

Министерство образования и науки Российской Федерации
Федеральное агентство по образованию

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

НАУЧНАЯ СЕССИЯ ТУСУР – 2006

**Материалы докладов
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР – 2006»,
посвященной 75-летию Ф.И. Перегудова,
4 – 7 мая 2006 г.**

В пяти частях

Часть 2

В-Спектр
2006

УДК 621.37/.39+681.518 (063)

ББК 32.84я431+32.988я431

Научная сессия ТУСУР – 2006: Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 4–7 мая 2006 г. – Томск: Издательство «В-Спектр», 2006. Ч. 2. – 324 с.

Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых посвящены различным аспектам разработки, исследования и практического применения радиотехнических, телевизионных и телекоммуникационных систем и устройств, вопросам проектирования и технологии радиоэлектронных средств, аудиовизуальной техники, бытовой радиоэлектронной аппаратуры, а также автоматизированным системам управления и проектирования. Рассматриваются проблемы электроники СВЧ- и акустооптоэлектроники, физической, плазменной, квантовой, промышленной электроники, радиотехники, информационно-измерительных приборов и устройств, распределенных информационных технологий, автоматизации технологических процессов, в частности в системах управления и проектирования, информационной безопасности. В сборнике представлены материалы по математическому моделированию в технике, экономике и менеджменту, антикризисному управлению, автоматизации управления в технике и образовании. Широкому кругу читателей будет доступна информация о социальной работе в современном обществе, философии и специальной методологии, экологии, мониторингу окружающей среды и безопасности жизнедеятельности, инновационных, студенческих идеях и проектах.

Конференция проводится при поддержке

ЦС РНТОРЭС им. А.С. Попова

Посвящается 75-летию Ф.И. Перегудова

ISBN 5-91191-003-9

ISBN 5-91191-005-5 (Ч. 2)

© Том. гос. ун-т систем управления
и радиоэлектроники, 2006

Федеральное агентство по образованию
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

**Всероссийская научно-техническая конференция
студентов и молодых ученых
"Научная сессия ТУСУР – 2006"
4–7 мая 2006 г.**

ПРОГРАММНЫЙ КОМИТЕТ

Кобзев А.В. – председатель, ректор ТУСУР, д.т.н., профессор.

Ильющенко В.Н. – сопредседатель, проректор по НР ТУСУР, д.т.н., профессор.

Малиук А.А. – декан факультета информационной безопасности Московского инженерно-физического института (МИФИ), к.т.н., г. Москва.

Майстренко В.А. – проректор по информатизации ОмскГТУ, д.т.н., профессор, г. Омск.

Кравченко В.Б. – зам. проректора по информатизации Российского государственного гуманитарного университета, к.т.н., г. Москва.

Кориков А.М. – зав. каф. автоматизированных систем управления (АСУ) ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор.

Московченко А.Д. – зав. каф. философии, д.ф.н., профессор.

Ехлаков Ю.П. – проректор по информатизации ТУСУР, д.т.н., профессор.

Шурыгин Ю.А. – первый проректор ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор.

Уваров А.Ф. – проректор по экономике ТУСУР, к.э.н.

Шарыгин Г.С. – зав. каф. радиотехнических систем (РТС), д.т.н., профессор.

Пустынский И.Н. – зав. каф. телевидения и управления (ТУ), заслуженный деятель науки и техники РФ, д.т.н., профессор.

Шелупанов А.А. – зав. каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС), д.т.н., профессор.

Осипов Ю.М. – зав. Отделением каф. ЮНЕСКО при ТУСУР, академик Международной академии информатизации, д.т.н., д.э.н., профессор.

Грик Н.А. – зав. каф. ИСР, д. ист.н., профессор.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Кобзев А.В. – председатель, ректор ТУСУР, д.т.н., профессор.

Ильющенко В.Н. – сопредседатель, проректор по НР ТУСУР, д.т.н., профессор.

Шурыгин Ю.А. – первый проректор ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор.

Акулиничев Ю.П. – председатель совета по НИРС радиотехнического факультета (РТФ), д.т.н., профессор каф. радиотехнических систем (РТС).

Еханин С.Г. – председатель совета по НИРС радиоконструкторского факультета (РКФ), д.ф.-м.н., профессор каф. конструирования узлов и деталей РЭС (КУДР).

Коцубинский В.П. – председатель совета по НИРС факультета вычислительных систем (ФВС), зам. зав. каф. компьютерных систем в управлении и проектировании (КСУП), к.т.н., доцент.

Мицель А.А. – председатель совета по НИРС факультета систем управления (ФСУ), д.т.н., профессор каф. автоматизированных систем управления (АСУ).

Орликов Л.Н. – председатель совета по НИРС ФЭТ, д.т.н., профессор каф. ЭП.

Казакевич Л.И. – председатель совета по НИРС гуманитарного факультета (ГФ), к.ист.н., доцент каф. ИСР.

Ярымова И.А. – зам. зав. отделения послевузовского профессионального образования (ОППО) ТУСУР, к.б.н.

ПОРЯДОК РАБОТЫ, ВРЕМЯ И МЕСТО ПРОВЕДЕНИЯ

Работа конференции будет организована в форме пленарных, секционных и стендовых докладов.

**Конференция проводится
с 4 по 7 мая 2006 г.**

**в Томском государственном университете
систем управления и радиоэлектроники**

**Регистрация участников будет проводиться
перед пленарным заседанием в главном корпусе ТУСУР
(пр. Ленина, 40) в актовом зале 4 мая с 9:00 до 10:00.**

СЕКЦИИ КОНФЕРЕНЦИИ

- Секция 1. РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ И РАСПРОСТРАНЕНИЕ РАДИОВОЛН** – *председатель Шарыгин Г.С., зав. каф. РТС, д.т.н., профессор; зам. председателя Тисленко В.И., к.т.н., доцент каф. РТС*
- Секция 2. ЗАЩИЩЕННЫЕ ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ** – *председатель Голиков А.М., к.т.н., доцент каф. РТС*
- Секция 3. АУДИОВИЗУАЛЬНАЯ ТЕХНИКА, БЫТОВАЯ РАДИОЭЛЕКТРОННАЯ АППАРАТУРА И СЕРВИС** – *председатель Пустынский И.Н., зав. каф. ТУ, д.т.н., профессор; зам. председателя Костевич А.Г., к.т.н., доцент каф. ТУ*
- Секция 4. ПРОЕКТИРОВАНИЕ И ТЕХНОЛОГИИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ. ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ РАДИООБОРУДОВАНИЯ** – *председатель Масалов Е.В., д.т.н., профессор каф. КИПР, зам. председателя Михеев Е.Н., м.н.с.*
- Подсекция 4.1. ПРОЕКТИРОВАНИЕ БИОМЕДИЦИНСКОЙ АППАРАТУРЫ** – *председатель Еханин С.Г., д.ф.-м.н., профессор каф. КУДР*
- Подсекция 4.2. КОНСТРУИРОВАНИЕ И ПРОИЗВОДСТВО РАДИОЭЛЕКТРОННЫХ СРЕДСТВ** – *председатель Михеев Е.Н., м.н.с.*
- Секция 5. ИНТЕГРИРОВАННЫЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ** – *председатель Катаев М.Ю., д.т.н., профессор каф. АСУ*
- Секция 6. КВАНТОВАЯ, ОПТИЧЕСКАЯ И НАНОЭЛЕКТРОНИКА** – *председатель Шарангович С.Н., зав. каф. СВЧиКР, к.ф.-м.н., доцент; зам. председателя Буримов Н.И., к.т.н., доцент каф. ЭП*
- Секция 7. ФИЗИЧЕСКАЯ И ПЛАЗМЕННАЯ ЭЛЕКТРОНИКА** – *председатель Троян П.Е., зав. каф. ФЭ, к.т.н., доцент*
- Секция 8. РАСПРЕДЕЛЁННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ** – *председатель Ехлаков Ю.П. проректор по Информатизации ТУСУР, зав. каф. АОИ, д.т.н., профессор; зам. председателя Сенченко П.В., к.т.н., доцент каф. АОИ*
- Секция 9. АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ** – *председатель Шелупанов А.А., зав. каф. КИБЭВС, д.т.н., профессор; зам. председателя Раводин О.М., к.т.н., профессор каф. КИБЭВС*

Подсекция 9.1. ПРОЕКТИРОВАНИЕ И ТЕХНОЛОГИЯ ЭВС

Подсекция 9.2. КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Подсекция 9.3 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Секция 10. АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА В СИСТЕМАХ УПРАВЛЕНИЯ И ПРОЕКТИРОВАНИЯ – *председатель **Шурыгин Ю.А.**, первый проректор ТУСУР, зав. каф. КСУП, д.т.н., профессор; зам. председателя **Коцубинский В.П.**, зам. зав. каф. КСУП, к.т.н., доцент*

Секция 11. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель – **Ильюшенко В.Н.**, проректор по НР ТУСУР, зав. каф. РЗИ, д.т.н., профессор; зам. председателя **Загоскин В.В.**, к.ф.-м.н., доцент каф. РЗИ*

Секция 12. ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И УСТРОЙСТВА – *председатель **Светлаков А.А.**, зав. каф. ИИТ, д.т.н., профессор; зам. председателя **Шидловский В.С.**, к.т.н., доцент каф. ИИТ*

Секция 13. РАДИОТЕХНИКА – *председатель **Титов А.А.**, д.т.н., профессор каф. РЗИ; зам. председателя **Семенов Э.В.**, к.т.н., доцент каф. РЗИ;*

Секция 14. ПРОМЫШЛЕННАЯ ЭЛЕКТРОНИКА – *председатель **Семенов В.Д.**, зам. зав. каф. ПрЭ по НР, к.т.н., доцент; зам. председателя **Шевелев М.Ю.**, к.т.н., доцент каф. ПрЭ*

Секция 15. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ В ТЕХНИКЕ, ЭКОНОМИКЕ И МЕНЕДЖМЕНТЕ – *председатель **Мицель А.А.**, д.т.н., профессор каф. АСУ; зам. председателя – **Зариковская Н.В.**, к.ф.-м.н., доцент каф. ФЭ*

Секция 16. ЭКОНОМИКА И УПРАВЛЕНИЕ – *председатель **Осипов Ю.М.**, зав. Отделением каф. ЮНЕСКО при ТУСУР, д.э.н., д.т.н., профессор; зам. председателя – **Василевская Н.Б.**, к.э.н., доцент каф. Экономики*

Секция 17. АНТИКРИЗИСНОЕ УПРАВЛЕНИЕ – *председатель **Семглазов А.М.**, д.т.н., профессор каф. ТУ; зам. председателя – **Бут О.А.**, ассистент каф. ТУ*

- Секция 18. ЭКОЛОГИЯ И МОНИТОРИНГ ОКРУЖАЮЩЕЙ СРЕДЫ**
– *председатель Карташов А.Г., д.б.н., профессор каф. РЭТЭМ*
- Секция 19. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ** – *председатель Хорев И.Е., д.т.н., профессор каф. РЭТЭМ; зам. председателя – Полякова С.А., к.б.н., доцент каф. РЭТЭМ*
- Секция 20. АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНОЙ РАБОТЫ В СОВРЕМЕННОМ ОБЩЕСТВЕ** – *Грик Н.А., зав. каф. ИСР, д.ист.н., профессор; зам. председателя – Казакевич Л.И., к.ист.н., доцент каф. ИСР*
- Секция 21. ФИЛОСОФИЯ И СПЕЦИАЛЬНАЯ МЕТОДОЛОГИЯ** – *председатель Московченко А.Д., зав. каф. Философии, д.ф.н., профессор; зам. председателя – Раутина М.Ю., к.ф.н., доцент каф. философии*
- Секция 22. ИННОВАЦИОННЫЕ ПРОЕКТЫ, СТУДЕНЧЕСКИЕ ИДЕИ И ПРОЕКТЫ** – *председатель Уваров А.Ф., проректор по экономике ТУСУР, к.э.н.; зам. председателя – Чекчеева Н.В., зам. директора Студенческого Бизнес-Инкубатора (СБИ)*
- Секция 23. АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ В ТЕХНИКЕ И ОБРАЗОВАНИИ** – *председатель Дмитриев В.М., зав. каф. ТОЭ, д.т.н., профессор; зам. председателя Андреев М.И., к.т.н., доцент ВКИЭМ*
- Секция 24. ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ ШКОЛЬНИКОВ** – *председатель Дмитриев И.В., директор ОЦ «Школьный университет», к.т.н.; зам. председателя – Шамина О.Б., начальник учебно-методического отдела ОЦ «Школьный университет», к.т.н., доцент*

Адрес оргкомитета:

**Россия, 634050, г. Томск, пр. Ленина 40, ТУСУР,
Научное управление (НУ), к. 205.
Тел.: 8-(3822)-51-47-57
E-mail: nirs@main.tusur.ru**

Материалы научных докладов, предоставленные на конференцию, опубликованы в сборнике «НАУЧНАЯ СЕССИЯ ТУСУР – 2006», состоящем из пяти частей.

В 1 часть сборника включены доклады 1 – 7 секций.

Во 2 часть – доклады 8, 10, 11 секций.

В 3 часть – доклады 9 секции.

В 4 часть – доклады 12 – 16 секций.

В 5 часть – доклады 17 – 24 секций.

СЕКЦИЯ 8

РАСПРЕДЕЛЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

*Председатель – Ехлаков Ю.П. проректор по Информатизации
ТУСУР, зав. каф. АОИ, д.т.н., профессор;
зам. председателя – Сенченко П.В., к.т.н., доцент каф. АОИ*

РЕАЛИЗАЦИЯ СПОСОБА ИЗВЛЕЧЕНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ ИЗ ПРОИЗВОЛЬНОГО ОКНА ОС WINDOWS

Е.А. Егорова, магистрант 6 курса ЭФ;

И.Г. Боровской, д.ф.-м. н., проф.

ТУСУР, г. Томск, egekaterina@yandex.ru

Основной целью работы является создание универсального способа, предоставляющего возможность извлечения текстового содержания из произвольного окна ОС Windows.

В работе [1] был проведен анализ поставленной задачи, указан ряд возможных путей ее решения, среди которых копирование содержимого окна в буфер обмена, копирование текста из объектов составного окна с привлечением СОМ-технологий и с использованием WinAPI функций, и доказана их несостоятельность. Для решения задачи предлагалось разработать универсальный подход, базирующийся на специальных методах перехвата вывода текста, так называемых графических ловушках, и позволяющий извлекать текстовую информацию как из обычных, так и из нестандартных окон ОС Windows.

Произвольное windows-окно, содержащее текст, для его отображения использует одну из 12 системных функций (в ANSI и UNICODE вариантах с суффиксом A и W соответственно): TextOut, ExtTextOut, DrawText, DrawTextEx, TabbedTextOut, PolyTextOut, – имеющих одним из своих параметров указатель на символьную строку, которую необходимо отобразить, и координаты вывода. Вызов этих функций происходит каждый раз, когда окно перерисовывает свою клиентскую область, т.е. при получении сообщения WM_PAINT.

