C/C++. Программирование на языке высокого уровня. СПб.: Питер, 2010.

[3]. Информационный ресурс Wikipedia
https://ru.wikipedia.org/wiki/Быстрая_сортировка
https://ru.wikipedia.org/wiki/Поразрядная_сортировка

Злыгостева Антонина Николаевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: antonina.zlygosteva@gmail.com

Жарова Ольга Юрьевна – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: ouzharova@yandex.ru

А.Н. Молчанов, Ю.Ю. Лагутин

МИКРОСЕРВИСЫ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время существует множество подходов к созданию программных продуктов. Обычно они основываются на различных архитектурах приложений, таких как монолитная,многоуровневая, клиент-сервер на основе микроядра, а также микросервисная архитектура.

Каждая архитектура базируется на определенных положениях и позволяет получить ряд преимуществ при разработке приложений, их внедрении и дальнейшей модификации в процессе эксплуатации.

Так, например, в многоуровневой архитектуре можно выделить

— наборфункций операционной системы, разделяемый на уровни (уровень управления аппаратурой, уровень файловой системы, уровень управления процессами и памятью и т.п.);
— определение интерфейса взаимодействиядля каждого уровня (т.е. некоторогорегламентированного набора правил, с помощью которого следует обращаться за ответами данного уровня);
— взаимодействие между уровнями организовано таким образом, что каждый уровень может обращаться за услугами только к соседнему нижележащему уровню через его интерфейс;
— недоступность внутренних структур данных каждого уровня и реализации процедур уровня другим уровням.

Идея клиент-серверной архитектуры состоит в том, что все компоненты операционной системы разделяются на программы, называемые - поставщики услуг (программы серверы, выполняющие определенные действия по запросам других программ) и программы – потребители услуг (программы клиенты, обращающиеся к серверам для выполнения определенных действий).

В настоящее время по-прежнему остается самым популярным создание приложений на основе монолитной архитектуры. Приложение,построенное на данной основе, представляет собой единое программное обеспечение, все части которого связанны в единое целое[1].

Монолитный сервер – это обработка запросов в одном процессе, с возможностью разделения приложений на классы, функции, пространственные имена[2].

Хотя данный вид архитектуры является основнымпри создании большинства приложений, приложения, созданные на основе данной архитектуры, имеютопределённое количество минусов.

Основным недостатком является слишком большой размеркода программного продукта, что повышает энтропию проявления ошибки,а любые изменения, даже самые небольшие, требуют новой сборки и развертывания всего монолита.

Для устранения подобных проблем требовалась более динамичная и гибкая в создании и эксплуатации архитектура. Одним из предложенных решений стала,так называемая, микросервисная архитектура.

Микросервисная архитектура (MicroServiceArchitecture, MSA) – это приложение, представляющее собой множество небольших сервисов, взаимодействующих между собой путем обмена сообщениями[3].

Микросервисный стиль — это подход, при котором единое приложение строится как набор небольших сервисов, каждый из которых работает в собственном процессе и взаимодействует с остальными используя легковесные механизмы, как правило HTTP. Сервисы построены вокруг бизнес-потребностей и развертываются независимо с использованием полностью автоматизированной среды. Существует абсолютный минимум централизованного управления этими сервисами. Сами по себе эти сервисы могут быть написаны на разных языках и использовать разные технологии хранения данных.

В настоящее время данный стиль набирает все большую популярность, что обусловлено рядом значительных плюсов.

— Каждой, даже совсем небольшой задаче предоставляется свой инструмент.
— Разрабатывать и администрировать небольшие сервисы проще, чем большие. Естественно, чем меньше кода, тем легче его анализировать и оптимизировать в дальнейшем.
— Выделение каждого значимого компонента в отдельный микросервис позволяет не только улучшить качество разработки, но и сократить количество разработчиков в рамках существующих задач[4].
— Так как проект создается из сервисов и занимает сравнительно небольшое количествострок, вероятность допущения ошибки сводиться к минимуму, к тому же применение юнитестов перестает быть необходимостью.
— Модульность проекта. В любой моментможно заменить, откатить или обновить сервис.
— Всегда есть возможностьэкспериментировать с новыми технологиями.
— Возможность выбора языка программирования и библиотек для каждого сервисадля максимизации эффективности решаемых этим сервисом задач.
— Горизонтально масштабируемый и отказоустойчивый код.

— При определенных параметрах вместо того, чтобы «хостить» большое количество сервисов на сервера, оперирующих огромным количеством ресурсов, становится существенно дешевле разделить систему на сервисы. Каждый из них затем развертывается на системах, дающих только нужные конкретному сервису ресурсы.

Однакоглобальное распространение микросервисов сталкивается с рядом препятствий.

Необходимость решать задачу логистики микросервисов. Так как количествомикросервисов может достигать огромного количества, обмен данными между ними может стать «узким местом» системы.Необходимо оптимизировать протокол обмена сообщениямимежду микросервисами, либо изначально микросервисы, которые взаимодействуют друг с другом «ставить» рядом.

Документирование. Большое количество сервисов требует гораздо большего объема работ по оформлению их спецификаций. Возникают задачи размещения, хранения и оперативного поиска необходимой в процессе работы информации о тех или иных сервисах.

Проблема повторного использования ранее написанного кода. Так в случае изменения разработанных ранее библиотек, использующихся в различных сервисах, потребуется оперативное обновление всех этих сервисов[5].

Несмотря на это, микросервисы находят своё применение в следующих областях разработки приложений:

— организация доступа к данным;
— отслеживание исключений;
— аутентификацияиавторизация;
— кэширование;
— параллельные вычисления
— транзакции;
— менеджмент настроек и конфигураций;
— логирование и мониторинг систем;
— пользовательские коммуникации;
— объектная связанность и сцепление;
— проверка данных;
— потоковые операции.

Ключевые возможности микросервисов - возможность разрабатывать один проект на разных языках программирования, запускать проектраспределённо на нескольких серверах, обеспечивать дополнительный уровень безопасности системы, за счет изолированности сервисов и использования защищенных протоколов несомненно вызывают интерес со стороны разработчиков сложных систем. Но на данном этапе

развитиямикросервисная архитектура слишком нестабильна и очень часто успешные проекты, которые разрабатываются с помощью нее могли найти решение в монолитном построении. Важно определить границы компонентов, провести декомпозицию всего приложения,таким образом, чтобы связи компонентов между собой были минимальны. В дальнейшем перенос кода и изменение интерфейсов требуют гораздо большей координации между группами разработчиков, что ведет к необходимости ввода дополнительных слоев совместимости и заметно усложняет процесс тестирования.

На практике, при использовании прочих архитектурных решений, как бы не изолировали модули, классы, библиотеки, разработчики постоянно нарушают границы между компонентами, что приводит к проникновению одних частей кода в другие. Возможность оперативного масштабирования и модернизации системы становятся минимальными. Поэтому, главное, что предлагает сейчас микросервисная архитектура – это способ сохранить это разделение в процессе работы над проектом.

Пристатейный библиографический список

[1]. Operating Systems: Design and Implementation ISBN 0-13-638677-6

[2]. Microservices.URL: http://www.martinfowler.com/articles/microservices.html

[3]. Плюсы микросервисной архитектуры.. URL: http://habrahabr.ru/post/261237/

[4].Micro Service Architecture. URL: https://yobriefca.se/blog/2013/04/29/micro-service-architecture/

[5]. Microservices. The good, the bad and the ugly. URL: http://sanderhoogendoorn.com/blog/index.php/microservices-the-good-the-bad-and-the-ugly/

Молчанов Алексей Николаевич – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

Лагутин Юрий Юрьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: lagutin.yurik2@gmail.com

А.А. Москвина, А.Б. Лачихина

ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ БАЗ ДАННЫХ ПРИ ПОМОЩИ СРЕДСТВА ЗЕРКАЛЬНОГО ОТОБРАЖЕНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Под доступностью данных понимается состояние ресурсов автоматизированной информационной системы, при котором субъекты могут беспрепятственно реализовывать свои права доступа.

Возможность получения пользователями разрешенной правами доступа информации является одной из наиболее важных задач для различных компаний, предприятий и других организаций, использующих базы данных, но также немаловажным показателем надежной системы является время отклика программы, что тоже входит в понятие доступности данных.

Процесс зеркального отображения БД – один из механизмов обеспечения доступности в SQL Server (рис.1).

Прежде чем приступать к рассмотрению данного средства защиты БД, необходимо ознакомиться с основными терминами, которые будут использоваться.

Основной сервер. Основным сервером является рабочий сервер-источник, на котором размещается база данных, постоянно отправляющая свои журналы транзакций зеркальному серверу и его базе данных.

Зеркальный сервер. Зеркальным сервером является сервер-получатель. На нём размещается резервная копия базы данных (зеркальная), которая постоянно синхронизируется с базой данных основного сервера.

Следящий сервер. Следящий сервер осуществляет наблюдение за работой основного и зеркального серверов, а также при сбое может запустить процесс автоматического перехода на другой ресурс.

Партнер. Партнером является основной или зеркальный сервер.

При использовании зеркального отображения базы данных, устанавливается связь, называемая сеансом зеркального отображения БД, между двумя разными экземплярами сервера, на которых размещены копии одной базы данных. Один из экземпляров сервера выступает в качестве основного, другой – в качестве зеркального. Синхронизация данного сеанса позволяет получить сервер, который способен поддерживать быструю отработку отказа без потери информации о зафиксированных транзакциях.

Зеркальное отображение базы данных заключается в том, что в зеркальной БД повторяются все операции изменения, удаления, вставки, и обновления, которые выполняются в основной базе. Для этого поток записей активных транзакций с максимально возможной скоростью

пересылается на зеркальный сервер. Зеркальный сервер получает журнал, после чего выполняет операции по его скорейшему применению. Как только журналы будут применены на зеркальном сервере, базы данных считаются синхронизированными и остаются такими до разрыва сеанса зеркального отображения.

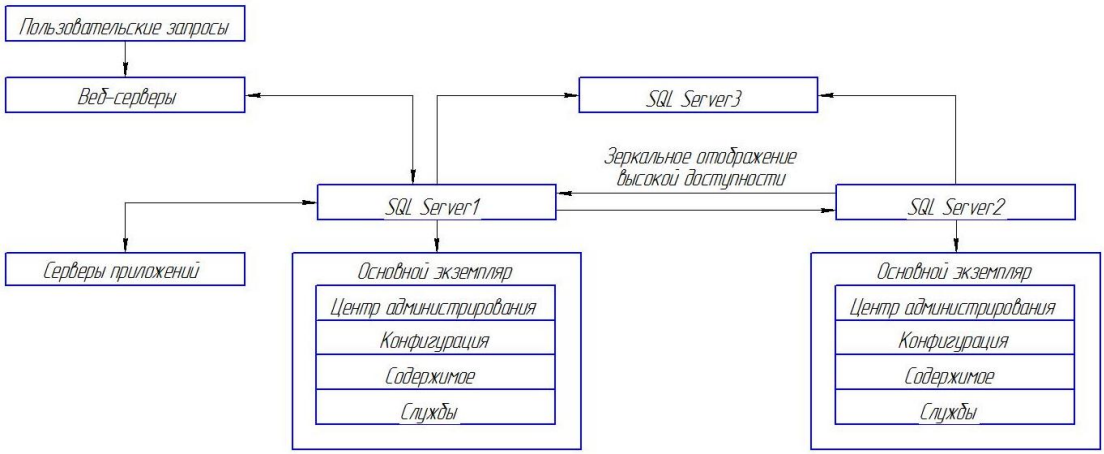


Рис.1- Процесс Зеркального отображения БД

В случае если происходит сбой, зеркальный сервер может начать процедуру автоматического переключения ресурсов, в этот момент следящий сервер осуществляет поддержку данного процесса - определяет доступна ли база данных основного сервера. Проблему необходимо устранять на том сервере, который в настоящий момент является зеркальным партнером, до того, как основа станет основным. Как только все процессы по устранению неполадок будут успешно завершены, начинается перемещение обратно на сервер зеркального партнера, и базы данных синхронизируются снова. После выполнения синхронизации сеанс зеркального отображения можно возобновить.

Так же в результате сбоя может значительно пострадать центральная база и для того, чтобы устранить подобные последствия, применяется команда принудительного восстановления:

ALTER DATABASE MIRROR_TEST SET PARTNER FORCE_SERVICE_ALLOW_DATA_LOSS

К сожалению, эта мера защиты допускает потерю части данных, которые не успели попасть на зеркальный сервер.

После завершения принудительного восстановления, зеркальная и основная базы меняются ролями.

Если возникает необходимость поменять роли баз данных вручную, необходимо использовать команду:

ALTER DATABASE MIRROR_TEST SET PARTNER FAILOVER

В случае запуска зеркалирования применяется следующая команда:

ALTER DATABASE MIRROR_TEST SET PARTNER RESUME

Основные преимущества зеркального отображения БД:

— процесс зеркального отображения позволяет избежать отставания при синхронизации данных и гарантирует идентичность копий данных на обоих серверах;
— повышает защиту данных за счет обеспечения полной избыточности данных;
— используются две копии базы данных, в результате чего повышается надежность работы;
— используемые сервисы не обязательно должны находиться рядом друг с другом;
— при наличии следящего сервера, переключение ролей может производиться автоматически в случае отказа основного сервера;
— процесс не требует применения специального оборудования;
— наличие возможности автоматического переключения на использование зеркальной копии;
— повышает доступность рабочей БД при обновлениях.

При верной оценке параметров системы и нагрузок, которым она подвергается, а также при необходимости сократить издержки, использование механизма зеркального отображения позволит добиться наиболее оптимальной производительности. В случае, когда производительность даже при значительных нагрузках не затрудняет взаимодействие пользователя с системой, говорит о высоком уровне доступности, и данный механизм обеспечения доступности способен справиться с подобной задачей.

Процесс зеркального отображения баз данных может стать удачным решением для широкого спектра предприятий, а также как малого, так и крупного бизнеса, разница заключается лишь в требованиях, предъявляемых к системе, и, несмотря на это, данное средство защиты удовлетворяет различным уровням потребностей организаций в реализации доступности данных.

Литература

[1]. Грабер М. *MasteringSQL*. Москва, Лори, 2007, 672 с.

[2]. *Зеркальное отображение базы данных (SQL Server)* URL: https://msdn.microsoft.com/ru-ru/library (дата обращения 24.10.2015).

[3]. Bagui S. *Learning SQL on SQL Server 2005*. O'Reilly, 2006, 342 p.

[4]. Лачихина А.Б., Петраков А.А., Москвина А.А. Обеспечение доступности в базах данных корпоративных информационных систем с помощью средств СУБД SQL Server. *Вопросы радиоэлектроники.* 2015, № 8 (8), С. 100-108.

Москвина Анастасия Александровна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: N.Haruka69@yandex.ru

Лачихина Анастасия Борисовна – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

А.Н. Молчанов, Д.А. Аверьянов, Ю.Ю. Лагутин

ОБЗОР ИНСТРУМЕНТОВ ДЛЯ РАЗРАБОТКИ БАЗ ДАННЫХ MYSQL

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Создание таблиц базы данных,связейимежду ними, организация работы индексов, написание необходимых запросов являются очень важными задачами при разработкеструктуры базы данных. В качестве основного инструмента при создании и администрировании базы данных можно использовать программные продукты, как входящие в комплект поставки СУБД, так и разработанные сторонними разработчиками и распространяемыми черезсеть Internet. Для каждой популярной СУБД можно найти десяток приложений, разработчики которых, заявляют, что именно их система позволяет максимально удобно и быстро выполнять все необходимые операции с базой данных.Было решено изучить и провести сравнение самых популярных инструментов для разработки баз данных MySQL[1].

MySQLWorkbench — официальная система для разработки и администрирования баз данных от издателей и разработчиков MySQL.Может использоваться для проектирования и администрирования баз данных. Установка данного продукта нетребует глубоких знаний администрирования вебсервераивыполняетсядостаточнобыстро.

Рекомендуемыесистемныетребования:CPUSingle Core 3GHz or higher, Dual Core 2GHz or higher, RAM4 GBor higher, Display1920×1200 or higher.[2]

Графический интерфейс данной системы позволяет легко создавать структуру базы любой сложности, а простота в использовании ипонятность позволит легко ориентироваться в ней.

Обеспечение безопасностисоздаваемой базы данных достигается по средствам наличия таких функций как: ведение журнализации, учет пользователейи последующее отслеживание их активности,создание пользователей с определенными правами.

MySQLWorkbench поддерживаетMySQLServerversions 5.1 и выше, так же совместим с более поздней версией MySQLServer 5.0.

Данный продукт до сих пор поддерживается разработчиком OracleCorporation. Последняя его версия 6.3.4. выпущенная 15 июля 2015 года. MySQLWorkbench является бесплатным продуктом на рынке.

Достоинства:

— При разработке не требуется подключение к серверу.

Недостатки:

— Скудный функционал буфера обмена.

— Отсутствует конструктор запросов, поэтому все запросынеобходимо писать вручную.

phpMyAdmin — инструмент, созданный для непосредственного администрирования. Данный сервис не практичен в использовании проектирования базы данных, в связи с тем, что основной задачей данного сервиса является администрирование. Конструктор запросов позволяет формировать запросы без их ручного написания.

Установка данного продукта, не требует особых навыков у пользователя, а системные требования очень демократичны.

Рекомендуемыесистемныетребования:CPUSingleCore 3GHzorhigher,RAM4 GB or higher, Display1024×768or higher

В таблице ниже приведенный системные требования. (Таблица 2)

Графический интерфейс программы не является запутанным и сложным в использовании, все функции легко доступны.

Наличиелицензии GNU GeneralPublicLicenseпредоставляют возможность интегрирования PHPMyAdmin в собственные разработки.

PHPMyAdminпредоставляет возможности безопасногоиспользованияСУБД и разработанных баз данных. Это достигается такими функциями как включение защиты от SQL инъекций в pmd_pdf.php и schema_export.php. Так же объект jsonстал наиболее защищенным в последней версии данного продукта. Осуществляется возможность управления пользователями и привилегиями, управление хранимыми процедурами и триггерами.

phpMyAdminподдерживает MySQLServerversions 5.1 и выше, так же совместим с более поздней версиейMySQLServer 5.0.[3]

Данный сервис является бесплатным на рынке. Последняя его версияphpMyAdmin 4.4.15. она была выпущена 22 сентября 2015 г.

Достоинства:

— Запуск возможен непосредственно с сервера это удобно при хостинге и когда хостер запрещает удаленный доступ к базе
— Возможность управлять СУБД MySQL без непосредственного ввода SQL команд;
— Панель управления PHPMyAdmin предоставляет возможность администрирования выделенных БД;[1]

Ar-wikBuilder — это онлайн сервис предназначенный для разработки структуры баз данных, работы по созданию запросов с использованием конструкторов.

Рекомендуемыесистемныетребования: CPU2МГц or higher, RAM512 GBor higher, Display1920×1200 or higher.

Графический интерфейс минималистичен и позволяет манипулировать таблицами, их полями и связями между ними.Визуальная среда, позволит легко и быстро спроектировать базу данных. Система импорта и экспорта облегчит использование предыдущих наработок, а система контроля кода предупредит о возможных ошибках. Сервис позволяет внедрять PHP код непосредственно в запросы, не заботясь о необходимости проверки данных. Все проверки выполняются автоматически.

Инструментов по обеспечению безопасности базы данных при работе с ней в системе не предусмотрено.Данный онлайн сервис является бесплатным и постоянно обновляется.

Достоинства:

— При разработке не требуется подключение к серверу.
— Существует возможность внедрения PHP функций с помощью конструктора запросов.
— Удобный импорт/экспорт проекта и его частей
— Присутствует возможность обмена проектами с другими пользователями сервиса[4]

Недостатки:

— Конструкторы для хранимых процедур и триггеров не предусмотрены, поэтому разработчику приходится писать их самому.
— Низкий функционал по обеспечению безопасности

DBToolsManager — этоинструмент, созданный с целью управления данными, с встроенной поддержкой MySQL, PostgreSQL, MSAccess, MSSQL Server, Oracle и других БД. DBToolsManager представлен в двух вариантах в бесплатном (Standard) и платном варианте (Enterprise).[5]

Рекомендуемыесистемныетребования:CPU1.0 GHZ or higher, RAM2 GB or higher, Display1024×768.

Интерфейс инструмента достаточно прост и удобен, все необходимые элементы эргономично расположены в рабочей области. Новичкам это позволит быстро адаптироваться к сервису.

Безопасность включает управление потоками данных, обеспечение безопасного импорта и экспорта данных.

DBToolsManager представлен в бесплатном (Standard) и платном варианте (Enterprise). Стоимость составляет 69.90 долл. США за одну лицензию.[5]

Достоинства данного продукта:

— управление базами данных, таблицами;
— наличие мастера создания форм и отчетов;
— Удобный импорт/экспорт данных из различных источников, среди которых MSAccess, MSExcel, Paradox, FoxPro, DBF, ODBC таблицы, текстовые и XML файлы;
— конструктор диаграмм и другие возможности.

MyDBStudio —инструмент для администрирования баз данных MySQL. Позволяет выполнять все необходимые действия, такие как: создавать, редактировать и удалять записи, таблицы и базы данных. Работает исключительно на платформе Windows.

Рекомендуемыесистемныетребования:CPUDualCore 2GHz or higher, RAM2 GBor higher, Display1920×1200 or higher.