В основе подхода, базирующегося на графических ловушках, лежит перехват API-функций, заключающийся в изменении некоторого кода в теле функции таким образом, чтобы при вызове этой самой API-функции управление передавалось не ей, а функции, подменяющей

системную. Эта функция, работая вместо системной, выполняет запланированные разработчиком действия, и затем вызывает оригинальную функцию.

Прием заключается в том, чтобы в начало перехватываемой функции записать команду `jmp <адрес функции-двойника>`. Очевидно, что затируемые байты необходимо при этом сохранить. После вызова приложением исправленной функции управление будет передано функции-двойнику, которая извлекает и сохраняет переданные ей параметры, т.е. информацию об отображаемой строке. Затем для вызова оригинальной функции необходимо восстановить затертые байты, вызвать ее, передав ей все необходимые параметры. После возврата из оригинальной функции, необходимо снова в начало кода функции записать команду перехода на функцию-двойника.

При такой схеме работы приложение будет получать информацию о перерисовке клиентской области со всех окон, а не только с целевого. Во избежание этого необходимо внедрить исполняемый код в адресное пространство целевого процесса. Одним из способов является использование hook-метода `WH_CALLWNDPROC`, который контролирует сообщения, посланные оконным процедурам. При его срабатывании необходимо установить графические ловушки, затем послать сообщение `WM_PAINT` целевому окну, а после его обработки снять графические ловушки.

В работе разработан нестандартный способ использования так называемых графических ловушек, который позволяет извлекать информацию из произвольных окон ОС Windows и может стать весомым дополнением операционной системы.

С практической точки зрения разработанный метод может найти применение при автоматизированной обработке текста. Например, при активизации пользователем модуля приложение извлекает текст и отправляет его на web-сервер, который может представлять собой базу данных или базу знаний. Полученный таким образом текст обрабатывается на сервере. Результатом анализа может служить энциклопедические данные, толкование значения, грамматические характеристики отдельных слов или другие подобного рода сведения.

ЛИТЕРАТУРА

1. *Егорова Е.А.* «Универсальный метод выборки текстовой информации из произвольного окна ОС Windows» // Сборник материалов всероссийской научно-технической конференции «Научная сессия ТУСУР – 2005», ч. 2, с. 47–48

**АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ВЕДЕНИЯ
НАУЧНО-СПРАВОЧНОГО АППАРАТА АРХИВОВ**
*Е.В. Коновалова, ТУСУР, 5 курс; И.И. Веберова, доцент каф. АОИ
ТУСУР, г. Томск, т. 42-34-33, knv@muma.tusur.ru*

В настоящее время в архивной службе Томской области существует множество проблем, связанных с учетом, хранением, обработкой документов архива и последующим удовлетворением запросов широкого круга пользователей. Решение этих вопросов осуществляется путем автоматизации бизнес-процессов архивного дела.

На основании Закона Томской области «Об утверждении областной комплексной целевой программы формирования единого информационного пространства Томской области на 2001–2004 гг.» был принят в разработку проект создания государственного автоматизированного информационного ресурса «Архив» (ГАИР «Архив»). Данная система предназначена для автоматизации технологических процессов комплектования, обеспечения сохранности, государственного учета, научного описания архивного фонда Томской области, управления и мониторинга архивного процесса, а также использования и предоставления архивных ресурсов [1]. ГАИР «Архив» является распределенным банком данных, актуализация и предоставление доступа к которому осуществляется с помощью автоматизированной информационной системы «Архив» по локальным и глобальным сетям передачи данных. АИС «Архив» – территориально-распределенная автоматизированная информационная система, обеспечивающая реализацию информационных процессов при формировании и использовании ГАИР «Архив». Функциональная структура АИС «Архив» состоит из следующих компонентов: модули поддержки бизнес-процессов архива, Web-сервер архивов Томской области, модуль администрирования, модуль сетевого взаимодействия, модуль взаимодействия с СУБД, модуль информационного обмена.

В настоящее время разработана ER-модель интегрированной базы данных и программно реализованы в средах СУБД Oracle 8i и Borland Delphi 7 следующие модули АИС «Архив»: государственного учета документов архива; учета и контроля исполнения социально-правовых запросов; обеспечения сохранности архивных документов, WEB-ресурс «Реестр архивов территории».

Автоматизация процессов ведения научно-справочного аппарата архива является наиболее важной и актуальной задачей и предполагает создание программных средств ведения описей и других архивных справочников, а также разработку эффективных алгоритмов поиска архивной информации [2]. В связи с этим особую значимость приобретает задача семантического моделирования в части организации ар-

хивных справочников. Анализ существующей ER-модели ГАИР «Архив» позволил сделать вывод о необходимости изменения атрибутивного состава сущности «Опись», имеющей линейную структуру. Опись содержит вторичную информацию об архивных документах, сгруппированную по разделам, имеющим иерархический порядок. Основными являются годовые разделы, внутри которых могут быть подразделы, они в свою очередь могут содержать другие подразделы. Иерархия разделов может достигать любой глубины. Таким образом, в ER-модели должны быть реализованы принципы моделирования иерархических структур данных [3]. Метод обхода дерева J.Celko неприменим для рассматриваемой предметной области из-за большого объема хранимых данных. Для решения проблемы в ER-модель необходимо добавить сущность «Раздел» и организовать иерархическую рекурсивную связь. Это простое решение позволит в одной таблице сформировать иерархию разделов любой глубины. Организация сущности «Раздел» представлена на рисунке.



Представление иерархий разделов описи с помощью рекурсивной связи

Представление иерархий разделов описи с помощью рекурсивной связи

Такая организация разделов позволит наиболее емко и достоверно отобразить структуру архивного справочника «Опись», что обеспечит корректное хранение информации о документах в базе данных и реализовать прозрачные и эффективные запросы.

ЛИТЕРАТУРА

1. Веберова И.И. Опыт создания государственного автоматизированного информационного ресурса «Архив» // Информационные технологии в территориальном управлении, промышленности, образовании. Томск: Томск. гос. ун-т систем управления и радиоэлектроники. С. 41–61.
2. Никольская Т.Е., Веберова И.И. Принципы построения подсистемы создания и ведения научно-справочного аппарата архива // Научная сессия ТУСУР-2005: Материалы Всеросс. науч.-техн. конф. студентов, аспирантов и молодых специалистов, Томск, 26-28 апреля 2005 г. Томск: Томс. гос. ун-т систем управления и радиоэлектроники, 2005. С. 54–56.
3. Стулов А. Хранилища данных: основные архитектуры и принципы построения в реляционных СУБД / А. Стулов [Электронный ресурс] : публикация сайта / Консалтинг. Аналитические системы для бизнеса. – 2005. Режим доступа: www.bipartnet.ru

ПРОБЛЕМА ИНФОРМАЦИОННОЙ СОВМЕСТИМОСТИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРИ МЕЖВЕДОМСТВЕННОМ ВЗАИМОДЕЙСТВИИ

***А.А. Корицунов, ТУСУР, 3 курс; И.И. Веберова, доцент каф. АОИ
ТУСУР, г. Томск, т. 41-48-57, vi @muma.tusur.ru***

В настоящее время задача формирования единой информационной среды (ЕИС) или единого информационного пространства (ЕИП) на всех уровнях электронного взаимодействия становится все более актуальной. В масштабах страны развернуты программы «Электронная Россия», «Единая информационно-образовательная среда», в каждом регионе – программы создания ЕИП. Организации, предприятия, фирмы, имеющие опыт эксплуатации информационных систем в сфере управления также принимают решение о модернизации систем в этом направлении.

Переход на принципы использования ЕИС обусловлен необходимостью преодоления проблем информационной совместимости автоматизированных ресурсов при внутрикорпоративном или межведомственном взаимодействии на уровне территории.

К основным проблемам обеспечения информационной совместимости на корпоративном уровне относятся:

- действующие программные комплексы (ПК) ориентированы на компьютерную поддержку функций соответствующих подразделений, функционируют автономно, дублируют не только состав хранимых данных, но и сбор одних и тех же данных от подразделений, часто сбор вторичных данных;

- одни и те же классификаторы и справочники в различных ПК актуализируются независимо и с течением времени становятся несопоставимыми, что ограничивает возможность совместного использования информации различных подсистем;

- не обеспечивается достаточный уровень достоверности и своевременности актуализации хранимой информации, особенно информации получаемой от других подразделений;

- эксплуатация и проектирование ПК в подразделениях не осуществляется с учетом других разрабатываемых ПК, и в процессе эксплуатации все, что не работает на текущие потребности подразделения, постепенно становится не адекватным текущему состоянию объектов предметной области.

Перечисленные проблемы являются актуальными и при межведомственном взаимодействии в рамках ЕИП территории.

В настоящее время одной из важнейших проблем развития ИТ-инфраструктуры территории является интеграция разнородных данных.

Довольно часто она понимается как проблема обмена различными форматами данных из различных физических источников. Однако при более детальном осмыслении проблемы становится очевидным, что согласование и правильное понимание информации невозможно без ее содержательного анализа на основе единых справочников и классификаторов. Опыт показывает, что правильным подходом к решению проблемы интеграции данных при межведомственном обмене информацией является создание единой системы классификации и кодирования технико-экономической и социальной информации с применением соответствующих стандартов, методик и программных средств [1].

Использование общероссийских классификаторов для кодирования информационных объектов, участвующих в информационном обмене в рамках ЕИП, является обязательным условием обеспечения согласованности межведомственных потоков информации. Кроме того, необходимо обеспечить сопоставимость классификаторов различных федеральных органов управления и международных организаций, а также информационную совместимость международных и национальных информационных систем. В России во многих регионах создается Единая система классификации и кодирования технико-экономической и социальной информации (ЕСКК). Ее основными составляющими являются общероссийские и территориальные классификаторы [2]. ЕСКК должна включать средства сбора данных и регистрации, анализа и согласования, ведения системы классификации и кодирования информации, предоставления эталонов классификаторов и их рабочих вариантов участникам информационного обмена, в том числе по телекоммуникационным каналам. Созданием такой системы, в настоящее время, активно занимаются государственные службы и частные организации в различных регионах России [3,4].

ЛИТЕРАТУРА

1. Веберова И.И. Создание и ведение единой системы классификации и кодирования технико-экономической и социальной информации / Отчет о научно-исслед. работе, 2006, 45 с.
2. Положение о разработке, принятии, введении в действие, ведение и применение общероссийских классификаторов технико-экономической и социальной информации / Постановление Правительства Российской Федерации от 10 ноября 2003 г. № 677.
3. www.mosreestr.ru.
4. www.budgetrf.ru/Publications/Magazines/VestnikCBR/2000/VestnikCBR26072000/VestnikCBR26072000470.htm

ОСНОВНЫЕ ФАКТОРЫ РАНЖИРОВАНИЯ И ИНДЕКСАЦИИ В ПОИСКОВЫХ СИСТЕМАХ. МЕТОДЫ ПОИСКОВОЙ ОПТИМИЗАЦИИ

Т.С. Кровякова, студент 4 курса каф. АОИ;

Д.А. Соловьев, к.т.н., ст. преп. каф. АОИ

ТУСУР, г. Томск, т. 42-81-23, torangel@yandex.ru

Поисковая оптимизация представляет собой набор методов, направленных на повышение позиций сайта в результирующей выборке поисковой системы. Необходимость применения оптимизации обусловлена следующим. Поисковые системы и тематические каталоги являются основным источником визитов новых посетителей Интернет-ресурсов. Для сайтов отдельной тематики, посетители, пришедшие с поисковых систем, формируют до 80% общего количества заходов, достигаемых путем рекламы в сети Интернет. Доказано, что пользователями поисковых систем просматриваются лишь первые несколько десятков ссылок, найденных по ключевому слову. Высокое позиционирование сайта достигается путем улучшения “видимости” сайта с точки зрения поисковой системы за счет адаптации структуры и содержания сайта к ее требованиям.

Таким образом, для достижения эффективного взаимодействия с целевыми аудиториями необходимо производить поисковую оптимизацию сайта. Причем, чтобы добиться лучших позиций в результатах поиска, необходимо знать о механизмах, используемых поисковыми системами, оценить возможные последствия и риски применяемых методов оптимизации.

Когда пользователь вводит ключевое слово и делает поиск, поисковая система отбирает результаты на основании постоянно меняющихся критериев. Причем решение о выдаче результатов принимается по определенному алгоритму, заложенному в поисковой системе.

Результаты поиска ранжируются на основании следующих факторов:

- Title (заголовок): Присутствует ли ключевое слово в заголовке?
- Domain/URL (Домен/адрес): Присутствует ли ключевое слово в имени домена или в адресе страницы?
- Style (стиль): Есть ли место на странице, где ключевое слово использовано в жирных, курсивных или Hx (H1, H2,...) текстовых заголовках?
- Density (плотность): Как часто ключевое слово употреблено на странице?

- MetaInformation (мета данные): Поисковые системы читают мета ключевые слова (meta keywords) и мета описания (meta description), описанные в мета-тэгах.

- Outbound Links (ссылки наружу): На кого есть ссылки на странице, и встречается ли ключевое слово в тексте ссылки?

- Inbound Links (внешние ссылки): Кто еще в Интернет имеет ссылку на данный сайт? Каков текст ссылки?

- Insite Links (ссылки внутри страницы): На какие еще страницы данного сайта содержит ссылки эта страница?

Как видно, поисковой системе необходимо делать множество уточняющих запросов, используя скаченную страницу целиком.

Кроме знания основных принципов индексации и ранжирования сайта в поисковых системах в общем, для успешного позиционирования сайта необходимо иметь представление об особенностях ранжирования в каждом поисковике в частности, при этом необходимо постоянно следить за изменением применяемых критериев и алгоритмов. Общая характеристика для каждой поисковой системы может быть представлена следующим образом:

- Google – очень большое значение придается внешним ссылкам. База Google используется очень большим числом других поисковых систем и порталов.

- MSN – больший, нежели у других поисковых систем, акцент на информационное содержимое сайта.

- Yandex – крупнейшая российская поисковая система. Уделяет особое внимание тематическим ссылкам. Понижает в рейтинге или исключает из индекса сайты, занимающиеся нетематическим ссылкообменом, а также сайты, участвующие в системах автоматического обмена ссылками.

- Rambler – понижает в рейтинге сайты, активно занимающиеся раскруткой (быстрое увеличение числа внешних ссылок). Ценит наличие поисковых терминов в простом тексте страницы (без выделения различными стилистическими тегами).

- Mail.ru – использует результаты поисковой системы Google после некоторой дополнительной обработки. Оптимизация под Mail.ru сводится к оптимизации под Google.

Таким образом, суть методов поисковой оптимизации заключается в синхронизации алгоритмов поиска поисковых машин и структурных элементов сайтов, их кода, текстов и прочих элементов.

Можно выделить следующие методы поисковой оптимизации:

- Анализ и выбор оптимальных ключевых слов и фраз: подбор ключевых слов и фраз, которые наиболее полно отражают содержимое конкретной страницы сайта.