Интерфейс приложения MyDBStudio позволяет переключаться между данными и режимом редактирования. Всё это быстро осуществляется посредством древовидного формата «база данных > таблица > колонки».[6]

BMyDBStudio легко настроить привилегии пользователей и их групп, администрировать учетные записи и отслеживать все изменения посредством журнализации. Это позволит обеспечить минимально необходимый уровень безопасности используемой базы данных.

Стоит отметить, что данный сервисявляется бесплатным ина текущий момент одним из самых востребованных на рынке инструментов по созданию баз данных MySQL.

Данный успех обусловлен следующими преимуществами:

— Количество данных к которым возможно подключиться неограниченно;
— Возможность подключения по SSH каналам;
— Существует функция создание откатов и экспорт БД в различные форматы;

dbForgeStudio—является универсальным инструментом для работы с MySQL сервером.

Рекомендуемые системные требования:CPUПроцессор с тактовой частотой 2 ГГц и выше, RAM1024 МБorhigher

С помощью элементов интерфейса разработчики и администраторы баз данных MySQL могут создавать и выполнять запросы, разрабатывать и отлаживать процедуры и функции, а также автоматизировать управление прочими объектами базы данных. Дополнительно содержит инструменты для сравнения, синхронизации, создания резервных копий базы данных по графику, а также для анализа и создания отчетов по данным таблиц MySQL.

dbForgeStudioforMySQL поддерживает все версии серверов MariaDB и все типы данных, которые представлены в MariaDB. Существует как бесплатная, так и платная версии программы. [7]

Достоинства:

— есть возможность централизованного администрирования;
— присутствуют инструменты, позволяющие сравнивать БД;
— визуальный профилировщик запросов;
— присутствует дизайнер БД, позволяющий строить визуальные диаграммы;

HeidiSQL— инструмент, поддерживающий ssh туннели, с возможностью синхронизировать структуры баз данных, управлять таблицами, просматривать и редактировать записи, управлять привилегиями пользователей, импортировать данные.

Рекомендуемые системные требования:CPUPentium III, Athlon или болеесовременные, RAM4 GB or higher, Display1024×768

Безопасность при работе с базой данныхдостигается с помощьюуправления пользователями и привилегиями, мониторингом и закрытием клиентскихпроцессов, атак же ведением журнализации.

HeidiSQL является бесплатным вплоть до последней версии9.1.0.4867.[8]

Достоинства.

— возможность подключаться к серверу с помощью командной строки;
— возможность пакетной оптимизации и восстановления таблиц;
— возможность редактирования столбцов, индексов и внешних ключей таблиц, редактирование тела и параметров SQL процедур, триггеров и др.;
— присутствует возможность синхронизации таблиц БД между различными базами данных и другие возможности. [1]

Ключевые характеристики программных продуктов удобно сравнивать в виде таблицы (8).

Таблица 1. Характеристики программных продуктов

приложение\критерий	Мультиплатформенность	Мин. Системные требования	интуитивный интерфейс	Конструкторы запросов	Конструкторы хран.процедур	HTTPS	пользователи и роли
MySQL Workbench	+	-	+	+	-	+	+
phpMyAdmin	+	+	+	+	+	+	+
Ar-wik Builder	+	-	+	+	-	-	-
DBTools Manager	-	-	+	+	+	-	-
dbForge Studio for MySQL	-	-	+	+	+	+	+
MyDB Studio	-	-	+	+	-	-	+
Heidi SQL	-	-	-	+	+	+	+

Как видим наиболее удобным, универсальным и функциональным средствомявляетсяphpMyAdmin. Минимальные системные требования, мультиплатформенность, бесплатность, открытость исходного кода и весь необходимый набор инструментов для работы и обеспечения безопасности есть только в данном продукте. Для пользователей операционных систем семейства Windows так же стоит отметить dbForgeStudioforMySQL, но к сожалению часть функций системы доступны только в платной версии. С точки зрения безопасности, правильным выбором могут стать такие продукты, какMySQLWorkbenchи Heidi SQL.

Литература.

[1]. Электронныйпортал http://habrahabr.ru/post/142385/

[2]. Сайтпроизводителя[Электронный ресурс] // http://dev.mysql.com /downloads/workbench/

[3]. Сайтпроизводителя[Электронный ресурс] // http://only-free-soft.ru/web-development/server-and-components/169-phpmyadmin.html

[4]. Сайтпроизводителя[Электронный ресурс] // http://ar-wik.com /builder/documentation

[5]. Сайтпроизводителя[Электронный ресурс] // http://www.dbtools.com.br/EN/dbmanagerpro/

[6]. Сайтпроизводителя[Электронный ресурс] // https://www.devart.com /ru/dbforge/mysql/studio/

[7]. Сайтпроизводителя[Электронный ресурс] // http://www.mydb-studio.com/

[8]. Сайтпроизводителя[Электронный ресурс] // http://www.heidisql.com/#featurelist

Молчанов Алексей Николаевич – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

Аверьянов Дмитрий Александрович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: overdmit@yandex.ru

Лагутин Юрий Юрьевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: lagutin.yurik2@gmail.com

В.А. Бессонов, М.К. Савкин

ОБЗОР ИНТЕРАКТИВНОГО ДИЗАССЕМБЛЕРА «IDA PRO»

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Во времена быстроразвивающейся программной индустрииважным аспектом является информационная безопасность разработанного программного обеспечения.В связи с этим возникает задача анализа угрози необходимость иметь представление о том, как устроены вирусы и руткиты. Их изучение становится возможным с использованием принципов обратной разработки.Данная задача может быть решена с использованием дизассемблераIDAPro.

Основным способомизучения программ без их исходных кодов является дизассемблирование– процесс преобразования двоичного кода процессора в исходный код программы на языке ассемблера. Так как ассемблирование является процессом с потерей данных, то полное восстановление исходных кодов программы невозможно.

Одной из основных проблем дизассемблирования является синтаксическая неотличимость адресов от констант[1]. В настоящее время не существует полностью автоматического дизассемблера, способногобезошибочно выдавать работоспособный код программы, поэтому его необходимо корректировать человеку.

Процесс дизассемблированияможе быть автономными интерактивным.

До начала автономного дизассемблирования пользователь должен задать все указания для дизассемблера, так как в дальнейшем он не позволяет вмешиваться в сам процесс[1]. Такой подход менее эффективен, так как конечный результат может оказаться неудовлетворительным и тогда, пользователь должен вручную исправлять полученный код или указать дизассемблеру на его ошибки и проделать всю процедуру вновь.

Интерактивный дизассемблер имеет удобный графический интерфейс, с помощью которого пользователь вручную корректирует поведение анализатора при обработке сложных участков кода. Например, пользователь может указать анализатору, является ли то или иное число адресом или константой.

Интерактивный дизассемблер более гибок по сравнению с автономным.Если при автономном дизассемблировании пользователь может только довольствоваться полученным листингом программы, то интерактивный создает все условия для изучения программы и получения более корректного листингаво время дизассемблирования.IDA имеет великолепную навигационную систему. Многооконный интерфейс позволяет одновременно наблюдать несколько фрагментов программы, то есть изучая работу программы мы можем наблюдать за каждым её шагом, изменением и поведением [2].

IDA – интерактивный дизассемблер и отладчик, работающий под управление операционных систем Windowsи Linux[3]. Это рабочая среда,

имеющая развитый интерфейс и множество удобных средств для разбора и изучения кода и структуры дизассемблированной программыПроцесс анализа кода в IDA ориентирован на постоянное взаимодействие с пользователем и в зависимости от решаемой задачи может протекать по-разному.Например, IDAимеет развитую навигационную систему. Многооконный интерфейс позволяет одновременно наблюдать несколько фрагментов программы – при этом результаты изменений, сделанные в одном из окон, тут же отображаются во всех остальных [2].IDAможет быть использована не только для анализа вирусов, троянов и других вредоносных программ, но и для оптимизации и поиска ошибок в легитимном программном обеспечении [4].

Программа имеет следующие отличительные особенности:

— развитая система навигации;
— система типов и параметров функции;
— встроенный язык программирования IDC;
— открытая и модульная архитектура;
— поддержка популярных процессоров и форматов файлов;
— встроенный отладчик для Win32;
— работа со структурами данных высокого уровня.

Интерактивный дизассемблер IDAPro является самой лучшей программой для дизассемблирования. Так как IDAPro является средой, ориентированной на качественное изучение программ, их дизассемблирования и анализ полученных кодов, пользователи IDAPro имеют большие возможности в изучении алгоритмов программ, поиска её слабых сторон. Такие условия позволяют активно совместно работать пользователю и IDAPro как одно целое, добиваясь выполнения труднодостижимых задач.Опыт работы с IDAPro позволяет разработать защиту для простых и сложных программ, понять, как устроены вирусы и другие вредоносные программы.

Литература

[1]. Крис КасперскиОбраз мышления – дизассемблер Том 1. Москва, СОЛОН-Р, 2001, 480 стр. (дата обращения: 10.10.2015)

[2]. IDA Pro - самый мощный дизассемблер в мире URL: http://www.idasoft.ru/disassembler/ (дата обращения: 18.10.2015)

[3]. Музыченко Е. Интерактивный дизассемблер IDAURL: http://eugene.muzychenko.net/articles/software/ida.htm (дата обращения: 24.10.2015)

[4]. IDAURL: https://ru.wikipedia.org/wiki/IDA (дата обращения: 10.10.2015)

Бессонов Валентин Андреевич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: valentbesson@gmail.com

Савкин Михаил Константинович – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

Я.А. Бланк, А.Б. Лачихина

ОБЗОР ПРОДУКТОВ ДЛЯ АВТОМАТИЧЕСКОГО ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ КОМПЬЮТЕРА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

С момента создания первого компьютера и до сегодняшнего дня обеспечение информационной безопасности остается одной из самых актуальных проблем, с которой так или иначе сталкиваются как пользователи персональных компьютеров, так и пользователи компьютерных систем. С развитием вычислительной техники и информационных технологий увеличивается сложность систем защиты информации. Конкуренция между предприятиями ставит вопрос информационной безопасности на первый план. Можно утверждать, что информация превратилась в стратегический ресурс. Угрозой считается возможность возникновения такой ситуации, явления или события, следствием которой может стать нарушение безопасности информации. Угрозой для информации могут являться вредоносное программное обеспечение, сбой оборудования, перебои в электропитании, помехи, некомпетентность самого пользователя и многое другое. Таким образом, обеспечение защиты информационной безопасности является задачей первостепенной важности.

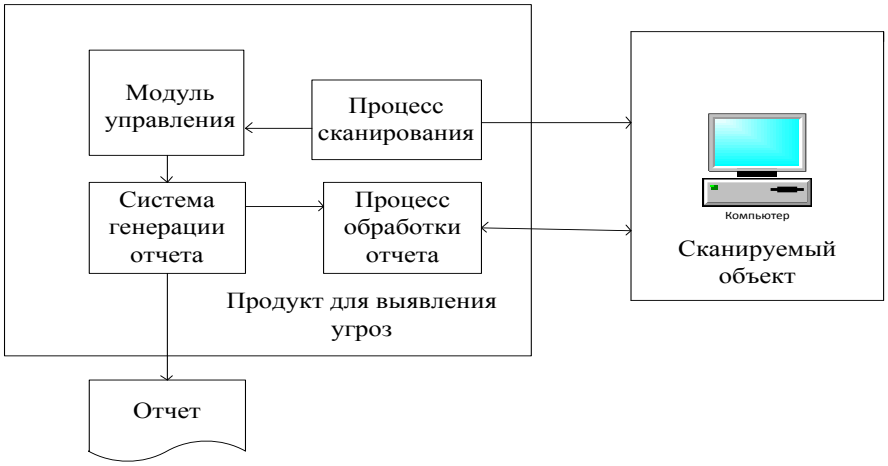


Рис.1 Общая схема проведения анализа уязвимостей

Важной составляющей информационной безопасности является проверка того, насколько реализованные или используемые механизмы защиты информации соответствуют положениям принятой политики безопасности, т.е. проверка системы на наличие уязвимостей, которыми может воспользоваться злоумышленник для реализации атаки. Данную проверку можно проводить вручную, однако, данный подход требует много времени и не исключает ошибки вследствие человеческого фактора. Поэтому целесообразнее использовать продукты для автоматического выявления уязвимостей.

Internet Scanner. Система анализа защищенности Internet Scanner разработана американской компанией Internet Security Systems, Inc. Компания была приобретена IBM в 2006 году. При помощи данного продукта можно проводить регулярные всесторонние или выборочные проверки операционных систем, сетевых сервисов, распространенного прикладного программного обеспечения, маршрутизаторов, межсетевых экранов, Web-серверов и пр. На основе сделанной проверки Internet Scanner создает отчет с описанием обнаруженных угроз и возможных способов их устранения. Система Internet Scanner может быть применена как к персональным компьютерам, так и компьютерам, подключенным к глобальной или локальной сети. Из возможностей можно отметить:

— невысокие системные требования к программному и аппаратному обеспечению;
— функционирование под управлением многих операционных систем;
— параллельное сканирование до 128 сетевых устройств и систем;
— использование протокола ODBC (Open Database Connectivity), вся информация о сканирование сохраняется в базе данных;
— простота использования и графический интерфейс, интуитивно понятный даже простому пользователю;
— централизованное управление процессом сканирования.

Пользователь может выбирать глубину сканирования из четырех предложенных (Light, Medium, Heavy, OS Identification) или же создать свой собственный вариант, который можно сохранить для последующего использования.

Алгоритм использования Internet Scanner включает в себя 4 этапа:

— задание глубины сканирования;
— выбор сканируемых узлов;
— запуск процесса сканирования;
— генерация и анализ отчета.

Отчеты можно создавать в различных форматах (текстовый, HTML, графическая карта сети (Network Map), содержащая данные об узлах сети и имеющихся на них уязвимостях).

XSpider. Частная программа-сканер уязвимостей, выпускаемая российской фирмой Positive Technologies. Ранее продукт являлся бесплатным, начиная с версии 7.0, выпущенной летом 2003 года, стал платным. XSpider может быть установлен на любую ОС семейства Windows.

XSpider может в полностью автоматическом режиме проверять компьютеры на предмет обнаружения уязвимостей. База уязвимостей постоянно пополняется специалистами Positive Technologies, что в сумме с автоматическим обновлением баз и модулей программы постоянно поддерживает актуальность XSpider.

Особенностями XSpider являются:

— низкие аппаратные требования;
— ведение полной истории проверок, что позволяет оценить объем сделанной работы и контролировать текущего состояния безопасности, охраняемого объекта;

— одновременное сканирование большого числа компьютеров до 10000 хостов для версии 7.8 (ограничивается, как правило, скоростью сетевого канала);
— возможность гибко настраивать сканирование: от регулярного аудита до выполнения комплексных проверок.

Этапы сканирования:

1. Сканирование портов

Сканируются либо порты из списка, используемого XSpider по умолчанию, и составленного экспертами Positive Technologies, либо порты из списка, определенного самим пользователем.

2. Идентификация сервисов

На этом этапе производится определение конкретного сервиса, установленного на том или ином порту.

3. Определение уязвимостей

Завершающий этап, на котором формируется окончательный результат работы сканера, качество которого зависит не только от результатов работы предыдущих этапов, но и от подходов, использующихся собственно при определении уязвимостей;

4. Создание отчета.

Nessus. Проект был основан в 1998 компанией Tenable Network Security. Первоначально являлся программным обеспечением с открытым исходным кодом. В октябре 2005 года компания приняла решение закрыть исходный код приложения и сделать его проприетарным. Исходный код Nessus 2 послужил основой проекта отрытого сканера уязвимостей OpenVAS. Последняя на сегодняшний день версия 6.3.4

Nessus обладает следующими характерными чертами:

— программа не имеет графического интерфейса в привычном его виде, а управляется через веб-интерфейс;
— открытость сценариев тестирования;
— реализован специальный скриптовый язык— **NASL (Nessus Attack Scripting Language)** для написания собственных тестов на проникновения;
— практически ежедневное обновление баз данных возможных уязвимостей;
— сохранение результатов сканирования в базе данных и возможность их последующего использования;
— сохранение и последующая загрузка сессии сканирования, если процесс сканирования не был завершен в первый раз.

Nessus является кроссплатформенным программным обеспечением, но зная, какая именно операционная система установлена на сканируемом узле, можно ускорить процедуру сканирования выбором только актуальных для этой системы тестов.

Алгоритм работы Nessus:

1. оператор задает некоторый набор IP-адресов или DNS-имен сканируемых узлов;

2. производится проверку доступности данного узла;

3. идентификация открытых портов и определение запущенных сетевых сервисов;

4. используя базу данных уязвимостей проверяются уязвимости сетевых сервисов, поочередно применяя тесты, подходящие для данного выбранного сервиса;

5. генерация отчета о сканировании.

В случае если в сканируемом объекте обнаружена уязвимость, отчет будет содержать следующие пункты: «Synopsis» — краткий обзор уязвимости, «Description» — ее описание, «Solution» — ссылка на web-страницу с детальным описанием уязвимости и мер, которые необходимо предпринять для ее устранения, «Risk Factor» — информация о степени опасности данной уязвимости и ссылки на эту уязвимость в различных базах данных уязвимостей.

При использовании продуктов для автоматического выявления уязвимостей компьютера проверяющий должен соблюдать повышенную осторожность, так как при тестировании они могут реализовывать атаки на уязвимые системы, что может спровоцировать нарушение нормальной работоспособности системы. Также важно знать, что данные продукты могут использоваться и злоумышленниками для выявления уязвимостей объектов с целью последующей атаки на них. В заключении стоит отметить, что в процессе контроля защищённости компьютерных систем следует использовать хотя бы 2 специализированных программных продукта.

Таблица 1. Сравнительная характеристика сканеров уязвимостей

Критерий сравнения	Internet Scanner	XSpider	Nessus
1.Поддерживаемые системы	Кроссплатформенное программное обеспечение (ПО)	Windows2000/XP/2003/Vista/7	Кроссплатформенное ПО
2.Сертификация	2 сентября 1998 сертификат Государственной технической комиссии при Президенте РФ № 195	Сертификат соответствия ФСТЭК России № 2530 от 26 декабря 2011 г.	18 сентября 2000 сертификат Государственной технической комиссии при Президенте РФ № 361
3.Цена	Стоимость варьируется в зависимости от количества IP адресов	Платный, стоимость варьируется в зависимости от кол-ва IP-адресов (от 8000 руб. за 4 хоста до 1 000 000 руб. за 10000 хостов)	2190$/год Имеется и бесплатная версия, отличающаяся регулярностью обновлений

4.Интерфейс	Интуитивно понятный графический интерфейс	Удобный и наглядный многооконный графический интерфейс	Веб-интерфейс
5.Отчет	Имеет текстовый, DIF (Data Inter-change Format), HTML, Micro-soft Word форматы	Отчеты с различными уровнями их детализации	Отчет, содержит характеристики найденных угроз, в том числе ее индекс в в базе данных CVE (Common Vulnerabilities and Exposures). Возможность сохранения отчетов в форматах nessus (xml), pdf, html,csv, nessus DB
6. Частота обновления	Регулярные обновления	Ежедневные обновления	Еженедельные обновления для пользователей бесплатной версии. практически ежедневные обновления для пользователей платной версии

Список литературы

[1]. *Хорошко В.А, Чекатков А.А.* Методы и средства защиты информации. К.: Юниор, 2003. — 504 с.

[2]. Сайт организации «Positive Technologies» Электронный ресурс. http://www.ptsecurity.ru/xs7/

[3]. Информационный ресурс citforum
http://citforum.ru/internet/securities/internet_scan.shtml

[4]. John Wack, Miles Tracy, Murugiah Souppaya Guideline on Network Security Testing. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 2003

Бланк Яна Андреевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: yanablank10@gmail.com

Лачихина Анастасия Борисовна – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

Т.С. Белова, А.Б. Лачихина

ОБЗОР СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Уже в течение нескольких десятилетий исследуются способы обнаружения всевозможных атак на объекты информации. Анализируются признаки вторжений, разрабатываются и эксплуатируются методы и средства обнаружения попыток несанкционированного проникновения через системы защиты, как межсетевой, так и локальной(как на логическом, так и на физическом уровнях).

Исследования в этом направлении были начаты в 1980 г. Джеймсом Андерсоном. Свои основные взгляды он изложил в статье "Мониторинг угроз компьютерной безопасности". А в 1987 г. данное направление было доработано Дороти Деннинг, в опубликованной еюстатье "О модели обнаружения вторжения".Были предложены различные методы, вдохновившие многих исследователей и заложившие основу для создания коммерческих продуктов в области обнаружения угроз.

Распознавание атак – одна из главных целей использования системы обнаружения вторжений. Данная система запрограммирована на поиск определенных типов событий, которые служат признаками атак.

Один из важнейших механизмов информационной безопасности сетей любого современного предприятия - системы обнаружения вторжений (СОВ). Увеличение количество атак на объекты информации, привело к тому, что системы обнаружения вторжения стали ключевым компонентом любой стратегии сетевой защиты. Благодаря улучшению качества и совместимости программ, за последние несколько лет их популярность значительно возросла.

Основные элементы СОВ следующие:

— Детекторная подсистема, которая накапливающая события сети или компьютерной системы;
— Подсистема анализа, обнаруживающаякибер-атаки и сомнительную активность;
— Хранилище для накопления информации о событиях, а также результаты анализа кибер-атак и несанкционированных воздействий;
— Консоль управления, при помощи которой можно задавать параметры СОВ, следить за состоянием сети (или компьютерной системы), иметь доступ к информации об обнаруженных подсистемах анализа атаки и неправомерных действий.