- Регистрация в поисковых системах и веб-каталогах: при регистрации сайт заносится в базу данных поисковика, то есть, поисковой системе становится известно о существовании данного сайта;
- Увеличение количества ссылок на сайт в Интернете: имеет большое значение при ранжировании, причем, оценивается не только количество ссылающихся сайтов, но и их тематическая направленность;
- Мониторинг положения сайта в поисковых системах, а также веб-страниц конкурентов: позволяет анализировать эффективность принимаемых мер для продвижения сайта;
- SEO копирайтинг: заключается в грамотном составлении текста страниц сайта с учетом специфики деятельности заказчика;
- Отслеживание трафика: анализ состава и качества посетителей сайта. Анализ можно производить по записям лог-файла;
- Оптимизация HTML-кода страниц: написание кода, наиболее полно отвечающего требованиям поисковых систем[1–3].

Кроме этого, существуют стандартные методы оптимизации, такие, как баннерная реклама, контекстная реклама и пр.

При использовании различных методов оптимизации следует помнить о рисках. К факторам риска относится запрет к индексации сайта по причине нарушение правил поисковых систем, изменение алгоритмов ранжирования поисковыми системами, использование «серых» методов продвижения, которые могут трактоваться поисковыми по-разному в зависимости от конкретного случая. [4].

Так или иначе, для проведения качественной оптимизации сайта и достижения высоких результатов следует учитывать множество особенностей применяемых приемов и отлично ориентироваться в сути используемых механизмов.

ЛИТЕРАТУРА

1. <http://www.searchengines.ru/>
2. <http://www.promostat.be/>
3. <http://www.site-seo.ru/>
4. <http://www.webinform.ru/>

ПРИНЦИПЫ ПОСТРОЕНИЯ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ПРОСТРАНСТВЕННОГО АНАЛИЗА ОБЪЕКТОВ ЭЛЕКТРОННОГО ГЕНПЛАНА

***И.С. Лакеев, Е.И. Юркин, ТУСУР, 4 курс
ТУСУР, г. Томск, т. 41-44-70, uei@ms.tusur.ru***

Технологии географических информационных систем (ГИС) применяются уже более тридцати лет. Однако в подавляющем большинстве люди все еще используют эти технологии в основном для создания карт. На самом же деле ГИС может делать гораздо больше. Используя ГИС для анализа, можно узнать, почему объекты взаимосвязаны, где находятся связанные объекты, и каким образом они связаны. Получение этой информации может помочь более глубоко понять ситуацию в данном месте, сделать правильный выбор или лучше подготовиться к предстоящим событиям и условиям.

В направлении оптимального хранения и анализа пространственных данных была выбрана СУБД Oracle 10g. Отличительной особенностью является то, что пространственные данные хранятся в единой базе с атрибутивными данными. Для этого корпорацией Oracle были разработаны дополнительные опции СУБД: встроенный модуль Oracle Spatial, который предоставляет объектный тип данных (SDO_GEOMETRY), содержащий в себе пространственные характеристики объектов, возможность индексирования и функции/операторы для манипуляций с этим типом. Эти механизмы позволяют хранить, запрашивать, быстро и эффективно анализировать пространственные данные внутри одной базы данных Oracle. Кроме того, Oracle Spatial обеспечивает целостность данных, преобразование системы координат и другую базовую логику. Это существенно упрощает работу с пространственными данными, интеграцию различных приложений, а также разработку программных продуктов.

Пространственные данные могут включать любые объекты, представляемые в векторном виде точками, линиями, полигонами.

Точками представляются объекты, не выраженные в масштабе карты – колодцы, опоры, места ремонтов.

Линиями изображаются линейно-протяженные объекты – дороги, ЛЭП, трубопроводы и т.п.

Полигонами отображаются объекты, выраженные в масштабе карты – здания и сооружения, массивы растительности и т.п.

Анализ задач, решаемых в рамках электронного генплана, показывает, что система должна отвечать следующим основным требованиям:

1. Систем должна поддерживать три категории простейших запросов согласно типам объектов: запросы с указанием точки, линии и полигона.

2. Система запросов должна иметь возможность поддерживать вложенные запросы. Результаты одних запросов поступают на вход других.

3. Пользователь может создавать свои комбинированные запросы или простые запросы на основе простых шаблонов или уже имеющих-ся пользовательских запросов с уточнением объекта запроса из первоначальной выборки.

Учитывая основные типы объектов (точка, линия, полигон), все запросы можно разбить на следующие группы, где пользователь указывает объект и место выборки (группа объектов, слой либо выборка из предыдущего запроса):

Запрос с указанием точки:

- Входящие и выходящие дуги;
- Совпадающие объекты (точка в точку);
- Объекты, содержащие внутри себя указанную точку;
- Выборка объектов по буферной зоне.
- Нахождение ближайшего объекта по прямой;
- Нахождение критического пути из одной точки в другую.

Запрос с указанием линии:

- Объекты на конечных точках;
- Пересекаемые объекты;
- Объекты из буферной зоны (полностью или частично попадающие);
- Нахождение критического пути из одной линии в другую;
- Все соприкасаемые объекты, то есть всю соединенную подсеть;
- Объекты, лежащие слева или справа от указанной линии.

Запрос с указанием полигона:

- Выборка объектов внутри полигона;
- Объекты, пересекающие границы полигона;
- Выборка объектов по буферной зоне полигона;
- Выбрать все объекты, имеющие смежные стороны к полигону.

Наряду с этим, необходимо реализовать запросы без указания определенного объекта:

- Все точки, которые являются вершинами полигонов;
- Все полигоны с N сторон;
- Выбрать из выборки объекты определенного типа или слоя;
- Операция инвертирования выборки и др.

Сформулированные в данной работе требования к системе пространственного анализа объектов и принципы ее построения легли в основу разрабатываемого авторами программного средства «Spatial Analyser (SA)», предназначенного для решения определенных задач при ведении электронного генплана ООО «Томскнефтехим».

«УМНЫЕ КЛИЕНТЫ» – ОПТИМАЛЬНЫЙ ТИП КЛИЕНТСКИХ ПРИЛОЖЕНИЙ

Е.В. Никитин, студент 4 курса каф. АОИ;

П.В. Сенченко, к.т.н., доцент каф. АОИ

ТУСУР, г.Томск, т. 41-48-57, eugenenikitin@ngs.ru, pvs@muma.tusur.ru

В настоящее время можно выделить три типа клиентских приложений автоматизированных информационных систем: rich client («толстые клиенты»), thin clients («тонкие клиенты») и smart clients («умные клиенты»). Отметим основополагающие принципы построения всех типов клиентских приложений.

«Толстые клиенты» изначально были спроектированы для получения преимущества при работе с локальными аппаратными ресурсами и клиентскими операционными системами [1]. Несмотря на впечатляющую функциональность многих таких приложений, они имели ограничения. Они были автономными и работали на клиентских компьютерах, практически, не используя его окружение, в которое входит сетевые компьютеры и сервисы. Зачастую, взаимодействие между приложениями ограничивалось передачей малого количества данных через буфер обмена.

Существует множество технологий, которые улучшают возможности взаимодействие «толстых клиентов». Например, двухзвенные приложения позволяют множеству пользователей получить доступ к данным, находящимся в сети, а технология DCOM помогает распределить логику и данные на множестве компьютеров [2].

Однако такого рода системы значительно сложнее разрабатывать. С ростом размеров и сложности программной системы, с усилением взаимосвязи между клиентскими приложениями и сервисами, все больше и больше растет сложность их сопровождения. Также с увеличением сложности и охвата предметной области программной системой, появляются проблемы с инсталляцией системы на рабочие места пользователей. Развертывание одного приложения легко может привести в неработоспособное состояние другое, одна из причин – несовместимость разделяемых компонент или библиотек, данный феномен

называется – application fragility [2]. Поэтому установка новой версии приложения, обычно, требует деинсталляции предыдущей.

Интернет предоставляет альтернативу модели «толстого клиента» и решает многие проблемы связанные с развертыванием и технической поддержкой клиентских частей системы. «Тонкие клиенты» – это приложения, основанные на web-технологиях, которые разворачиваются и обновляются на web-сервере, поэтому нет необходимости устанавливать и настраивать приложения на клиентском компьютере [1]. Такая модель позволяет компаниям эффективно работать с обширной и разнообразной группой внешних пользователей, таких как заказчики и партнеры.

Несмотря на простоту установки «тонкие клиенты» имеют ряд недостатков. Браузер должен постоянно иметь соединение, это означает, что мобильные пользователи не имеют доступ к приложению, если соединение было разорвано, что происходит часто на мобильных устройствах, поэтому пользователям приходится заново вносить данные в систему. Также «тонким клиентам», в большинстве случаев, не доступны такие технологии как drag-and-drop, undo-redo и контекстно-зависимая помощь. Так как вся логика приложения располагается на сервере, «тонкий клиент» постоянно обращается к серверу за данными и обработкой. Браузер должен дожидаться ответа от сервера, прежде чем пользователь продолжит работу. Эти проблемы усугубляются при плохих каналах связи.

Для «умного клиента» характерно объединение преимуществ «толстого» и «тонкого клиентов». «Умные клиенты» были разработаны с целью объединения удобств работы «толстых клиентов» и легкости развертывания и технической поддержки «тонких клиентов». «Умные клиенты» различаются в плане технической реализации, однако, имеют основные общие черты [2]:

- активное использование локальных ресурсов
- активное использование сетевых ресурсов
- поддержка время от времени подключенных пользователей (occasionally connected users)
- поддерживают интеллектуальную инсталляцию и обновление
- поддерживают разнообразные клиентские устройства (настольные компьютеры, КПК, смартфоны)

Грамотно спроектированный «умный клиент» обеспечивает богатый пользовательский интерфейс и мощную возможность клиентской обработки информации. Он должен позволять производить сложные манипуляции с данными, качественную визуализацию, поиск и операции по сортировке. «Умный клиент» может использовать клиентские аппаратные ресурсы (телефоны, сканеры штрих-кодов), а также кли-

ентское программное обеспечение, такое как Microsoft Office или другие line-of-business (LOB) приложения [2]. «Умный клиент» должен интегрироваться с другими программными решениями и координировать их для достижения максимальной эффективности работы пользователя. «Умный клиент» активно использует язык XML и технологию XML Web Services для интеграции в единую распределенную информационную систему.

«Умные клиенты» должны максимально использовать различные сервисы в сети для получения данных из множества различных источников, что необходимо пользователю при проведении анализа данных.

«Умный клиент» должен быть спроектирован таким образом, чтобы обеспечивать поддержку время от времени подключенных пользователей. Это означает, что система в целом должна функционировать оптимально даже при медленных каналах связи или в случаях временной отключения сетевых соединений. «Умный клиент» должен управлять соединениями так, чтобы пользователь работал максимально эффективно. Одним из важнейших преимуществ использования «умного клиента» является обеспечение максимальной функциональности даже при работе offline.

Кроме того, «умные клиенты» должны быть спроектированы так, чтобы обеспечивалось их гибкое развертывание и сопровождение. Существует несколько вариантов развертывания «умных клиентов»:

- простое копирование файлов на локальный компьютер;
- автоматическое скачивание модулей программной системы с центрального сервера, используя бесконтактное (no-touch) развертывание;
- используя инсталляционные пакеты Windows Installer и Microsoft Management Server (SMS)

.NET (dot Net) Framework, на основе которого разрабатываются «умные клиенты», позволяет назначить строгие имена компонентам приложения, что гарантирует использование компонентов именно той версии, которая необходима пользователю. .NET Framework изолирует приложения друг от друга, установка одного приложения никак не скажется на работе другого. Все эти возможности упрощают развертывание клиентской части и позволяют избегать проблемы, связанные с «толстыми клиентами».

Исходя из вышеизложенного, можно сделать вывод о целесообразности использования «умных клиентов» при разработке современных распределенных информационных технологий.

ЛИТЕРАТУРА

1. *Скот Хильер*. Создание COM+ приложений в среде Visual Basic: Вильямс, 2001. 412 стр.
2. MSDN Library for Microsoft Visual Studio 2005 beta 2.

ТЕХНОЛОГИЯ ВЕДЕНИЯ ПРОСТРАНСТВЕННЫХ ДАННЫХ ОБ ОБЪЕКТАХ ИНЖЕНЕРНОЙ ИНФРАСТРУКТУРЫ В WEB-ОРИЕНТИРОВАННЫХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ

С.С. Ощенко, ТУСУР, 4 курс

ТУСУР, г. Томск, т. 41-43-11, oss@muma.tusur.ru

Одной из проблем, возникающих при работе с электронными картами в Web-приложениях, является то, что объекты на всех слоях этих карт статичны, т.е. пользователь может только просматривать информацию о них, для редактирования же данных необходимо создавать новый модуль, предназначенный для реализации этих функций. Также существуют и играют важную роль такие объекты, которые можно назвать временными, то есть эти объекты должны обозначаться на электронной карте по мере необходимости и существовать какое-то определенное время, по истечении которого их необходимо удалять, а информацию об этом событии помещать в архив.

В качестве примера можно рассмотреть такое событие, как ремонт. Если на крупном предприятии, какой либо объект выходит из строя (будь то линия связи, коммуникаций или же имеет место ремонт какого-нибудь производственного цеха) то необходимо в кратчайшие сроки устранить эту неполадку и обозначить этот объект как находящийся в процессе ремонта. Для этих целей необходим механизм, способный реализовать эти функции. Когда ремонт закончится, необходимо удалить с электронной карты его обозначение. Также можно рассмотреть ситуацию с внесением информации о каких-либо новых объектах электронного генплана, когда пользователь, зная координаты месторасположения объекта, может занести данные об объекте, работая с картой непосредственно через Web-браузер.

В Web-ориентированных геоинформационных системах проблема динамического создания и удаления объектов при работе с электронной картой стоит наиболее остро, так как нет какого-либо стандартного средства, реализующего возможность создания собственных объектов на электронной карте с последующим занесением атрибутивной информации о них в базу данных.

Для решения данной проблемы была поставлена задача: предоставить пользователю возможность работы с объектами электронной карты (добавление, удаление, редактирование данных) из web-приложения.

Для решения данной задачи необходимо осуществить связь между клиентским приложением и базой данных, в которой хранятся пространственные данные об объектах электронной карты.

Такая связь может быть реализована с помощью следующих средств:

- Autodesk MapGuide;
- Oracle Spatial.

В Autodesk MapGuide – наиболее широко распространенном комплексе программных средств, предназначенных для обеспечения доступа через Интернет к интерактивным картам, чертежам, различной пространственно увязанной информации, есть возможность создания собственных объектов и собственных слоев.

Oracle Spatial (дополнение к СУБД для хранения географической информации) предоставляет SQL-схему и функциональность, которые способствуют хранению, получению и изменению пространственных данных в Oracle9i.

Spatial состоит из следующих компонентов:

- схема (MDSYS), которая предопределяет хранение, синтаксис и семантику поддерживаемых геометрических типов данных;
- механизм пространственного индексирования;
- набор операторов и функций для выполнения пространственных запросов и аналитических операторов;
- набор административных утилит.

В комплексе Autodesk MapGuide имеется модуль Autodesk MapGuide Provider для Oracle Spatial, который позволяет непосредственно, без каких-либо преобразований, работать с данными, хранимыми в базах данных Oracle Spatial.

Учитывая изложенное выше был разработан механизм, который позволяет динамически создавать объекты и заносить атрибутивную информацию о них в базу данных. Пользователь также может редактировать данные об объекте и удалять его по мере надобности.

Принцип реализации данного механизма заключается в следующем: при выборе опции “создание объекта” на электронной карте создается временный слой типа «redline» – это единственный тип из всех существующих в Autodesk MapGuide, на котором можно создавать собственные объекты любого типа: линейные, площадные или точечные. Затем, при выборе объекта, информация о нем (геометрические координаты, определяющие его местоположение на карте, идентификатор, название самого объекта и названия слоя, которому принадлежит данный объект) посылаются на сервер, где она обрабатывается php-скриптом и заносится в базу данных Oracle. Далее, при обновлении карты, этот объект отображается на постоянном слое карты, используя данные, которые хранятся в базе данных.

Универсальность данного механизма состоит в том, что он может использоваться со всеми типами объектов (полигон, линия, точка или текст), также данная технология может применяться при работе как с вновь созданными объектами, так и с уже существующими на электронной карте.

Описанный механизм был реализован в подсистеме «WebГИС» в составе геоинформационной технологии создания и ведения электронного генерального плана ООО «Томскнефтехим» при работе с местами ремонтов на объектах этого предприятия.

ТЕХНОЛОГИЯ WEB-ОПУБЛИКОВАНИЯ ПРОСТРАНСТВЕННЫХ ДАННЫХ

А.В. Отчалко, ТУСУР, 3 курс

ТУСУР, г. Томск, т. 41-44-70, alexey_otchalko@mail.ru

Сегодня, с развитием технологий автоматизации, когда различные географические информационные системы (ГИС) становятся неотъемлемой частью автоматизированных комплексов, возникает растущая потребность в хранении и обработке пространственных данных. Это позволяют сделать различные системы управления пространственными базами данных (СУПБД) во взаимодействии с инструментальными ГИС. Но здесь кроется другая проблема: необходимо обеспечить удобное совместное использование пространственных данных и элементы управления ими большому числу пользователей и свести при этом к минимуму затраты на внедрение. На практике, в больших распределенных системах, наилучшим образом этим критериям удовлетворяет технология web-доступа [1]. Рассмотрим подробнее некоторые аспекты практического применения данной технологии.

Со стороны клиента для реализации технологии web-опубликования пространственных данных требуется лишь наличие компьютера с выходом в Internet/Intranet и web-браузера [1]. Введение именно такого минимального набора инструментов позволяет добиться следующих преимуществ для заказчика:

- значительно снижаются финансовые затраты на внедрение ГИС на крупных предприятиях за счет отказа от покупки лицензионного клиентского программного обеспечения;
- уменьшается время обучения персонала работе с новым программным продуктом – все действия происходят в привычной для пользователя среде web-браузера;

- доступ к ГИС может быть произведен с любого компьютера предприятия.

Но такая конфигурация рабочего места имеет существенный недостаток: возможно отображение лишь растровой графики. Это очень нерационально с точки зрения сетевого трафика и накладывает ограничения на возможности взаимодействия пользователя с ГИС. Для реализации поддержки векторной графики на стороне пользователя целесообразно использовать специальные надстройки (add-ons) браузера (например, ActiveX компонент Autodesk MapGuide Viewer ActiveX Control для web-публикатора пространственных данных Autodesk MapGuide). Также использование таких надстроек позволяет расширить возможности пользователя по взаимодействию с ГИС и облегчают работу программистов по реализации многих функций ГИС-сервера. При этом программист должен выложить данные надстройки на сервер, чтобы обеспечить удобное скачивание при необходимости.

Со стороны сервера технология web-доступа требует обеспечения обработки поступающих запросов, выполнения необходимых вычислений и манипуляций и возвращения запрошенной пользователем информации. Обработку запросов и часть вычислений можно возложить на языки «web-программирования» (PHP, ASP и др.), манипуляции с пространственными данными – на СУБД, а возвращение информации пользователю находится на стыке этих двух механизмов. При этом все должно происходить в динамическом режиме, чтобы получаемая информация являлась наиболее актуальной. Тогда можно выделить следующие преимущества реализации доступа к пространственным данным с помощью web-технологий:

- возможна тонкая подстройка ГИС под нужды заказчика, реализация специфичных функций;
- динамическое взаимодействие пользователя с ГИС;
- легкое администрирование и сопровождение проекта.

Также нельзя забывать и о реализации параллелизма в web-ГИС. Наилучшим выходом из создавшейся проблемы, на наш взгляд, является хранение в базе данных (БД) всей информации о пространственных данных, составными частями которой являются:

- описательная информация о присутствующих в ГИС объектах, пользователях и функциях ГИС;
- собственно пространственная информация об объектах ГИС.

Пользовательский интерфейс системы включает множество HTML-документов с включениями элементов JavaScript [1]. Для обеспечения динамичности, данные документы должны формироваться на основе описательной информации из БД по шаблонам. Кроме того,

появляется проблема динамического формирования специфического для каждого web-публикатора файла, который затем будет передан клиенту для отображения векторной графики. Не лишним будет и предусмотреть механизм формирования растрового изображения карты для пользователей, которые по каким-либо причинам не могут скачать и установить надстройку на web-браузер.

Подводя итоги, можно сказать, что технология web-опубликования пространственных данных имеет множество преимуществ, как для заказчика, так и для программиста. Но вместе с этим она довольно сложна в плане практической реализации – необходимо организовать сложное взаимодействие БД, web-публикатора и HTML-содержимого сервера в динамике. Более сложным становится и реализация контекстно-зависимой помощи пользователю. Несмотря на это, данная технология находит все большее и большее применение, причем не только в глобальной сети Internet, но и в локальных корпоративных Intranet сетях предприятий.

ЛИТЕРАТУРА

1. *Ш. Шекхар, С. Чаула*. Основы пространственных баз данных. М.: КУДИЦ-ОБРАЗ, 2004

ПОДСИСТЕМА ВЕДЕНИЯ АРХИВНЫХ ДОКУМЕНТОВ В СРЕДЕ ЭЛЕКТРОННОГО ГЕНЕРАЛЬНОГО ПЛАНА

Н.Б. Рыбалов, ТУСУР, 5 курс

ТУСУР, т. 41-47-09, fisher@muma.tusur.ru

На каждом крупном промышленном предприятии существует генеральный план его территории, содержащий информацию об объектах инженерной инфраструктуры. Этот документ определяет прохождение всех коммуникаций, например таких как: водопровод, канализация, сети связи и т.д. Документ в составе проекта разрабатывается как чертеж (карта) или комплект чертежей (карт), на котором в определенном масштабе показано взаимное расположение всех зданий и сооружений, транспортных и энергетических коммуникаций в увязке с рельефом местности и планировочными решениями на площадке с учетом требований технологии и транспорта. Генплан используется инженерными подразделениями для планирования и организации ремонтных и строительных работ, а также для согласования участков нового строительства с другими подразделениями. За ведение данного документа отвечает подразделение генплана.

Многие предприятия ведут электронный вариант генерального плана. В качестве сред проектирования часто используются такие ГИС, как Autodesk Map и MapInfo. Доступ к электронной карте может быть реализован двумя способами: в виде клиентского приложения, работающего с файлом карты, либо в виде Web-приложения, которое взаимодействует с ВЕБ-ГИС сервером. Последний вариант более удобен с точки зрения актуализации данных и удобства конечного пользователя, так как для доступа к приложению необходим любой компьютер, имеющий доступ к сети Internet/Intranet, но накладывает ограничения на реализацию функциональных возможностей.

Архитектура ВЕБ-ГИС сервера включает в себя следующие компоненты:

- СУБД Oracle Spatial – используется в качестве хранения и анализа пространственных данных;
- Autodesk MapGuide (Server, Dynamic Authoring Toolkit) – публикатор пространственных данных, обеспечивает связь с Oracle Spatial и динамическое формирование карты;
- Microsoft Internet Information Services – web-сервер, обрабатывающий запросы пользователей.

С течением времени в различных подразделениях предприятия может накапливаться большое количество смежной информации. Например, в подразделении генплана – это сопроводительная документация, фотоснимки инженерных коммуникаций, регламенты на проведения строительных и ремонтных мероприятий. В других подразделениях – более узкая техническая информация об инженерных сетях, история проведения ремонтов, наиболее проблемные и опасные участки сетей и т.д. На предприятии, использующем электронный генеральный план, смежная информация может храниться и в электронном виде.

Большое количество и разнообразие документов, содержащих информацию о характеристиках и состоянии элементов инженерных сетей, затрудняет анализ их технического состояния и планирование ремонтно-профилактических работ. Материалы, содержащиеся в архивах подразделений, не до конца упорядочены, отсутствует точная информация о находящихся в архиве документах. Атрибутивные описания объектов инженерной инфраструктуры находятся на бумажных носителях и носят фрагментарный, неупорядоченный характер, что ставит потенциальную работоспособность инженерных объектов в большую зависимость от состояния отдельных исполнителей.

Для повышения эффективности действий подразделений при планировании и организации строительных и ремонтных работ, была разработана технология, обладающая функциями хранения, привязки,

поиска и получения данных из архивов. Созданная на основе этой технологии система «Архив» предоставляет пользователям электронного генерального плана возможность прикреплять к различным объектам, слоям и областям карты документацию и мультимедийную информацию.

Доступ к архиву документов может получить каждый зарегистрированный на ВЕБ-ГИС сервере и прошедший авторизацию пользователь. Система имеет двух основных пользователей: технический администратор и пользователь.

- Технический администратор – человек, имеющий доступ на проведение операций добавления, редактирования, удаления документов архива. Он также имеет право редактировать словари областей, типов, видов документов.

- Пользователь – любой человек, имеющий доступ к ВЕБ-ГИС серверу. Ему доступен поиск документов и просмотр. Права на просмотр документов определяются из доступа на соответствующие слои карты. Если пользователь имеет доступ к слою, то, следовательно, он имеет доступ к документу, который прикреплен к нему, и к документу, прикрепленному к объекту слоя. Документы, прикрепленные к областям карты для просмотра доступны всем.

Возможности программы. Система ведения документации электронного генерального плана состоит из двух подсистем: администрирования и предоставления документации. Система администрирования включает в себя функции ведения архива, привязки документов к слоям, областям и объектам карты. Система предоставления документации обладает функциями поиска документов на карте, генерации списка документов по указанной точке карты и загрузки найденного документа.

Основными достоинствами данной технологии являются:

- Инженерные подразделения могут получить самые последние версии документов. Администраторы нескольких подразделений могут оперативно реагировать на требования пользователей и публиковать самые актуальные данные;

- Ограничение доступа к документации. Привязка документов может осуществляться к слою, к слою + область, к объектам. Следовательно, для получения документа необходимо иметь доступ к соответствующему слою;

- Пользователи могут легко отслеживать поступление новых документов. Пользователь имеет доступ к списку документов, из которого осуществляется переход к связанной области генплана, а также доступна загрузка документа.

Описанная технология была применена в проекте «Информационная технология создания и ведения электронного генерального плана ООО «Томскнефтехим». Ее использование позволило:

- Пользователям ВЕБ-ГИС сервера своевременно получать интересующую документацию о различных инженерных коммуникациях и областях генерального плана;
- Снизить риск материальных затрат на устранение возможных ошибок строительства и аварий, связанных с несогласованными действиями различных подразделений;
- Решить проблему отсутствия доступа к необходимой документации о предполагаемой области, объекте ремонта или строительства.

**ПРИНЦИПЫ ПОСТРОЕНИЯ ЕДИНОЙ СИСТЕМЫ
КЛАССИФИКАЦИИ И КОДИРОВАНИЯ ИНФОРМАЦИИ**
*А.С. Сергеев, ТУСУР, 3 курс; И.И. Веберова, доцент каф. АОИ
ТУСУР, г. Томск, т. 41-48-57, vi@muma.tusur.ru*

Единая система классификации и кодирования технико-экономической и социальной информации (ЕСКК) представляет собой совокупность общероссийских, ведомственных и территориальных классификаторов и справочников технико-экономической информации, нормативных и методических документов по их разработке, ведению и применению в информационно-вычислительных и телекоммуникационных комплексах.

Главной целью создания и ведения единой системы классификации и кодирования информации является обеспечение информационной совместимости автоматизированных информационных ресурсов территории для межведомственного взаимодействия [1].

Основными задачами ЕСКК являются:

- создание условий для формирования единого информационного пространства территории;
- систематизация информации по единым классификационным правилам и их использование при прогнозировании социально-экономического развития территории;
- обеспечение совместимости информационных ресурсов и систем, участвующих в межведомственном обмене данными;
- обеспечение межотраслевого обмена территориальными информационными ресурсами;

- обеспечение согласованного информационного взаимодействия органов власти, предприятий и организаций;

- гармонизация ЕСКК с общероссийскими и международными классификациями и стандартами.

Методы и средства создания ЕСКК территории должны опираться на следующие принципы:

- Эволюционность, или поэтапный переход к современным технологиям ведения СКК, обеспечивающий существование старых и новых систем классификации и кодирования;

- Адаптивность ЕСКК к специфике существующих систем классификации и кодирования информации АИРИС и способность интегрироваться с внешними системами;

- Преимущество, или способность сохранить все лучшее и ценное, накопленное десятилетиями, позволяющее использовать потенциал специалистов в области классификации и кодирования научно-справочной информации (НСИ);

- Стандартизация и унификация регламентов и методики использования и сопровождения НСИ в масштабах территории.

- Учет человеческого фактора, а именно субъективных мнений экспертов НСИ при классификации и кодировании, т.е. отнесение объекта классификации к той или иной классификационной группировке или признаку классификации.

ЕСКК должна функционировать исходя из некоторых общих принципов: открытость и доступность ЕСКК для пользователей; обеспечение методического и организационного единства ЕСКК; комплексность ЕСКК, предусматривающая наиболее полный охват технико-экономической и социальной информации, используемой при межотраслевом обмене; постоянная актуализация системы классификации и кодирования [2].

Объектами классификации и кодирования в ЕСКК являются технико-экономические и социальные объекты и их свойства, используемые в различных видах экономической деятельности и при межотраслевом обмене информации в рамках территории. Субъектами деятельности в рассматриваемой предметной области являются: органы власти, владельцы автоматизированных информационных ресурсов и систем (АИРИС), источники актуализации, эксперты, оператор ЕСКК, пользователи.

Процесс создания и ведения ЕСКК можно разбить на следующие составляющие: сбор данных и регистрация НСИ; анализ и согласование данных; разработка и внедрение классификаторов; ведение ЕСКК; предоставление и использование; управление единой системой классификации и кодирования.