Рис.1 Связь между основными элементами локальной архитектуры СОВ

Существуют несколько подвидов СОВ:

1. Подвиды по способу мониторинга

— Узловаясистемаобнаруженияторжений (*Host-basedintrusiondetectionsystem, HIDS*). Располагается на отдельном узле и отслеживает признаки атак на данный узел.

— Сетевая система обнаружения вторжений (*network intrusion detection system,* NIDS). Находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети.

2. Подвиды IDS по методам выявления атак

— Системы обнаружения вторжений на основе политик.Создание правил сетевой безопасности

— Системы обнаружения вторжений на основе сигнатуры. Выявляет деятельность, которая соответствует предопределенному набору событий, уникальноописывающих известное нападение.

— Системы обнаружения вторжений на основе выявления аномалий.обнаруживают нападения, идентифицируя необычное поведение (аномалии) на сервере или в сети

Таблица 1. Возможности СОВ

Возможности СОВ	
Могут	Не могут
— повысить защищенность сети; — проводить мониторинг сетевого трафика за межсетевым экраном; — проверять содержимое сетевого сообщения и определять тип атаки; — выявлять изменения в файлах и директориях; выявлять необычное время и тип доступа к ресурсам.	— обеспечить полную защищенность сети

Наиболее распространенные СОВ**:**

— СОВ, встроенныев прокси-серверы и брандмауэры (KerioWinRouteFirewall или Microsoft ISA Server). Несмотря на малую функциональность, т.е. в них встроено всего несколько правил обнаружения вторжений (например, на сканирование портов), такое решение может успешно применяться для немедленного реагирования на нападения;

— Система SNORT. Изначально созданнаяпод Unix, немного позже была перенесена и под платформу Windows. Преимущества SNORT - это надежность, большое количество документации и дополнительных утилит, а также бесплатное использование. Недостатки–это сложностипри установке и настройке, а также то, что программа требует большого количества компонентов, которые необходимо устанавливать отдельно (Apache, Perl, mySQL и т.п.).

— Коммерческие системы обнаружения вторжений. Они являются очень дорогими, но чрезвычайно мощными, с автоматически обновляемыми сигнатурами атак. Примерами данных систем могут служить McAfee Entercept или ETrust Intrusion Detection фирмы Computer Associates.

— Персональные системы обнаружения атак. Они предназначены для защиты единственного рабочего компьютера, просты в настройке и нересурсоемки. К одной из программ такого рода можно отнести Internet Periscope. Кроме обнаружения вторжений, данная система умеет также в автоматическом режиме находить сведения о домене и IP-сети, из которой пришел злоумышленник, показывать координаты для контактов его провайдера и т.п.

— Специальные программы, которые проводят не анализ сетевого трафика, а постоянный мониторинг журналов событий Windows. Примером таких систем является GFI SELM.

— Аппаратные системы обнаружения вторжений, зачастую объединенные с аппаратными брандмауэрами. Наиболее распространены такие устройства фирм CheckPoint и NetScreen.

В настоящее время защита, обеспечиваемая брандмауэром и антивирусами, уже не достаточно эффективна против сетевых атак и вредоносных ПО. Поэтому на первый план выходят СОВ, которые могут обнаруживать и блокировать как известные, так и еще не известные угрозы.

Таким образом, СОВ – это одно из средств хорошей архитектуры обеспечения безопасности сети и многоуровневой стратегии её защиты. Она имеет как преимущества, так и недостатки. Но не стоит забывать, что первые можно улучшить, а последние устранить, применяя СОВсовместно с другими средствами обеспечения безопасности информации.

Список литературы

[1]. *П. Покровский*. Развертывание системы обнаружения вторжений. «LAN», № 6/2003 .

[2]. *Милославская Н.Г., Толстой А.И.* Интрасети: обнаружение вторжений. М.:ЮНИТИ-ДАНА, 2001.

[3]. Информационный ресурс it-sector URL: http://it-sektor.ru/obnaruzhenie-vtorzheniyi.html

[4]. Информационный ресурс askit. URL: http://www.askit.ru/custom/win2003_sec/m3/03_04_ids_honeypots.htm

[5]. Информационный ресурс FB. URL: http://fb.ru/article/186268/ids---chto-eto-takoe-sistema-obnarujeniya-vtorjeniy-ids-kak-rabotaet

Белова Татьяна Сергеевна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: tanya.belova19@yandex.ru

Лачихина Анастасия Борисовна – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

М.А. Хорошилова, О.Ю. Жарова

ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ С ГЛОБАЛЬНОЙ СЕТЬЮ INTERNET

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Мы живем в мире высокоразвитых информационных технологий, одной из которых является глобальная компьютерная сеть передачи данных - Internet. На настоящий момент времени данная технология проникла почти во все аспекты человеческой жизни и используется повсеместно, для поиска информации, общения, работы, отдыха.С каждым годом сеть Internetразвивается, увеличивает свой функционал, улучшая тем самым нам жизнь, но в то же время «нахождение» в сети становится все более небезопасным вследствие негативных действий мошенников и кибер-преступников, которые могут привести к утечке, повреждению целостности или уничтожению персональных данных, краху компьютерной системы или некорректной её работ, а также слежке.

Для того чтобы такого не произошло, необходимо соблюдать несколько простых правил при работе с сетью. Первое и самое главное правило - перед тем как начать изучать просторы Internet установите себе антивирусное программное обеспечение с компонентом «Проактивной защиты», который сможет предотвратить заражение компьютера трояном или вирусом, отследив момент проникновения этого вредоносного ПО в систему и заблокировав его. Таким образом, можно избежать проблем, связанных с восстановлением работоспособности системы после вирусной атаки.Также для более эффективной работы антивирусного ПОнужно периодически обновлять его базы. Это можно сделать вручную, когда будет удобно, или автоматически, тогда при появлении обновлений программа сама загрузит новые данные.

Второе не менее важное правило – следите за выходом новых обновлений для вашей операционной системы и интернет браузера. Своевременное их обновление поможет устранить уязвимости, допущенные производителем в предыдущих версиях ПО и выявившиеся в результате столкновения с новыми вирусами. Это увеличит стойкость системы к вредоносному ПО.

Следующее, что необходимо сделать - это правильно настроить систему и её содержащиеся в ней пользовательские приложения против вредоносных программ: запретить автоматический запуск приложений, распаковку архивов, поставить фильтры на сайты, принимаемые на почте сообщения. Это уменьшит риск воздействия вирусов и подверженность сетевым атакам.

Если вы пользуетесь wi-ficетью, её следует зашифровать и сделать скрытой. На сегодня лучшим доступным стандартом шифрования считается WPA2. Также не будет лишним сменить стандартный IP-адресроутера на любой другой возможный.

Желательно выполнять выход в Internetиз-под учетной записи, не имеющих прав администратора.Хотя это доставляет некоторые неудобство при установке новых программ и работе с системой, такой подход значительно повысит её безопасность. В этом случае при заражении вирус не получит неограниченных прав доступа к содержимому компьютера и ущерб им причиненный будет минимальным.

Регулярно делайте резервные копии важной информации на портативный носитель. Заведите и держите при себе системный загрузочный диск, с которого в случае потенциального заражения системы можно будет загрузиться и проверить антивирусной программой.

Никогда не храните свои персональные данные и пароли от социальных сетей, почтовых ящиков и уж тем более от онлайн банков в текстовых файлах на компьютере. При попадании вируса в систему эти данные в лучшем случае пропадут, в худшем будут незаметно пересланы злоумышленнику и использованы по его усмотрению. Записывайте всю учетную информацию в бумажный блокнот, чтобы иметь возможность зайти под своим аккаунтом, даже если вы забудете пароль.

Теперь перейдем к правилам взаимодействия с с глобальной сетью и браузером. Одним из сервисов Internet является электронная почта, через которую злоумышленник может нанести удар по системе. Никогда не переходите по ссылкам в сообщениях почты от неизвестного вам адресата, так как скорее всего такая гиперссылка перебросит на сайт с хранящейся там вредоносной программой. Так же не стоит запускать исполняемые файлы, вложенные в письма, даже если они отправлены со знакомого адреса, потому как большая часть данных, пересылаемых по почте, это документы, видео- и аудио файлы, но не программы. Текстовые сообщения, которые вызывают подозрения, рекомендуется читать в режиме быстрого просмотра, сделав один щелчок мышкой на письме в списке. В этом случае его содержание выведется в основном окне программы, а не будет открывать новое. Но лучше такие сообщения сразу удалять.

Обращайте внимание на расширение присланных файлов. Большую опасность могу представлять файлы с расширениями: *.ade, *.adp, *.bas, *.chm, *.com, *.cpl, *.crt, *.eml, *.hlp, *.hta, *.inf, *.ins, *.isp, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.pcd, *.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vbs,*.vbe, *.wsf, *.wsh, *.wsc. Для просмотра реального расширения в системе необходимо настроить режим отображения расширений файлов.

Далее о том, что можно и нельзя делать, непосредственноработая с сайтами сети Internet. Во-первых, не следует кликать по баннерам с рекламой, неважно с какой целью вы это делаете, для просмотра рекламной информации или чтобы убрать закрывающее половину экрана окно (рис. 1). И в том и в другом случае данное действие,скорее всего,приведет к желаемому результату, но может активировать вирус, который в последствие нанесет вред системе.

Рисунок 1. Пример рекламных баннеров

Аналогичная ситуация обстоит с выделением текста зараженныхсайтах. Код страницы может содержать java-script, который при взаимодействии пользователя с фрагментом текста среагирует как гиперссылка и перейдет на другой сайт с возможно вредоносным содержанием.

Если все же вы случайно или преднамеренно кликнули по вредоносному баннеру, в результате чего компьютер был заблокировани появилось сообщение с вымогательством денег, никогда не переводите денежные средства на указанный номер, кода разблокировки вы не получите (рисунок 2). В этом случае можно обратиться к сайтам производителей антивирусного ПО, на которых по представленным в сообщении данным подбирается подходящий код разблокировки системы.

Рисунок 2. Пример вируса-вымогателя

Прежде чем перейти по ссылке, обратите внимание на её адрес.Если он ведет на сайт с доменом третьего уровня (например, vkontakte-fotos.h16.ru) – то это не внушает доверия и не следует использовать данную ссылку. То же самое относится к «сокращателям ссылок». Если ссылка стоит на подозрительном сайте и, к тому же, сокращена (например, до вида goo.gle/1fg45) – то лучше по ней не переходить.

Если для просмотра или загрузки какой-либо информации, например, фильма, на странице неизвестного сайта, вас просят ввести свои паспортные данные, адрес проживания или телефон, этого делать не следует. Если же вы попались на уловку и ввели номер телефона, в результате чего со счета были сняты деньги – свяжитесь со своим сотовым оператором и отключите появившиеся на номере услуги и сервисы.

При загрузке файлов из Internet из ненадежных источников никогда не устанавливайте и не сохраняйте их без обязательной проверки антивирусной программой. Подозрительные файлы лучше сразу удалить. По возможностихотя бы раз в месяц проверяйте компьютер полностью.