Ведение ЕСКК предполагает поддержание классификаторов и справочников в достоверном и актуальном состоянии, автоматизированное внесение изменений в электронные версии общероссийских и территориальных классификаторов, ведение истории изменений.

Управление и контроль функционирования ЕСКК осуществляет соответствующий орган государственной власти или по его поручению Оператор.

Функциональные возможности ЕСКК должны соответствовать основам деятельности, изложенным в нормативно-правовых документах, и учитывать мировой опыт и опыт создания ЕСКК в других регионах России [3,4]. Создание и внедрение ЕСКК территории позволит значительно повысить эффективность информационного взаимодействия и обеспечить лингвистическую совместимость автоматизированных информационных ресурсов и систем.

ЛИТЕРАТУРА

1. Веберова И.И. Создание и ведение единой системы классификации и кодирования технико-экономической и социальной информации / Отчет о научно-исслед. работе, 2006, 45с.
2. Положение о разработке, принятии, введении в действие, ведение и применение общероссийских классификаторов технико-экономической и социальной информации/Постановление Правительства Российской Федерации от 10 ноября 2003 г. № 677.
3. www.mosreestr.ru.
4. www.budgetrf.ru/Publications/Magazines/VestnikCBR/2000/VestnikCBR2607200/VestnikCBR26072000470.htm

ПОСТРОЕНИЕ КОМПЬЮТЕРНОЙ СЕТИ ДЛЯ IP ТЕЛЕФОНИИ

*Д.Г. Осетров, инженер каф. СВЧиКР; З.А. Шелковников,
С.С. Чаунин, С.А. Шибельгут, Я.А. Глушков, студенты 5 курса РТФ
ТУСУР, г. Томск, т.42-81-40, loykozak@mail.ru.*

Реализация полноценной компьютерной сети для IP-телефонии с возможностью подключения любого абонента, имеющего широкополосный либо кабельный доступ в интернет.

Рынок IP-телефонии во всем мире растет быстрыми темпами. Согласно исследованию, проведенному аналитической фирмой TeleGeography, в начале 2005 г. количество пользователей услуги Voice over Internet Protocol составляло 1,3 млн. человек, но уже через три месяца на услуги VoIP подписалось еще 900 тыс. человек, а к концу года

количество пользователей составило 4,5 млн. человек. TeleGeography полагает, что в ближайшие три-четыре года сфера VoIP будет стабильно прибавлять около 3 млн. пользователей в год.

Такую популярность IP-телефония получила благодаря следующим своим преимуществам перед традиционной телефонией: сокращение затрат на поддержку и обслуживания телефонии (включает в себя дополнительные услуги типа адресных книг, конференц-связи, автоответчика и т.п.); гибкое размещение абонентов (перемещение абонентов не требует перенастройки УАТС). Все эти сервисы стали возможными благодаря нарождающемуся новому классу конвергентных сетей.

Перевод корпоративной телефонии с традиционных телефонных линий и средств (УАТС, телефонные аппараты) на IP-основу позволяет повысить качество, функциональность и эффективность услуг связи в рамках компании при значительном сокращении издержек на обслуживание корпоративных коммуникаций и обеспечивает базу для дальнейшего расширения функций связи (включая построение конвергентных сетей, ЦОВ, интегрированных с CRM и ERP систем).

Конвергентные сети позволяют объединить телефонные услуги (включая голосовую и факсимильную связь), электронную почту, интернет-услуги, передачу данных и мультимедиа (включая документооборот компании, видеосвязь и др.) в рамках единой корпоративной сети, позволяя достичь:

- уникальной функциональности на каждом рабочем месте (работа с любыми видами информации);
- существенной экономии за счет многофункциональности терминалов конечных пользователей и упрощения корпоративных сетей;
- повышения производительности труда в компании как за счет упрощения коммуникаций между сотрудниками, так и за счет возможности масштабной автоматизации коммуникаций.

Конвергентные сети предусматривают также возможности администрирования, ведения отчетности и интеграции с бизнес-системами. В качестве потребителей услуг могут выступать операторы на ПК, КПК, удаленные пользователи, менеджеры и автоматические службы.

Здесь решается задача реализации компьютерной сети для IP-телефонии с возможностью подключения любого абонента, имеющего широкополосный либо кабельный доступ в интернет. Для реализации данной задачи была проведена оценка количества потребителей услуг VoIP в г. Томке и Томской области, на основании которой было принято решение о разработке собственной модели USB телефона для IP-телефонии.

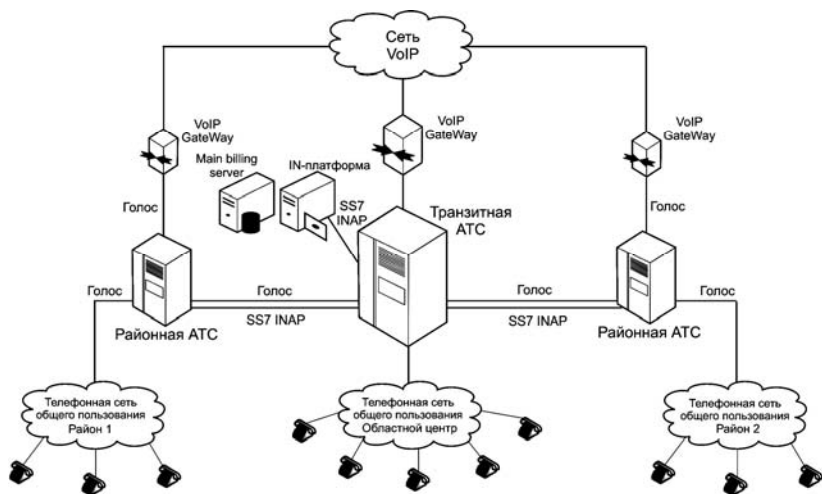


Рис. 1. Сеть IP-телефонии

На рис. 1 показано решение подключения сети IP-телефонии к ТФОП. Одним из основных требований к создаваемой сети было отсутствие особой привязки к какому-либо стандартному или специфическому оборудованию. На практике это означает не только упомянутую выше способность работать с широким спектром доступного оборудования, но и возможность максимально гибкого использования существующего оборудования заказчика. Архитектура сети может быть как распределенной по множеству серверов (например, с целью повышения эффективности обслуживания удаленных офисов компании, а также повышения надежности системы), так и сосредоточенной на единственном сервере (при условии его достаточной производительности) без ограничений на количество функций системы.

ЛИТЕРАТУРА

1. *Центры обслуживания вызовов (Call Centre)* (Росляков А.В., Самсонов М.Ю., Шибаева И.В.). М. 2002, Эко-Трендз. 343 с.
2. *Call Center на 100%. Практическое руководство по организации Центра обслуживания вызовов* (Самолубова А.Б.). М. 2004, Альпина Бизнес Букс. 467 с.
3. www.itconnection.ru
4. www.astera.ru

ТЕХНОЛОГИИ ИНТЕРАКТИВНОГО ВЗАИМОДЕЙСТВИЯ ВЕБ-ПРИЛОЖЕНИЙ В СРЕДЕ ИНТЕРНЕТ

В.В. Силич, ТУСУР, аспирант кафедры АОИ

ТУСУР, г. Томск, т. 55-34-08, acid@ms.tusur.ru

Как правило, даже простой современный сайт – больше чем набор текстов с картинками. Посетители видят только единство оформления, а разработчики знают, что за этим единством скрывается еще и общее программное ядро. Сайт – это фактически программа. То есть цельная система, с архитектурой, аналогичной структуре настольных приложений, за тем исключением, что специфика Интернет накладывает свои ограничения на работу системы.

В упрощенном виде, традиционную модель интерфейса веб-приложений можно свести к последовательности нескольких этапов. Пользователь запрашивает страницу с сайта, которая создается на сервере, а затем пересылается браузеру. У данной страницы есть HTML-элементы, описывающие форму, в которую пользователь вводит данные. После этого пользователь отправляет данные на сервер и получает новую страницу, основанную на введенных данных, и процесс повторяется. Весь этот процесс определяется самой природой HTTP-протокола и отличается от того, как происходит работа с обычными приложениями, интерфейс которых неразрывно связан с программной логикой. Поэтому, самой яркой особенностью веб-приложений является оторванность интерфейса от ядра – данные хранятся и обрабатываются на сервере, а отображаются клиентом.

Данные ограничения протокола HTTP влекут за собой один очень неприятный момент – любое действие с данными вызывает перезагрузку страницы. Скажем, когда на каком-либо сайте, пользователь нажимает на кнопку «Голосовать», чтобы принять участие в интерактивном опросе, страница заново перегружается. Или когда в галерее фотографий происходит переход к очередному снимку, вместе с ним снова запрашиваются все неизменившиеся части страницы. Т.е. для того чтобы получить данные от пользователя и среагировать на них, системе необходимо произвести полную перезагрузку страницы. Даже если изменится лишь малая часть содержания страницы, а остальные компоненты останутся прежними, при обновлении страницы обязаны будут загрузиться все ее элементы заново, что приводит к избыточной нагрузке на сервер и каналы связи. Такая избыточность оборачивается для пользователя лишними мегабайтами трафика, а также минутами и часами, потраченными на ожидание перезагрузки. Это является большой проблемой для клиента.

В результате, стали появляться попытки разработчиков обеспечить интерактивное взаимодействие клиента с сайтом, без необходимости часто перегружать страницу. При этом все предложенные подходы должны были не выходить за рамки протокола HTTP, на котором основывается вся работа с веб-приложениями.

Одним из первых решений для загрузки данных на страницу без ее полной перезагрузки стало использование тега `<IFRAME>`. Этот тег появился впервые в стандарте HTML 4.0, и предназначен для вставки «внутритекстового фрейма» на веб-страницу. Фактически при помощи этого элемента можно было создать «окно в окне», т.е. разместить на странице еще одну независимую страницу. Поэтому с использованием этого элемента стало возможным отправлять необходимые данные на сервер не с самой страницы, на которой находится пользователь, а с окна `<IFRAME>`, которое может перегружаться не вызывая перегрузку основного окна. Однако данный подход ознаменуется несколькими значительными недостатками [1]. Прежде всего, это то, что при использовании `<IFRAME>`, раздается характерный щелчок, и в журнале истории браузера остаются записи о работе с фреймом, в результате чего стандартная навигация браузера кнопкой Back (Назад) начинает работать неправильно. Другой недостаток `<IFRAME>` – большой расход памяти и медлительность: фактически, для каждого фрейма создается новый отдельный браузер, который независимо обрабатывает загруженный HTML-код. Также не последнюю роль играет невозможность при данном подходе загрузки в окно фрейма большого объема данных, т.к. взаимодействие с сервером происходит через метод GET, применение которого накладывает ограничение на посылку данных более 2083 символов.

В результате, большинство разработчиков были вынуждены отказаться от использования `<IFRAME>` для обеспечения интерактивного взаимодействия. Также были попытки использования технологии Flash для этих целей, однако, в силу тяжести конечного объекта, а также отсутствие полной поддержки этой технологии браузерами (для ее работы требуется дополнительный plug-in) привело к тому, что эти разработки не были внедрены в массовое использование. По этой же причине не прижились и Java-апплеты. Однако решение все же было найдено – подход AJAX.

AJAX – аббревиатура от Asynchronous JavaScript And XML (Асинхронный JavaScript и XML). Это техника, описанная впервые Джесом Джеймсом Гарретом, представляет собой комплекс решений, используемый веб-разработчиками для создания интерактивных веб-приложений, при котором web-страница, не перезагружаясь, сама дог-

ружает нужные пользователю данные. Т.е. фактически AJAX – это не конкретный язык программирования или представления данных, а подход, объединяющий в себе приемы использования других технологий, таких как DHTML (XHTML/HTML, Javascript, CSS, DOM), XMLHttpRequest, XML [2].

В AJAX-приложениях HTML-страница, пересылаемая сервером Web-браузеру, содержит не только видимый контент страницы, но и активный клиентский программный модуль. Этот модуль работает в фоновом режиме, когда страница выводится в окне браузера, и взаимодействует с сервером в асинхронном режиме. В техническом же плане, движок AJAX основан на компоненте XMLHttpRequest, которая встроена во все современные браузеры [3]. При наступлении определенного события на странице, создается объект XMLHttpRequest, которому передаются необходимые параметры, основанные на введенных пользователем данных. Затем этот объект в фоновом режиме посылает запрос на сервер и получает оттуда ответ в виде данных (оформленных в виде XML или любом другом формате). И, наконец, объект AJAX преобразует эти данные в нужный формат и выводит в нужном месте на странице. В таком виде могут быть подгружены на страницу необходимые данные без полной ее перезагрузки. Наиболее наглядными примерами, демонстрирующими работу веб-приложения по схеме AJAX, являются Google Maps (<http://maps.google.com>) и Gmail (<http://gmail.com>).

Таким образом, в настоящее время существует достаточно развитый подход (AJAX), с применением которого, можно приблизить удобство и функциональность работы с веб-приложениями к настольным программам. С его использованием можно повысить эффективность работы как с отдельными модулями сайта (формами, голосованиями и т.д.), так и полностью реализовать динамический веб-сайт минуя обновление всей страницы.

ЛИТЕРАТУРА

1. *Subsys_JsHttpRequest*: динамическая подкачка данных без перезагрузки страницы (AJAX) [электронный ресурс]. – режим доступа: http://dklab.ru/lib/Subsys_JsHttpRequest/
2. *Ajax* (programming) [электронный ресурс]. – режим доступа: <http://en.wikipedia.org/wiki/AJAX>
3. *Ajax: A New Approach to Web Applications* [электронный ресурс]. – режим доступа: <http://adaptivepath.com/publications/essays/archives/000385.php>

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ AUTODESK MAPGUIDE LITEVIEW ДЛЯ ПРЕДСТАВЛЕНИЯ ДИНАМИЧЕСКИХ РАСТРОВЫХ КАРТ В WEB-ПРИЛОЖЕНИЯХ

А.В. Степанов, ТУСУР, 4 курс

ТУСУР, г. Томск, т. 41-43-11, onegin-1985@mail.ru

Широкое распространение геоинформационных систем (ГИС) объясняется их способностью совмещать графическое представление совокупности площадных, линейных и точечных объектов карты или плана (схемы) с хранением в базах данных (БД) атрибутивной информации, описывающей свойства и взаимосвязи этих объектов. Особенно актуальным является создание электронных карт для общественного пользования. Можно предложить два способа реализации такого проекта, это в виде Windows – приложения, либо в виде Web – приложения. Вариант реализации проекта в виде Web – приложения более удобен с точки зрения конечного пользователя, так как приложение становится доступным с любого компьютера имеющего доступ к сети Internet/Intranet. В работе рассматривается реализация проекта на основе платформы AutoDesk.

Клиентская часть приложений предоставляет пользователю возможность просмотра электронной карты в векторном (ActiveX компонент или Java апплет, встраиваемый в HTML страницу) или в растровом виде. В векторном варианте значительно просто реализуется получение и вывод атрибутивной информации об объектах карты, но предполагает установку на компьютере клиента специальных модулей. Для установки модуля его необходимо предварительно получить с сервера, что ведет к дополнительным затратам времени и неудобству для конечного пользователя, к тому же установка возможна только при наличии у пользователя прав администратора на локальном компьютере.

При использовании растрового варианта, на сервере из источников пространственных данных формируются запрошенная область карты, а затем посылается в виде файла растрового формата данных по запросу обратно в браузер. К тому же реализация всех функциональных возможностей ложится на серверную сторону. Мы будем рассматривать реализацию проекта с использованием растрового варианта.

Просматривать карты в браузере без установки plug-in позволяет Autodesk MapGuide LiteView – Java-программа, запускаемая как серверное приложение и конвертирующая MWF в формат PNG. Autodesk MapGuide LiteView делает проекты и карты доступными любому пользователю, на какой бы платформе он ни работал и каким бы браузером он ни пользовался. Ускоряет доступ к информации в формате интерактивных растровых изображений (PNG).

Рассмотрим функции, которые были разработаны при работе с Autodesk MapGuide LiteView и способы их реализации.

- Навигация по карте – навигация осуществляется при помощи кнопок, которые позволяют двигаться в восьми основных направлениях.

- Масштабирование карты.

- История действий – все ваши действия по перемещению и масштабированию сохраняются. Вы можете поочередно отменить ряд произведенных вами действий. А если случайно отменили действие, то можете воспроизвести его снова.

- Режим панорамирования карты – когда данный режим активен, вы можете при помощи мыши перетаскивать область карты.

- Режим получения информации об объекте – когда данный режим активен, по щелчку мыши отображается окно с характеристиками указанного объекта.

- Режим получения информации пространственных запросов (выбор прямоугольником или кругом), то есть когда этот режим активен, вы можете выбрать несколько объектов, выделив их рамкой, после чего отображается окно с характеристиками выделенных объектов.

- Поиск объектов – когда этот режим активен, отображается окно с полем для ввода идентификатора объекта, после ввода на карте отображается найденный выделенный объект.

- Просмотр карты по слоям – пользователь может отключать и включать слои, если слой отключен, то обозначение его объектов не производится. Включение/отключение изображения слоя приводит к перезагрузке изображения карты с сервера. На разных масштабах карты вам доступны разные наборы слоев.

- Измерение расстояния на карте – функция позволяет измерять расстояние между двумя точками местности или суммарный путь нескольких точек с помощью ломанной прямой.

Использование растровых карт подходит для просмотра пространственных и атрибутивных данных, однако уступает по функциональности просмотру векторных карт. Несмотря на это, растровый метод имеет свои преимущества – это возможность использования интернет – выюеров, не привязанных к платформе Microsoft Windows, а также отсутствие необходимости в загрузке ActiveX – компонент.

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЗАДАЧЕ ПРОГНОЗИРОВАНИЯ РЕЖИМНЫХ ПАРАМЕТРОВ И ХАРАКТЕРИСТИК В ЭНЕРГОСИСТЕМАХ

В.Г. Курбацкий, д.т.н., проф. каф. Систем электроснабжения;

Н.В. Томин, аспирант каф. Систем электроснабжения

Братский государственный университет (ГОУ ВПО «БрГУ»),

г. Братск Иркутской обл., frosty1.61@mail.ru

В последнее десятилетие в связи с развитием новых информационных технологий (НИТ) для решения задачи прогнозирования режимных параметров (величины электрической нагрузки, перетоков мощности и т.д.) и характеристик (например, потерь электроэнергии, метеоданных) в энергетике используются искусственных нейронных сетей (ИНС) [1]. ИНС можно определить как систему, состоящую из большого числа простых вычислительных элементов, имеющих нейронную основу и работающих параллельно, способную приобретать, запоминать и использовать приобретенные знания.

Как показано в [1, 2, 3], что достаточно точный прогноз режимных параметров и характеристик в электрических сетях можно получить с использованием ИНС типа многослойный персептрон (MLP*) [1], обученного по методу *обратного распространения ошибки*. Несмотря на хорошие прогнозные способности MLP результаты экспериментальных исследований указывают на ряд ограничений в структуре MLP, которые, в отдельных случаях, существенно затрудняют решение ряда задач, в том числе и задачи прогнозирования.

В настоящее время разработаны новые архитектуры ИНС – радиально-базисные сети (RBF**) и обобщенно-регрессионную сеть (GRNN***) [1], обеспечивающие более эффективное решение задачи, по сравнению с традиционными структурами ИНС.

В дополнении к ним, для эффективного решения задачи прогнозирования, в качестве алгоритмов предварительной обработки входных данных, авторами используются специализированные алгоритмы, а именно:

1) **Нейрогенетический алгоритм отбора входных данных (НГО)** [1] – соединяет в себе возможности генетических алгоритмов (ГА) и вероятностных ИНС для автоматического поиска оптимальных комбинаций входных переменных

* Multilayer Perceptrons – многослойный персептрон

** Radial Basis Functions – радиально-базисная функция

*** Generalized Regression Neural Network – обобщенно-регрессионная нейронная сеть

2) **Нелинейный анализ главных компонент (NPCA****)** [1] – эффективно снижает размерность входных данных.

3) **Кластеризация на базе карт Кохонена** [1] – представительный массив ретроспективных данных разбивается на компактные группы с близкими свойствами – кластеры и прогнозирование осуществляется для каждого отдельного кластера.

Наряду с этим, в работе применяются автоматические процедуры формирования и обучения нейросетевых моделей, такие как:

- **метод имитации отжига (МИО)** – используется выбора оптимальной архитектуры ИНС для каждого конкретного энергорайона или сетевого участка для того, чтобы существенно повысить качество прогнозирования и сократить время на выбор типа ИНС.

- **валидационный метод** – обеспечивает регулирование процесс обучения ИНС, что дает возможность получить в условиях малой предыстории эффективную нейросетевую модель.

Результаты прогнозирования электрической нагрузки в двух энергорайонах г. Иркутска представлены в таблице. Из нее видно, что использование ИНС типа GRNN и RBF, которые были получены как результат работы алгоритмов МИО и НГО, позволили получить достаточно низкие ошибки прогноза.

Прогнозирование электрической различными архитектурами
«прогнозных» ИНС в энергорайонах г. Иркутска

Прогнозируемые сутки и энергорайон		Средние ошибки «прогнозных» ИНС, %		
		GRNN	RBF	MLP
Второй энергорайон	Четверг 22 апреля	1,43	–	4,48
	Пятница 23 апреля	1,58	–	2,71
Шестой энергорайон	Пятница 23 апреля	–	1,07	1,45
	Суббота 24 апреля	–	1,25	2,41

В задаче прогнозирования температуры наружного воздуха $t_{\text{нв}}$ для формирования расходов тепловой энергии использование валидационного метода при создании нейросетевой модели, позволило получить значительно точные прогнозы, по сравнению с методом наименьших квадратов (МНК) (рис. 1).

**** Nonlinear Principal Component Analysis

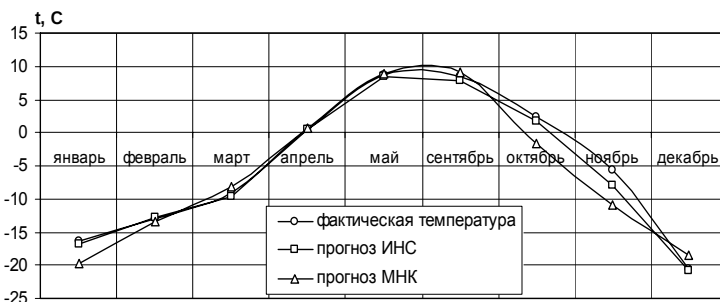


Рис. 1. Результаты прогнозирования $t_{\text{нв}}$ на отопительный период 2004 г.

Использование нейросетевого подхода для повышения точности прогноза сверхнормативных потерь электроэнергии (СПЭ) в распределительных электрических сетях 0,4–10 кВ г. Братска [4] обеспечили достаточно точные прогнозы СПЭ (рис. 2)

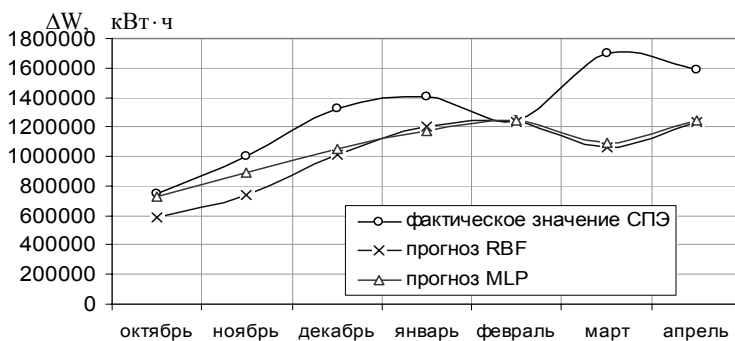


Рис. 2. Результаты прогнозирования СПЭ в распределительных электрических сетях 0,4–10 кВ г. Братска

ЛИТЕРАТУРА

1. Осовский С. Нейронные сети для обработки информации / Пер. с польского И.Д. Рудинского. М.: Финансы и статистика, 2004. 344 с.
2. Курбацкий В.Г., Томин Н.В. Управление в электроэнергетике с использованием методов искусственного интеллекта // Электрика. 2005. №9 С. 20–28.
3. Манов Н.А., Чукреев Ю.Я. и др. Новые информационные технологии в задачах оперативного управления электроэнергетическими системами. Екатеринбург, УрО РАН, 2002. 205 с.
4. Курбацкий В.Г., Томин Н.В., Шуманский В.Б. Применение нейросетевых моделей в задаче формирования тарифов на тепловую и электрическую энергию. Энергетика: управление, качество и эффективность использования энергоресурсов: Сб. трудов четвертой Всероссийской науч.-техн. конф. В 2 т. Благовещенск: АмГУ, 2005. С. 32–38

ЛАБОРАТОРНАЯ ИНФОРМАЦИОННО-МЕНЕДЖМЕНТСКАЯ СИСТЕМА

*А.И. Труфакина, А.С. Русановский, Д.Н. Замятин,
студенты 5 курса каф. АОИ ФСУ
ТУСУР, г. Томск, т. 67-67-24*

Аналитическая лаборатория – это неотъемлемая часть предприятия любой отрасли промышленности: атомной, горнометаллургической, нефтеперерабатывающей, химической, пищевой, фармацевтической, а также и других областей жизнедеятельности человека.

Аналитические лаборатории, как правило, имеют большой штат сотрудников и разнообразную номенклатуру. Через лаборатории проходит очень большой объем материальных, финансовых и информационных потоков.

В аналитических лабораториях до сих пор отсутствует автоматизация обработки информации: хранение и поиск информации, заполнение форм, журналов, отчетов, проведение расчетов, а самое главное анализ результатов функционирования лаборатории производится вручную. Поэтому целью создания ЛИМС является автоматизация работы аналитической лаборатории.

Лабораторные информационно-менеджментские системы – это компьютерные информационные системы, предназначенные для автоматизации работы контрольно-аналитических лабораторий и отделов контроля качества производственных предприятий.

Структура разработанной для ОАО «Томскводоканал» ЛИМС представлена на рис. 1. Сервер системы реализован на базе СУБД InterBase 6.5. Сервер осуществляет хранение информации и некоторые расчеты. Клиентские приложения реализованы на Delphi и представляют собой интерфейс взаимодействия пользователя с сервером для получения и записи информации. Клиент также выполняет некоторые вычисления.

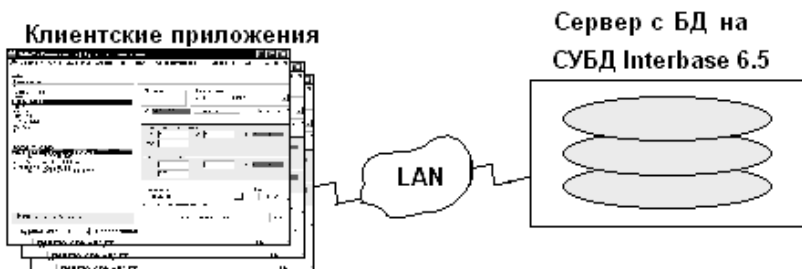


Рис. 1. Структура ЛИМС

Разработанная ЛИМС обеспечивает следующие функции:

- регистрация образцов, поступающих на анализ;
- расчеты анализов по трем методам, необходимым водоканалу;
- ведение сопутствующих справочников;
- регистрация результатов анализов;
- контроль выполнения анализа архивных проб;
- отслеживание руководителем или администратором процесса проведения анализов;
- автоматическое создание сертификатов анализа ;
- создание различных отчетов.

Разрабатываемая ЛИМС внедряется на лаборатории Томского водоканала и адаптируется для работы на нем. В данный момент система проходит тестирование и доработку.

ЛИТЕРАТУРА

1. *Абдрахимов Ю.Р., Воробьев К.В., Замятин Н.В.* Лабораторная автоматизированная информационно-управляющая система, Сборник статей «Информационные технологии в территориальном управлении, промышленности, образовании». Томск: Томский государственный университет систем управления и радиоэлектроники, 2002.
2. *Катеман П., Пийперс Ф.В.* Контроль качества химического анализа/ Под ред. Карпова Ю.А. Челябинск, 1989.
3. *Автоматизация и механизация работ в химико-аналитических лабораториях/* Под ред. Ляликова. Кишинев: Штиница, 1976.
4. <http://www.ciet.kiev.ua/portfolio/lims.html>
5. <http://www.lims.ru>

ИНФОРМАЦИОННО-СПРАВОЧНЫЙ ПОРТАЛ БЫСТРОГО РАЗВОРАЧИВАНИЯ КОММЕРЧЕСКИХ САЙТОВ

*Д.П. Вагнер, магистрант 2 курса ЭФ
ТУСУР, г. Томск, adios@lenta.ru*

Не секрет, что в современном мире Интернет-технологии произвели определенные изменения в характере и особенностях деятельности большинства организаций. В наибольшей степени эти изменения касаются работы служб, занимающихся ведением переписки, сбором и распространением информации, рекламой и продвижением товаров и услуг. На сегодняшний день обмен информацией через Интернет гораздо популярнее других средств связи, а отсутствие у организации собственного e-mail, становится признаком «дурного тона», и равно-

сильно отсутствию телефона. В ближайшее время подобное определение будет применимо и в случае отсутствия у компании собственного сайта (в виде электронной информации или электронного магазина).

Можно с уверенностью сказать, что в деятельности большинства компаний рано или поздно встает проблема создания собственного сайта в сети. Стоит заметить, что основная масса сайтов создается, главным образом, ориентируясь на определенные – первостепенные функции, и лишь только крупные компании могут заказывать себе полноценные многофункциональные сайты с уникальным дизайном, когда стоимость проекта намного превышает сумму 1000\$.