При регистрации на сайтах составляйте сложные пароли, то есть состоящие не менее чем из 11 символов и включающие в себя цифры и буквы разных регистров, а лучше алфавитов. Регулярно меняйте пароли при появлении подозрении, что пароль был перехвачен, либо хотя бы раз в год.Вводить изменения следует после обновления антивирусного ПО и поверки всего компьютера. Это снизит риск утечки нового пароля из-за активности вредоносных программ.

Если приходится работать с чужого или публичного компьютера – удаляйте историю за тот период времени, что вы им пользовались. Перед вводом своих учетных данных отключите функцию автоматического сохранения личной информации в используемом браузере.

Выполнения данных рекомендаций повысит уровень безопасности системы в целом и поможет снизить риск заражения вирусом и утечки персональной информации при работе с глобальной сетью Internet.

Литература

[1]. Sobinam. URL: http://sobinam.ru/blog/better_world/154.html/ (дата обращения: 20.10.2015)

[2]. Фиабанк. URL: http://www.fiabank.ru/safety/4/(дата обращения: 19.10.2015)

[3]. Организационная безопасность. URL: http://www.orgpsiholog.ru/pr.bezop.htm(дата обращения: 20.10.2015)

Хорошилова Мария Александровна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: mary.hory@yandex.ru

Жарова Ольга Юрьевна – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: ouzharova@yandex.ru

Е.И. Антипова, М.К. Савкин

ПРИНЦИПЫ АТАКИ ВНЕДРЕНИЯ SQL

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Для написания web-приложений часто применяются базы данных. Их использование наиболее уместно для хранения пользовательских регистрационных данных, идентификаторов сессий, организации поиска, а также других задач, требующих обработки большого количества данных. Для обращения к БД используются серверные технологии: PHP, PERL, ASP, и т.д.Многие web-страницы для обработки пользовательских данных формируют специальные SQL-запросы к БД.Из-за недостаточнойпроверки и некорректной обработки данных, которые передаются от пользователя, возникает уязвимость типа внедренияSQL, дающая возможность злоумышленникам выполнять непредвиденныекодом программы SQL-запросы, например, чтение содержимого любых таблиц или удаление всех данных. Этоттип уязвимости распространен по всему интернету, ивзломы часто происходят именно благодаряэтому дефекту. При разработке сайтов и прикладных программ, работающих с базами данных, необходимо знать о таких уязвимостях и принимать меры противодействия инъекциям SQL. В данной работе исследованы возможные методы атаки типа внедрения SQL для дальнейшего анализа способов защиты от них.

Основная форма атаки SQL Injectioncостоит в прямой вставке кода в пользовательские входные переменные, которые объединяются с командами SQL и выполняются. Менее явная атака внедряет небезопасный код в строки, предназначенные для хранения в таблице или в виде метаданных. Когда впоследствии сохраненные строки объединяются с динамической командой SQL, происходит выполнение небезопасного кода [1].

Атака осуществляется посредством преждевременного завершения текстовой строки и присоединения к ней новой команды. Поскольку к вставленной команде перед выполнением могут быть добавлены дополнительные строки, злоумышленник заканчивает внедряемую строку меткой комментария «--». Весь последующий текст во время выполнения не учитывается.