Большинство же компаний среднего и малого бизнеса в основном ориентируются на такие стороны, как возможность предоставления своим клиентам коммерческой информации, а также более удобное взаимодействие с потребителями и поставщиками, особенно из других регионов, посредством обмена информацией через службы обмена сообщениями, электронные каталоги товаров, специальные формы оформления заказа, кроме того, важным фактором открытия собственного сайта является привлечение потенциальных клиентов.

В настоящее время при выборе способа создания собственного представительства в Интернет все большей популярностью пользуются так называемые «Конструкторы сайтов». Использование таких конструкторов практически не требует знаний в области web разработок, здесь встает проблема лишь информационного наполнения и выбора одного из предложенных шаблонов структуры и дизайна. «Конструктор сайтов» представляет собой специализированный портал либо программный продукт, предоставляющий возможности создания и управления собственным интернет-сайтом, и обычно включает следующие функции: создание и управление навигационной структурой сайта, выбор шаблона оформления внешнего вида, подключение стандартных модулей, например, новости, форум, гостевая книга, контакты, опросы, поиск, электронный каталог товаров и т.п., оперативное внесение изменений на сайте при необходимости.

Таким образом, воспользовавшись подобной системой, компания сможет получить достаточной качественный сайт, который позволит оперативно размещать информацию и упростит взаимодействие с постоянными клиентами и поставщиками. Однако для привлечения потенциальных покупателей и продвижения товара на рынок с помощью интернет-технологий только лишь разработка и поддержка собственного сайта не является достаточным основанием. Встает вопрос: «как потенциальные покупатели узнают о сайте вашей фирмы или предлагаемых вами товарах и услугах?» Особую важность этот фактор при-

обретает в связи с тем, что в настоящее время все больше потребителей используют Интернет для поиска информации о товарах и услугах (исследования IMPACT компании Datamonitor показывают, что эта цифра в 2000 г. достигала 80% от числа всех потребителей в Европе).

Для поиска информации о товаре пользователи Интернет чаще всего прибегают к услугам поисковых систем, специализированных каталогов либо интернет-магазинов. В последние годы стали появляться информационно-справочные системы, предназначенные специально для поиска товаров. Такая система представляет собой базу данных товаров различных фирм, которые размещают в ней информацию о собственных товарах и услугах, а также предоставляют минимальную контактную информацию о себе (например, ссылку на собственный сайт или e-mail). Пользователи системы имеют возможность получить подробное описание товара, сравнивать цены или параметры различных товаров разных фирм.

Размещение информации в такой системе позволяет компании привлекать новых покупателей за счет различных рычагов, например, грамотной ценовой политики или широкого ассортимента товаров и услуг по сравнению с конкурентами. Даже при наличии собственного web-сайта информация, предоставленная подобной системе может сыграть значительную роль в продвижении товара на рынок, нежели информация на вашем собственном сайте.

Исходя из вышесказанного, предлагается создание информационно-справочного портала с возможностью быстрого разворачивания коммерческих сайтов. Такой портал предоставляет возможности компаниям после регистрации в системе быстро создавать собственное представительство в Интернет, на основе «Конструктора сайтов», разработанного для зарегистрированных пользователей системы. Компании получают возможность создавать сайт с учетом их текущих потребностей, подключать стандартные модули новостей, электронного каталога, гостевой книги или форума и др. Пользователи портала, получают возможность поиска информации о товарах и услугах, сравнения цен компаний, зарегистрированных в системе и предоставившим информацию о товаре в каталог.

В основе проекта лежит использование единой базы данных в рамках системы. База данных хранит в себе информацию о структуре, разделах, шаблоне каждого сайта, всю контактную и текущую информацию, кроме того, данные о товарах и услугах каждой из компаний – название товара, его описание, стоимость, изображение. Это и позволяет организовать механизмы поиска, сравнения и выбора товаров клиентами на страницах портала в наиболее удобной форме, без необходимости заходить на сайт каждой из компаний.

Работа портала основана на технологии php с использованием базы данных Ogate. Каждый из сайтов, использует необходимый набор готовых подключаемых модулей, которые обеспечивают вывод, добавление и редактирование информации в базе данных для разных разделов, например работу с новостным блоком или модерирование форума.

Подводя итоги, стоит отметить, что в ходе работы был проведен анализ проблем, связанных с созданием собственного коммерческого сайта и продвижением товара на рынок с помощью интернет-технологий, а также предложено решение – создание информационно-справочного портала с возможностью быстрого разворачивания коммерческих сайтов на основе единой базы данных и стандартных модулей, предоставляющего услуги потребителям в поиске, сравнении и выборе товаров.

ЛИТЕРАТУРА

1. *Гречков В.Ю.* Современное состояние и перспективы электронной коммерции // Маркетинг в России и за рубежом. 2003. № 6.
2. *Орлов М.* Интернет как инструмент бизнеса // Практический маркетинг. 2000. № 9.

АИС «ОБЪЕКТЫ ИНЖЕНЕРНЫХ СЕТЕЙ»

В.Ю. Вишняков, ТУСУР, 5 курс

ТУСУР, г. Томск, т. 41-44-70, slavikbox@gis.tusur.ru

Крупное промышленное предприятие, такое как ОАО «НКМК» (Новокузнецкий металлургический комбинат) имеет в своем распоряжении огромное количество различных объектов инженерных сетей, таких как трубы, фермы, эстакады, водопроводы, колодцы, оборудование и т.д. Совокупность однотипных объектов образуют различные сети – телефонные, железнодорожные, газовые. На территории комбината могут появляться и новые объекты.

В силу сложности производства на комбинате присутствует большая концентрация элементов различных инженерных коммуникаций на единице площади, что требует существенных временных затрат на согласования при проведении ремонтных и строительных работ со службами эксплуатации различных сетей. Как правило, ведением учета инженерных коммуникаций каждой из сетей занимается эксплуатационная служба этой сети. Таким образом, теряется возможность вести эффективный учет и мониторинг технического состояния всей совокупности объектов инженерных сетей.

АИС «Объекты инженерных сетей» представляет собой Windows – приложение, устанавливаемое на рабочих местах в различных цехах и подразделениях предприятия. Вся информация об объектах инженерной инфраструктуры накапливается в едином хранилище данных, расположенном на удаленном сервере предприятия. В качестве сервера базы данных используется Oracle 9i.

Использование единого хранилища данных для хранения разнообразной информации позволит работнику эксплуатационной службы в любой момент времени получить необходимую информацию как об объектах «своей» инженерной сети, так и о смежных объектах, принадлежащих другой сети. Безусловно, доступ к параметрам того или иного объекта осуществляется в соответствии с правами доступа, которые назначает администратор для каждого пользователя системы. Таким образом, пользователь получает доступ только к тем объектам, которые он непосредственно обслуживает в процессе своей деятельности и на которые установлены разрешающие права.

АИС «Объекты инженерных сетей» написана в среде Borland Delphi 7 и состоит из следующих подсистем:

Подсистема учета:

- Ввод и редактирование новых объектов учета
- Ввод и редактирование параметров значений объектов
- Ведение истории изменений значений параметров объектов
- Формирование отчетов по текущему техническому состоянию объектов, а также на любой момент времени в прошлом
- Формирование отчета «Список объектов для инвентарной сверки».

Подсистема конструирования:

- Создание любых описаний объектов
- Создание любых свойств (характеристик)
- Назначение описаниям объектов свойств
- Установление произвольных отношений между объектами
- Создание описаний событий и назначение их описаниям объектов.

Подсистема расчетов:

- Возможность расчета и представления планов-графиков плановых предупредительных работ (ППР) оборудования
- Возможность расчета трудозатрат на проведение ППР с детализацией по каждой единице оборудования и в целом.

Подсистема поиска:

- Возможность поиска объектов по сложным критериям
- Возможность поиска событий, происходивших на объектах, по сложным критериям
- Возможность сохранения настроек поиска для дальнейшего быстрого возвращения к ним.

Подсистема управления правами доступа:

- Создание пользователей системы
- Создание ролей и назначение их пользователям
- Определение доступа к участкам, к объектам и их параметрам на уровне ролей

В основе АИС лежит универсальная модель представления, описывающая структуру базы данных. В силу непрерывного развития и изменения инженерных коммуникаций как в пространстве, так и во времени, была спроектирована гибкая, адаптирующаяся структура БД, которая позволяет накапливать сведения об объектах любого типа без необходимости производить реструктуризацию базы данных. Используя эту модель, можно решать оперативные и стратегические задачи управления сетями, а также задачи моделирования и оптимизации режимов инженерных сетей, производственно-технические и экономические задачи, вести учет и мониторинг технического состояния оборудования.

Ключевым понятием в АИС является объект. Под объектом понимается любой объект инженерной инфраструктуры, независимо от его типа, например, колодец, труба, электрический кабель. Каждый объект обладает специфическими свойствами, к примеру, для колодца – это глубина залегания; для трубы – протяженность; для кабеля – волновое сопротивление. На любом объекте могут происходить различные события (аварии, ремонты и т.п.). Подсистема конструирования АИС «объекты инженерных сетей», доступная администратору, позволяет описать любой объект учета. При этом описанию объекта назначаются специфические свойства и возможные типы событий, которые могут происходить на объектах такого типа. После этапа конструирования объектов, пользователь сможет вести их учет, получать и изменять значения свойств, запрашивать и вводить события, которые происходили на объектах. Модульная архитектура и эргономичный интерфейс делают работу с программой удобной и эффективной.

Основными моментами, определяющими эффективность использования АИС «Объекты инженерных сетей» в процессе управления инженерными коммуникациями крупного промышленного предприятия, такого как «НКМК», являются:

- возможность объединения в единую картину разрозненной информации об отдельных коммуникациях;
- сокращение сроков согласования работ по производству работ на инженерных сетях;
- уменьшение аварийности при эксплуатации инженерных сетей;
- увеличение объема ремонтных и профилактических работ без увеличения затрат за счет увеличения информированности руководящего персонала всех звеньев

В настоящий момент АИС «Объекты инженерных сетей» находится в процессе эксплуатации на таких предприятиях, как ОАО «НКМК» и ООО «Томскнефтехим».

ЛИТЕРАТУРА

1. Вишняков В.Ю. //Универсальная модель представления атрибутивных описаний объектов инженерных сетей. Тез. докл. междунар. конф. студентов «Студент и научно-технический прогресс». - Новосибирск, 2005, с.141

УПРАВЛЕНИЕ РАСПРЕДЕЛЕННЫМИ БАЗАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВЕТЕРИНАРНОГО УЧРЕЖДЕНИЯ ГОРОДА И РАЙОНА

А.Н. Ваздаев

*Юргинский технологический институт
Томского политехнического университета (ЮПИ ТПУ), г. Юрга,
т. (384-51) 6-49-42, wazdaev@ngs.ru*

Ветеринарное управление в процессе своей основной деятельности по отслеживанию и профилактике эпидемической ситуации в районе выдает в адрес физических и юридических лиц различные бланки строгой отчетности (свидетельства и разрешения), фиксирующие и подтверждающие определенные их действия в области, касающейся ветеринарии.

Выдаваемые бланки в зависимости от ситуации имеют различную стоимость для лиц, их получающих. Кроме того, по всем выданным бланкам ветеринарное управление обязано отчитываться перед вышестоящими органами их управления и контроля.

Перед автором была поставлена задача по созданию эффективной модели учета, контроля и анализа движения бланков строгой отчетности, с последующим построением на основе этой модели автоматизированной информационной системы.

В соответствии с правилами существующей предметной области была построена модель деятельности ветеринарного управления. Затем модель была претворена в систему алгоритмов.

На основе них была построена информационная система, призванная помочь в регистрации, учете, контроле и анализе документооборота бланков строгой отчетности. В качестве среды программирования была выбрана программа 1С:Предприятие, как наиболее эффективная оболочка для хранения и обработки существующих данных.

Для хранения информации в системе используется два типа объектов: справочники – предназначены для хранения условно-постоянной информации – и документы – для хранения оперативно-учетной информации.

Справочников в системе восемь. В них содержится информация о врачах ветеринарного учреждения, владельцах животных, продавцах и производителях, местах реализации, ветеринарных станциях, регионов, населенных пунктах и пользователях системы. Кроме того, информационная система ведет учет в разрезе каждого владельца количественный и качественный состав поголовья подворья.

Документов в системе двадцать два. В основном они предназначены для хранения основных фактов деятельности ветеринарного учреждения.

Для получения количественного и качественного анализа хранимой в информационной системе информации предназначено большое количество встроенных в систему отчетов – в системе их двадцать пять. Все отчеты обладают максимальной информативностью, включают в себя первичный анализ и имеют возможность вызова исходных документов непосредственно из самих отчетов.

Все отчеты обладают возможностью отбора по ряду критериев (таких как, владелец, врач, продавец, серия, номер, продукция и др.), что существенно уменьшает время создания отчета и делает информацию в нем более узконаправленной.

В случае организационной структуры ветеринарного учреждения, когда организация представляет собой территориально распределенную структуру, сохраняется потребность в ведении единой системы учета. То есть необходимо иметь возможность работать в едином пространстве документов, получать отчеты, отражающие состояние дел как в территориально удаленных подразделениях организации, так и в организации в целом. При этом не всегда имеется возможность организовать работу всех подразделений с единой информационной базой в режиме он-лайн.

Для решения подобных задач предназначена компонента «Управление распределенными ИБ». С помощью указанной компоненты можно организовать двухуровневую структуру информационных баз (ИБ) системы 1С:Предприятие, состоящую из одной центральной и нескольких периферийных информационных баз, работающих с единой конфигурацией. При этом система будет стремиться поддерживать одинаковое состояние объектов данных во всех узлах распределенной ИБ.

Содержимое информационных баз синхронизируется путем переноса измененных объектов данных между каждой из периферийных и центральной ИБ. Для переноса данных используются файлы пе-

реноса данных. Перенос изменений выполняется только между центральной и периферийными ИБ. Перенос данных непосредственно между периферийными ИБ невозможен. Поэтому изменения данных, произведенные в одном из периферийных узлов распределенной ИБ попадают в другие периферийные узлы только через центральную ИБ.

Кроме того, возникла необходимость в том, чтобы объекты того или иного типа никогда не попадали в те или иные узлы распределенной ИБ. Для обеспечения такой возможности предназначен механизм настройки параметров миграции объектов. С его помощью можно ограничить распространение изменений объектов того или иного вида.

Однако, для того, чтобы документы, элементы справочников и другие объекты, созданные в разных узлах распределенной ИБ, имели заведомо непересекающиеся пространства номеров, кодов и т. п., потребовалось внести в конфигурацию некоторые изменения, которые препятствуют разрушению ссылочной целостности системы.

Для переноса измененных объектов в распределенной ИБ и для первичного создания периферийной ИБ используется файл переноса данных. Он представляет собой упакованный файл, содержащий объекты информационной базы (все при создании периферийной ИБ или измененные при передаче изменений) в специальном формате. Формат данного файла не предназначен для использования его способами отличными от тех, которые предусмотрены механизмами выгрузки/загрузки и передачи изменений. Файл переноса фактически отражает содержимое объектов информационной базы в формате, не зависящем от формата базы данных. Это позволяет использовать в распределенной информационной системе в различных узлах различные форматы хранения данных, поддерживаемые системой 1С:Предприятие.