Следующий сценарий показывает простую атаку внедренияSQL в строковые параметры. Сценарий формирует SQL-запрос, выполняя объединение жестко запрограммированных строк со строкой, введенной пользователем:

```
varShipcity;
ShipCity = Request.form ("ShipCity");
varsql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

Пользователю выводится запрос на ввод названия города. Если пользователь вводит Redmond, то запрос, построенный с помощью сценария,будет следующим:

SELECT * FROM OrdersTable WHERE ShipCity = 'Redmond';drop table OrdersTable--'

Если измененный код будет синтаксически правилен, то он будет выполнен сервером.

Для разделения команд в языке SQL используется символ **;** (*точка с запятой*). Внедряя этот символ в запрос, злоумышленник получает возможность выполнить несколько команд в одном запросе, однако не все диалекты SQL поддерживают такую возможность[2].Если в параметры скриптазлоумышленником передается конструкция, содержащая точку с запятой, например *12;INSERT INTO admin (username, password) VALUES ('HaCkEr', 'foo');*то в одном запросе будут выполнены 2 команды:

SELECT * FROM news WHERE id_news = 12;
INSERT INTO admin (username, password) VALUES ('HaCkEr', 'foo');

Таким образом, в таблицу будет несанкционированно добавлена запись.

Использование оператора UNION позволяет объединить результаты выполнения двух или более запросов SELECT. Данная техника заключается в добавлении нужного запроса SELECT при помощи оператора UNION к первоначальному запросу [3]. Для корректности результирующего запроса, полученного при помощи оператора UNION, необходимо, чтобы удвух выражений SELECT совпадало количество итип столбцов результата. В противном случае СУБД сгенерирует исключение. Взависимости от логики работы приложения либо будет выведено сообщение овозникшем при работе сСУБД исключением, либо страница отобразится пользователю некорректно.Первоначально злоумышленник перебором определяет количество аргументов вSQL-запросе. Универсальным методом определения количества аргументов является использование оператора сортировки ORDER BY.

Для определения количества аргументов вкачестве уязвимого строкового параметра передаются последовательно следующие значения [4]:

SELECT * FROM members WHERE name = -1 ORDER BY 1 # Успешно

SELECT * FROM members WHERE name = -1 ORDER BY 2 # Успешно

SELECT * FROM members WHERE name = -1 ORDER BY 3 # Ошибка

Таким образом, количество аргументов в SQL-запросе равно двум. Напрактике применяется не линейный, а бинарный поиск.

После определения количества аргументов перебором определяется, для каких аргументов задано ограничение *notnull*итип этих аргументов (числовой, строковый или дата). В качестве остальных аргументов передается *null*.

UNIONSELECT ‘test’, null, nullFROMdual #Возникло исключение
UNION SELECT null, ‘test’, null FROM dual#Запрос выполнен

После определения количества аргументов и определения ненулевых аргументов (*notnull*), атакже их типов (числовой, строковый и дата), в качестве второго параметра злоумышленник передает нужный SQL-запрос, который должен возвращать строку [3].

Дляполучения хэша пароля пользователя SYS из таблицы dba_users можно передать следующее выражение в качестве уязвимого строкового параметра:

‘UNION SELECT null, (SELECT username ||‘--’|| password FROM dba_users WHERE username = ‘SYS’), null FROM dual

Зачастую, SQL-запросимеет структуру, усложняющую или препятствующую использованию UNION.

$res = mysql_query("SELECT author FROM news WHERE id=" . $_REQUEST['id'] ." AND author LIKE ('a%')");

Этот скрипт отображает имя автора новости по передаваемому идентификатору id только при условии, что имя начинается с буквы a, и внедрение кода с использованием оператора UNION затруднительно.

В таких случаях, злоумышленниками используется метод экранирования части запроса при помощи символов комментария(# или /* или -- в зависимости от типа СУБД).

В данном примере, злоумышленник может передать в скрипт параметр id со значением *-1 UNION SELECT password FROM admin/**, выполнив таким образом следующий запрос:

SELECT author FROM news WHERE id=-1 UNION SELECT password FROM admin/* AND author LIKE ('a%')

Часть запроса (*ANDauthor LIKE ('a%')*) помечена как комментарий и не влияет на выполнение.

Если приложение корректно обрабатывает исключения, использовать UNION SQL-инъекцию может быть затруднительно. В этом случае может быть применена техника атаки BlindSQL [5], суть которой в том, что, модифицируя запрос, можно влиять на логику работы приложения: приопределенных входных данных некоторые страницы могут отображаться неправильно или запрос будет возвращать только часть информации.

Составляется SQL-выражение, которое при истинном значении не нарушает логику работы приложения. Приложном же значении возникает аномальное поведение вработе web-приложения: страницы неправильно отображаются, либо возвращается только часть данных. Сцельюпроверки логических условий вкачестве подобного SQL-выражения можно использовать следующее:

INJECTION– SQL-запрос, который возвращает значение, либо null
ANDNVL(INJECTION,0) != 0 # null – страница некорректно отображается

Врезультате успешной реализации SQL-инъекции злоумышленник может обойти логику работы приложения, получить доступ к конфиденциальной информации, содержащейся вСУБД, апри определенных условиях даже получить полный доступ ксерверу, накотором функционирует СУБД. Если при этом учесть, что отдельные приложения интегрированы друг сдругом внутри сети компании, получение несанкционированного доступа куязвимому приложению позволит злоумышленнику получить контроль над всей информационной системой.

Список литературы

[1]. Атака SQL Injection. URL: https://technet.microsoft.com/ru-ru/library/ms161953(v=sql.105).aspx

[2]. Внедрение SQL-кода. URL: https://ru.wikipedia.org /wiki/%D0%92%D0%BD%D0%B5%D0%B4%D1%80%D0%B5%D0%BD%D0%B8%D0%B5_SQL%D0%BA%D0%BE%D0%B4%D0%B0

[3]. М. Егоров.Выявление и эксплуатация SQL инъекций в приложениях. URL:http://www.cnpo.ru/doc/echelon-sql.pdf

[4]. SQL-инъекции: простое объяснение для начинающих (часть 1). URL: http://webware.biz/?p=4576

[5]. SQL Injection. URL: http://hakipedia.com/index.php/SQL_Injection #UNION_Statements

Антипова Евгения Игоревна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: evgenia2504@gmail.com

Савкин Михаил Константинович – ассистент кафедры КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

Е.А. Коваленко

УГРОЗЫ СИСТЕМЫ ANDROID

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Первая вредоносная программа для ОС Android была обнаружена в августе 2010 года. С течением времени число угроз для Android продолжало расти и в конце 2011 года количество вредоносных программ для этой платформы увеличилось примерно в 20 раз.

Рассмотрим некоторые примеры основных угроз данной системы.

Самой распространенной угрозой можно назвать СМС-троян (семейство Android.SmsSend). Android.SmsSend — это семейство вредоносных программ, работающих на мобильных устройствах под управлением ОС Android. Троянцы этого семейства предназначены для отправки СМС-сообщений с повышенной тарификацией и подписки пользователей на различные платные контент-услуги и сервисы, в результате чего с абонентского счета может списываться определенная денежная сумма. Часть стоимости этих сообщений поступает в карман злоумышленников, обогащая их. Большинство троянцев Android.SmsSend представляют собой самостоятельные программные пакеты с относительно простой архитектурой и функционалом, и чаще всего распространяются при помощи мошеннических сайтов под видом популярных игр и приложений, а также их обновлений. Подобные программы практически ничем не отличаются друг от друга, кроме как незначительными изменениями в интерфейсе и короткими номерами, на которые будет выполняться отправка сообщений. Чаще всего они распространяются под видом популярных приложений и игр, таких как OperaMini, ICQ, Skype, AngryBirds и т. п., при этом используется соответствующая иконка.

Далее описанные вредоносные программы, в зависимости от семейства, обладают таким функционалом, как, например, сбор конфиденциальной информации пользователя, добавление закладок в браузер, выполнение команд, поступающих от злоумышленников, отправка СМС-сообщений, установка других приложений и т. п. Чтобы реализовать возможность установки приложений, не вызывая подозрений со стороны пользователя, троянцам необходимы права root (права, с которыми работает ядро системы).

Троянцы Android.Gongfu распространяются через различные каталоги программ, а также на популярных сайтах и форумах в модифицированных злоумышленниками легитимных играх и приложениях. Способны запускаться автоматически вместе с загрузкой операционной системы.

Этот вирус способен не только выкачивать всю интересующую информацию с мобильного устройства, но и выполнять конкретные

команды, удаленно передаваемые злоумышленниками. Таким образом, вирус может устанавливать на Android-устройство самые разные приложения без вмешательства самого пользователя. Фактически, Android.Gongfu, попавший на смартфон или планшетный компьютер, может дополнительно устанавливать и другие вредоносные программы, скачивающие информацию, деньги и т.д. При этом антивирус не всегда может успеть заметить все загруженные вирусы.

Android.Wukong - это еще одно семейство вредоносных программ, поражающих мобильные устройства под управлением ОС Android. Распространяются эти программы в модифицированных злоумышленниками легитимных приложениях. После их установки и наступления определенных системных событий (например, загрузка операционной системы или запуск инфицированного приложения) троянцы этого типа автоматически запускаются в качестве фонового сервиса и подключаются к удаленному серверу. Сервер, в свою очередь, предоставляет вредоносным программам информацию о номере платного сервиса, на который необходимо осуществить отправку СМС-сообщений. Текст всех сообщений начинается со строки "YZHC", а интервал их отправки составляет 50 минут. Для того чтобы скрыть следы вредоносной деятельности, троянцы Android.Wukong удаляют отправленные ими СМС, а также входящие сообщения с информацией об успешном приеме платежа оператором.

Вредоносные программы Android.DreamExploid распространяются в модифицированных злоумышленниками легитимных приложениях. После того как пользователь установил и запустил инфицированную программу, троянцы этого семейства производят попытку повысить текущие системные привилегии при помощи root-эксплойтов, которые содержатся в ресурсах самих вредоносных программ. В случае успешного повышения привилегий скрытно от пользователя осуществляется установка второго вредоносного приложения. Оно имеет возможность загрузки и установки других программ из Интернета, а также обладает функционалом для сбора различной информации об инфицированном устройстве и отправки ее злоумышленникам.

Троянцы Android.Geinimi обладают внушительным функционалом, который включает такие возможности как определение местоположения мобильного устройства, загрузка файлов из Интернета (в частности, могут загружаться другие программы), считывание и запись закладок браузера, получение информации из телефонной книги, совершение звонков, отправка, чтение и редактирование СМС, а также ряд других. Вредоносные программы функционируют в качестве фонового сервиса, поэтому они продолжают свою работу даже после того, как пользователь закроет инфицированное приложение.

Семейство Android.Spy распространяется на популярных сайтах (преимущественно китайских) в составе легитимных игр и приложений,

которые модифицированы злоумышленниками. После установки программы автоматически запускаются при старте операционной системы. Они обладают возможностью чтения и записи контактов, приема и отправки СМС-сообщений, определения GPS-координат, чтения и записи закладок браузера, получения сведений об IMEI мобильного устройства и номере мобильного телефона. Имеется функционал для осуществления специализированного веб-поиска и перехода по определенным ссылкам в браузере. Предусмотрена возможность загрузки обновлений троянцев, однако для их установки требуется участие пользователя.

Троянцы Android.Crusewind распространяются при помощи СМС-спама, который сообщает о получении новых настроек MMS и GPRS и предлагает установить их, для чего требуется перейти по приведенной в сообщениях ссылке. Если пользователь откроет данную ссылку, на его мобильное устройство будет загружено вредоносное приложение. Троянские программы семейства Android.Crusewind способны рассылать СМС-сообщения в соответствии с настройками, находящимися в xml-файле, который скачивается с удаленного сервера. Также возможна загрузка обновлений троянцев и отправка на сервер сведений об установленных на мобильном устройстве приложениях.

Итак, мы рассмотрели наиболее распространенные угрозы, с которыми могут столкнуться пользователи устройств под управлением операционной системы Android. Одной из главных проблем безопасности при работе с ОС Android, прежде всего, является человеческий фактор. Какой бы защищенной ни была операционная система, беспечность, невнимательность, самоуверенность и простая неосведомленность рано или поздно подвергнут опасности обладателя устройства. Например, уверенность пользователя в том, что ему ничего не угрожает, заставляет его игнорировать средства безопасности, такие как антивирусные программы. Когда подделывается известный сайт, игра или приложение, а пользователь при этом неопытен, он может и не осознавать, что подвергается какому-либо риску, устанавливая ту или иную программу или вводя свою конфиденциальную информацию. Следующая важная проблема косвенно связана с первой и касается программной уязвимости как самой операционной системы, так и прикладного ПО. Таким образом, пользователи сталкиваются, например, с вредоносными программами, использующими root-эксплойты для повышения привилегий в системе.

Средства массовой информации не перестают рассказывать нам об огромном количестве вредоносных программ на Android. От этих программ может спасти один из полноценных антивирусов для Android, однако избежать опасности можно и самостоятельно. Для этого необходимо:

— С осмотрительностью скачивать все приложения
— Не пользоваться подозрительными сторонними магазинами приложений
— С осторожностью относиться к приложениям из GooglePlay

— Остерегаться фишинга - вида интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Если все-таки с устройством произошла неприятность, и на нем был обнаружен вирус, необходимо проделать следующие действия:

— Сделать сканирование и чистку устройства с помощью антивирусной программы. Для этого необходимо подключить устройство к ПК (это наилучший способ для качественной проверки на вирусы) и отсканировать компьютерной программой-антивирусом устройство.
— После того как все вирусы удалены, нужно отключить устройство от компьютера и вернуть стандартные настройки на телефон. Чтобы все сделать быстро и без утери важных данных, нужно скопировать всю необходимую информацию с памяти телефона на резервный носитель памяти. После этого сделать синхронизацию данных в телефоне
— Первым делом после синхронизации данных нужно установить антивирусную программу. Для операционной системы Android разработаны такие виды антивирусных программ, как KasperskyMobileSecurity или Avast. Это самые популярные антивирусные программы для Android, которые не только блокируют установку подозрительных программ, но и блокируют звонки и отправку сообщений на короткие номера

Список источников:

[1]. http://habrahabr.ru
[2]. http://vms.drweb.ru
[3]. http://android-mobile.ru/
[4]. http://www.drive2.ru/
[5]. http://www.winline.ru/
[6]. https://ru.wikipedia.org
[7]. http://geekk.ru/

Коваленко Елизавета Александровна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: www.yoursmile@yandex.ru

С.М. Твердова, А.О. Волкова, Е.Е. Коваль, И.Л. Луговский

УСТРАНЕНИЕ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Одной из проблем, возникающих при работе с высокочастотной аппаратурой, являются электромагнитные помехи, имеющие различные источники формирования - блоки питания, внешние наводки, сложная электромагнитная обстановка (большое количество электроустановок),и др. Как правило, они проявляются в той же полосе частот, что и рабочие сигналы. Беспрепятственно минуя входные фильтры, далее они обрабатываются так же, как и полезные сигналы, вызывая дополнительные ошибки в каналах передачи данных, а в отдельных случаях и физическое повреждение элементов сигнального тракта, если амплитуда помехи значительно превышает ту величину, на которую были рассчитаны защитные элементы. Устранение влияния этих помех является важной технической задачей.

В данной работе рассмотрено влияние помехи, создаваемой внешними наводками, на работу высокочастотного генератора прямоугольных импульсов и предложен метод их нейтрализации.

ВЧ генератор импульсов, электрическая схема которого приведена на рисунке 1, построен на микросхеме КР1006ВИ1 (NE555).

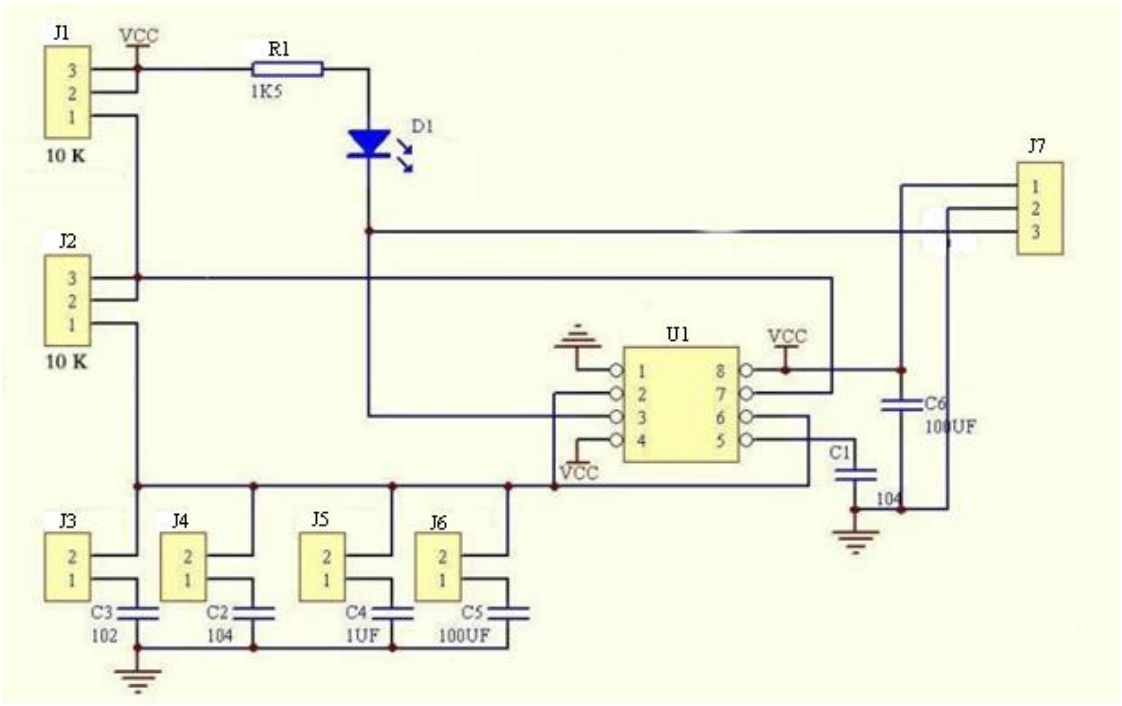


Рис.1. Схема электрическая принципиальная

Микросхема U1 представляет собой таймер, который и осуществляет генерацию прямоугольных импульсов в зависимости от приложенных к нему сигналов. Напряжение питания, равное обеспечивает блок питания MSSTECH HY3005.

Конденсаторы C2, C3, C4, C5 – являются времязадающими, и ограничивают верхнюю частоту генерации. Потенциометры J1 J2 - управляют скважностью и частотой в пределах поддиапазона. Резистор R1 - ограничивает ток для диода D1, являющегося индикатором при низких частотах генерации. Конденсаторы C1, C6 - фильтры по питанию.

На рисунке 2 показана осциллограмма 1 с побочным импульсом, причиной появления которого является возмущение напряжения питания, вызванное наличием нелинейных элементов в сети электропитания. К таким элементам относят сердечники трансформаторов, импульсные блоки питания, силовые полупроводниковые преобразователи и др.

Для устранения их влияния используют RC, или LC - фильтры, специальные устройства ограничения перенапряжений (разрядники, варисторы и т.п.), экранированные кабели.

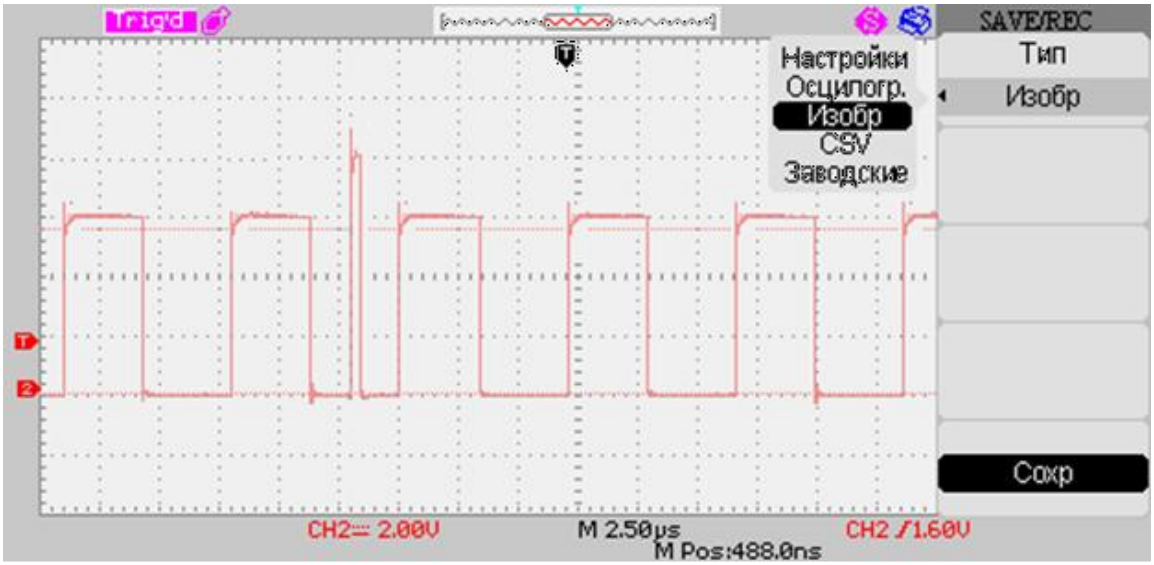


Рис.2. Осциллограмма 1

Данная помеха помимо опасности повреждения элементов (амплитуда импульса на 30% выше расчётного значения) может быть принята как рабочий импульс, что приведет к некорректной работе. Чтобы этого не произошло, были использованы фильтры питания, а так же экранированные кабели для подключения к блоку питания. В результате побочный импульс, вызванный электромагнитной помехой, был устранен, что и показывает осциллограмма 2 на рисунке 3.

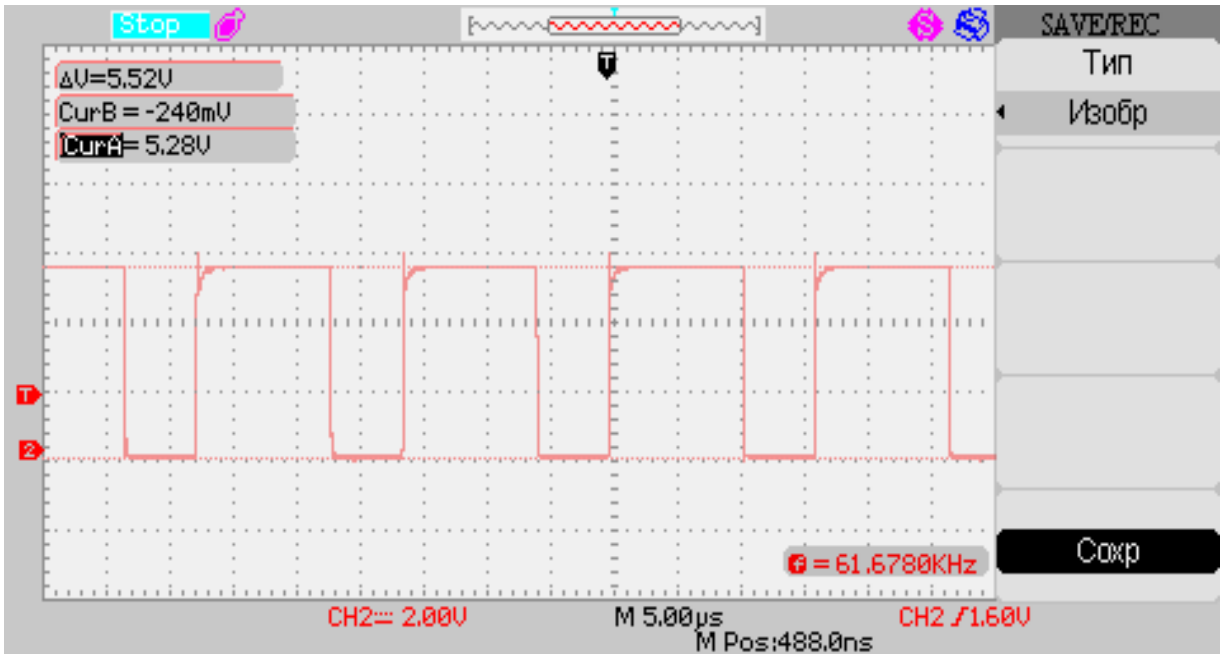


Рис.3. Осциллограмма 2

Улучшая характеристики фильтра добиваемся результата вида как на осциллограмме 3 – рисунок 4.

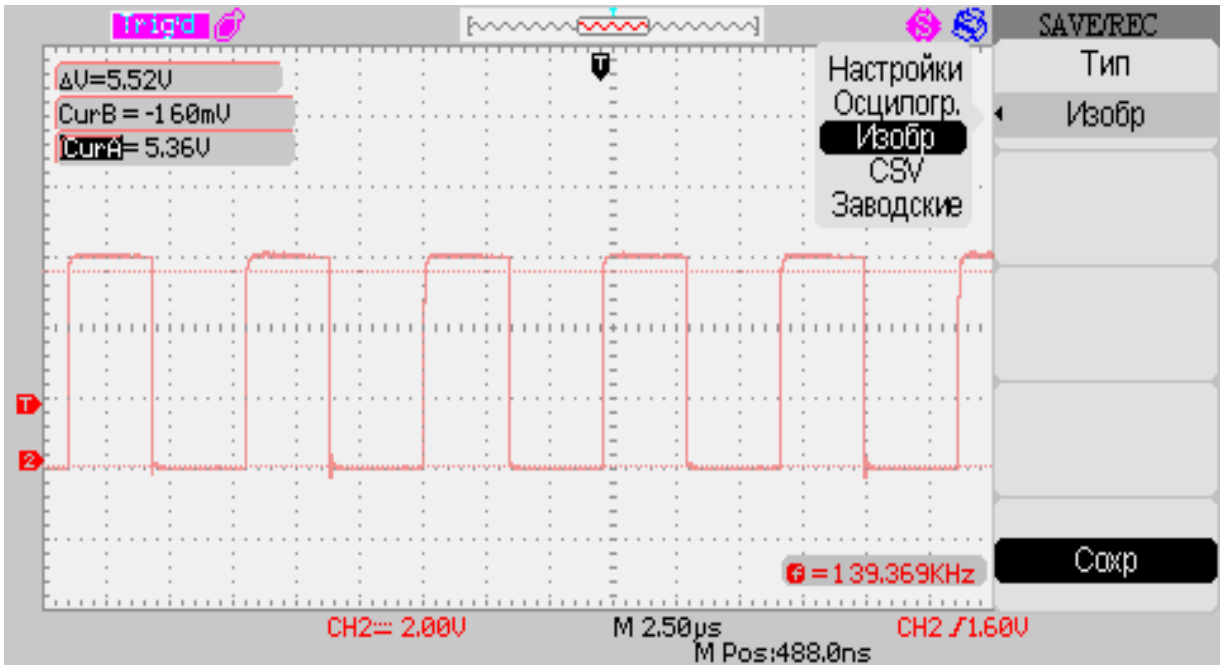


Рис.4. Осциллограмма 3

В результате были опробованные методики подавления помех в высокочастотной технике.

Список литературы:

[1]. Хоровиц П., Хилл У. «Искусство схемотехники»

[2]. Барри Уилкинсон. «Основы проектирования цифровых схем»

[3]. Бессонов Л. А. «Теоретические основы электротехники. Электрические цепи»

Твердова Светлана Михайловна – преподаватель КФ МГТУ им. Н.Э. Баумана. E-mail: ivalug@rambler.ru

Волкова Анастасия Олеговна - студент КФ МГТУ им. Н.Э. Баумана. E-mail: ivalug@rambler.ru

Коваль Евгений Евгеневич - студент КФ МГТУ им. Н.Э. Баумана. E-mail: ivalug@rambler.ru

Луговский Иван Леонидович - студент КФ МГТУ им. Н.Э. Баумана. E-mail: www.yoursmile@yandex.ru

СОДЕРЖАНИЕ

НАУКОЕМКИЕ ТЕХНОЛОГИИ
В ПРИБОРО - И МАШИНОСТРОЕНИИ
И РАЗВИТИЕ ИННОВАЦИОННОЙ
ДЕЯТЕЛЬНОСТИ В ВУЗЕ

Материалы
Всероссийской научно-технической конференции

Том 3

Научное издание

Все работы публикуются в авторской редакции. Авторы несут ответственность за подбор и точность приведенных фактов, цитат, статистических данных и прочих сведений

Подписано в печать 11.11.2015.
Формат 60x90/16. Печать офсетная. Бумага офсетная. Гарнитура «Таймс».
Печ. л. 14,75. Усл. п. л. 12,72. Тираж 50 экз. Заказ № 165

Издательство МГТУ им. Н.Э. Баумана
107005, Москва, 2-я Бауманская, 5

Оригинал-макет подготовлен и отпечатан в Редакционно-издательском отделе
КФ МГТУ им. Н.Э. Баумана
248000, г. Калуга, ул. Баженова, 2, тел. 57-31-87