Особую актуальность данная информационная система приобрела в последнее время, когда резко ухудшилось общемировое эпидемиологическое состояние домашнего скота. Использование данной системы позволяет проводить постоянный мониторинг и оперативно принимать решению по предотвращению массовых эпидемий.

В настоящее время система активно функционирует в Ветеринарном управлении г. Юрга и Юргинского района, имеются реальные результаты, выраженные в экономии материальных средств и получении дополнительных доходов. Приблизительные расчеты показывают увеличение поступлений денежных средств от владельцев и продавцов животной продукции в Ветеринарное управление г. Юрга и Юргинского района не менее чем на 25–30% по сравнению с 2004 г. (когда система еще не функционировала), Это при том, что стоимость получения бланков в 2005 г. не изменилась, а общее поголовье домашних животных в районе уменьшилось.

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ УЧЕТА ПРОИЗВОДСТВЕННЫХ ЗДАНИЙ И СООРУЖЕНИЙ В СРЕДЕ ЭГП ООО «ТОМСКНЕФТЕХИМ»

***Е.И. Юркин, И.С. Лакеев, ТУСУР, 4 курс
ТУСУР, г. Томск, т. 41-44-70, uei@ms.tusur.ru***

Автоматизированная информационная система «Техпаспорт» входит в состав геоинформационной технологии создания и ведения электронного генерального плана (ЭГП) ООО «Томскнефтехим» при работе с техническими паспортами производственных зданий и сооружений.

Технический паспорт – специализированный документ, который составляется на каждое капитальное здание и сооружение и является основным документом, содержащим конструктивную и технико-экономическую характеристику объекта и все основные сведения, необходимые в процессе его эксплуатации. Основная проблема, с которой сталкивается крупное промышленное предприятие при ведении технических паспортов – это огромный объем данных, который хранится в большом количестве бумаг и папок. Данный способ хранения информации затрудняет работу с документами: в тот момент, когда на полках хранится более тысячи папок с паспортами, поиск необходимого занимает много времени и усилий у работников; раньше для редактирования в нем информации возникала необходимость прибегать к вспомогательным канцелярским средствам – это уже в прошлом. А дублирование и заполнение нового тех. паспорта занимает еще больше времени. Все это приводит к избыточной загрузке сотрудников предприятия.

На сегодняшний день существует множество специализированных программ, назначение которых – автоматизация основных процессов деятельности организаций. Но, к сожалению, очень трудно реализовать программный продукт, который подходил бы под многие предметные области и учитывал бы малейшие изменения в стандартах оформления документов.

В направлении автоматизации ведения технических паспортов была спроектирована и реализована структура хранения данных о производственных зданиях и сооружениях под СУБД Oracle 9.x. На основании спроектированной базы данных был разработан АРМ «Техпаспорт» в среде визуального программирования Borland Delphi 7.0. Выбор именно этой среды обусловлен эффективностью средств разработки приложений баз данных, то есть программ, обслуживающих электронные хранилища информации. Эффективность определяется двумя обстоятельствами: высокопроизводительной машиной доступа к данным разного формата и наличием многочисленных компонентов, ориентированных на эту сферу применения.

На этапе проектирования существовало два подхода к разработке модели представления технических паспортов на производственные здания и сооружения:

1. Построение универсальной модели, в которой технические характеристики добавляются динамически, в процессе заполнения БД. Построение такой модели сводится к проектированию модели описывающей параметры характеристик. К преимуществам данного подхода можно отнести универсальность получившейся модели. К недостаткам – большие требования к ресурсам для хранения больших объемов данных.

2. Построение модели, в которой набор характеристик будет статичен, каждая характеристика будет описана отдельной сущностью или полем сущности. Преимущества – низкие требования к ресурсам системы, высокая скорость выполнения запросов. Недостатки – отсутствие возможности изменения набора характеристик.

Ссылаясь на Положение о технической эксплуатации промышленных зданий и сооружений (пункт 12.6. Паспорт заполняется по единой форме в соответствии с Положением о проведении ППР производственных зданий и сооружений), был выбран второй подход, так как набор характеристик в техническом паспорте определен и постоянен. Также от системы требуется высокая скорость обработки запросов.

Требования к визуальному интерфейсу исходили относительно структуры технического паспорта. Поэтому программа обеспечивает быструю адаптацию пользователя к ней. Также система обладает удобным, наглядным, простым и гибким интерфейсом.

Основными функциями, реализованными в приложении «Техпаспорт», являются:

- Создание и редактирование паспорта на производственные здания и сооружения. При создании нового паспорта пользователь видит на экране монитора чистую форму тех. паспорта, с которой он привык работать на бумаге. Тем самым не возникает никаких проблем при использовании электронного варианта.

- Создание записи в любых типах справочников (фундаменты, лестницы, полы и т.д.) и присваивание их созданным паспортам. При заполнении однотипных документов зачастую возникает проблема повторения. То есть одни и те же поля, в основном текстовые, заполняются одинаковыми значениями. Для решения данного вопроса были предусмотрены справочники, в которых хранятся введенные ранее значения характеристик. Теперь пользователь может просто выбирать из списка необходимые значения.

- Занесение и хранение места эксплуатации, производства и объектов недвижимого имущества с их адресами и номерами свидетельств о госрегистрации права на объекты. Данная функция несет юридическую смысловую нагрузку.

– Ведение расширенного поиска и фильтрация созданных ранее паспортов. Крупные промышленные предприятия имеют до 1000 (и более) производственных зданий и сооружений! Имея в базе данных такое количество записей, встает вопрос о быстром поиске необходимого тех. паспорта. Для этого существует фильтрация по трем критериям: по объектам недвижимого имущества, по производству и месту эксплуатации, а также организован поиск по любому из доступных полей.

– Сохранение и откат изменений. В процессе работы с программой доступна функция сохранения документа, что увеличивает вероятность корректного заполнения технического паспорта. Функция отката изменения до последнего сохранения обеспечивает защиту информации от непредусмотренного изменения данных.

– Вывод технического паспорта на печать. Данная функция предусматривает предварительный просмотр документа с его дальнейшим печатанием на принтере.

Разработанная система имеет все необходимые средства для выполнения операций над техническими паспортами промышленных зданий и сооружений.

При этом, вышеизложенный функциональный набор позволяет значительно сэкономить время и средства при работе с данным видом документации и дает возможность полностью сосредоточиться на поставленной задаче, при максимальных надежности и качестве результата. Все вышеперечисленные факты делают идею разработки данной системы востребованной.

РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ ОФИСНЫХ ПРИЛОЖЕНИЙ MS WORD И MS EXCEL ДЛЯ РЕШЕНИЯ СТАТИСТИЧЕСКИХ ЗАДАЧ

Ю.Т. Юсупова, магистрант 6 курса гр. 840-м ЭФ;

И.Г. Боровской, д.ф.-м.н., проф. каф. ЭМИС ЭФ

ТУСУР, г. Томск, julus@yandex.ru

На сегодняшний день практически каждый пользователь компьютера использует в своей работе пакет офисных программ Microsoft Office. Широкой популярностью пользуются такие офисные приложения как текстовый редактор Word и электронные таблицы Excel. Используя перечисленные приложения, можно решать задачи, связанные с хранением различного рода текстовых данных, их структурированием и последующей обработкой для получения из данных необходимой информации.

Хотя приложения используются в самых различных сферах человеческой деятельности для решения абсолютно разного рода задач, однако обработка вводимых данных часто однотипна и сводится к последовательности определенных действий, имеющих в наличии у офисных приложений. Например, для обработки числовых значений, используя стандартные средства, довольно просто подсчитать сумму либо среднее арифметическое чисел.

Однако часто возникает проблема нехватки существующих возможностей приложений. Например, для дополнительной статистической обработки каких-либо числовых данных, когда нет необходимости решать сложные статистические задачи, а необходимо только произвести простые, часто встречающиеся на практике решения задач над выборками. Для решения подобного рода статистических задач, нет необходимости покупать и устанавливать сложные пакеты статистических программ. В таких случаях встает вопрос о расширении существующих возможностей офисных приложений.

В данной статье рассматривается возможность дополнения приложений MS Word и MS Excel средствами для решения задач о статистической значимости. Задачи подобного рода встречаются довольно часто в медико-биологических и социальных исследованиях. Когда имеются две выборки и необходимо определить уровень статистического расхождения между ними с использованием какого-либо критерия, например критерия Стьюдента и Вилкоксона-Манна-Уитни.

Целью работы являлось разработать удобный для пользователя инструмент, который встраивается в офисное приложение, для решения изложенной задачи.

Инструментарий реализован в виде панели инструментов, содержащей кнопки, позволяющие пользователю выбирать критерий, по которому необходимо провести исследование на значимость. Пользователь выделяет блок данных, который необходимо обработать и нажимает на кнопку в этой панели. Результат обработки вставляется в строку, следующую за выделением.

Обработка событий о нажатии клавиш производится с помощью встроенного в офисные приложения языка VBA. Язык Visual Basic является оптимальным для работы с офисными компонентами, однако, для проведения сложных расчетов и необходимости быстрой обработки больших объемов информации требуется использование более мощного языка, в качестве которого в данной работе выбран язык С.

Таким образом, схема работы состоит в следующем. Средствами VB снимается информация из выделенного пользователем блока и передается на обработку в функции, написанные на языке С, которые

помещаются в специальную dll. Такая схема работы позволяет сочетать гибкость и мощь языка С с возможностями офисных приложений.

Итак, необходимо подключить dll к макромодулю офисного приложения. При этом накладываются значительные ограничения на вызовы функций из dll и возникает задача согласования интерфейсов двух различных языков. Поэтому целые и вещественные числа передаются в функции по ссылке. Также для данной работы необходимо передавать значения выборок. Передача массивов из функций VB в функции С невозможна, поэтому принято решение передавать массивы в виде текстовых строк, а в функциях С производить разбор строк и преобразовывать их в массивы чисел. Причем, такой подход позволяет фильтровать ошибки пользовательского ввода, например, когда пользователь в качестве десятичного знака вводит вместо точки запятую.

Для вызова dll из VBA модуля необходимо либо явно указать путь к файлу, либо расположить dll в системном каталоге. Так как инструментарий должен быть переносим, то от явного указания путей необходимо отказаться. Чтобы облегчить пользователю задачу установки инструментария, создан установочный файл.

Итак, в процессе создания инструментария можно выделить несколько этапов.

На первом этапе создается библиотека, написанная на языке С, которая содержит все функции необходимые для решения поставленной задачи. При этом следует учитывать то, что интерфейс вызова функций должен быть согласован с требованиями, накладываемыми языком Visual Basic.

На втором этапе создаются шаблоны Word и Excel, содержащие панель инструментов и методы, обрабатывающие нажатия кнопок. При выполнении этих методов вызываются функции из dll.

На последнем этапе создается установочный файл, который автоматически разместит написанные dll библиотеки и шаблоны в нужных каталогах.

В результате выполненной работы решена задача объединения возможностей языков С и Visual Basic для написания удобного инструментария, который позволяет не подготовленному пользователю, знающему лишь основы работы с офисными приложениями, решать задачи по определению статистической значимости выборок.

СЕКЦИЯ 10

АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА В СИСТЕМАХ УПРАВЛЕНИЯ И ПРОЕКТИРОВАНИЯ

*Председатель – Шурыгин Ю.А., первый проректор ТУСУР,
зав. каф. КСУП, д.т.н., профессор;
зам. председателя – Коцубинский В.П., зам. зав. каф. КСУП,
к.т.н., доцент*

ПРОГРАММНЫЙ МОДУЛЬ «МЕНЕДЖЕР СМК» ДЛЯ ОРГАНИЗАЦИИ УПРАВЛЕНИЯ ДОКУМЕНТАЦИЕЙ В СЛУЖБЕ КАЧЕСТВА ИОА СО РАН

*Р.Р. Абушаев, студент 5 курса ФВС;
О.Е. Аркатова, зам. руководителя СлК ИОА СО РАН
ТУСУР, кафедра КСУП, г. Томск*

Проблемы качества товаров и услуг, предлагаемых на российском рынке, как и во всем мире, стоят на первом месте. Российская специфика заключается в хроническом снижении объемов производства, взаимных неплатежах, что объясняется низкой или вообще отсутствием конкурентоспособности промышленности по качеству производимых товаров и услуг [1].

Сертификация предприятия на соответствие стандартам качества серии ISO 9000 стала первой большой задачей в области постановки современного менеджмента, понятной и востребованной широкими массами российских руководителей. Система управления качеством по международным стандартам является неотъемлемой частью системы управления предприятиями [2].

Поэтому решение этой задачи может дать мощный толчок к совершенствованию системы управления предприятия в целом, приближения ее к общепринятой мировой практике.

Современная система менеджмента качества (СМК) базируется на информационной системе, поддерживающей автоматизированное документирование процессов обеспечения качества на всех стадиях жизненного цикла продукции (изделия) и автоматизированное управление этими процессами с обеспечением соответствующей документации. Тогда СМК становится неотъемлемой частью интегрированной автоматизированной системы управления предприятием [3].

Первая проблема, с которой сталкивается предприятие при попытке внедрить СМК – это количество порождаемых процессом внедрения СМК документов, которые достоверно отражают состояние дел в любой момент времени (в актуальном состоянии). То есть, при любом существенном изменении в деятельности компании эти документы должны отражать текущее, а не прошедшее положение дел. Взаимосвязанная актуализация большого количества бумажных документов является практически невыполнимой задачей.

Поэтому необходимо автоматизировать процессы в системе управления качеством на предприятиях. Автоматизация работы по внедрению СМК позволяет:

- осуществлять надзор и контролируемость, соблюдение требований и применение процессов СМК в жизненных циклах продукции;
- оформлять в установленном порядке протоколы и акты по результатам проверки работы СМК;
- осуществлять экспертизу нормативной документации в части контролируемых показателей, методов и средств испытаний [4].

Для решения этой задачи разработана программа «Менеджер СМК», которая предназначена для автоматизации документооборота СМК в ИОА СО РАН.

При разработке системы менеджмента качества (СМК) в соответствии с принципами, заложенными в стандарты ИСО 9000, целесообразно выделять 2 основных аспекта:

- организационное и нормативно-методическое обеспечение системы качества;
- система сбора, регистрации, хранения и обработки данных о качестве.

Созданная программа реализует эти аспекты, что позволяет поддерживать документацию СМК в рабочем состоянии

Программный продукт отвечает следующим требованиям:

- простота интерфейса;
- возможность одновременного доступа к базе данных нескольких пользователей;
- наличие системы защиты от несанкционированного доступа;
- наличие системы помощи по программе;
- фильтрация и генерация отчетов по документам.

Все данные представляются в виде документов Word, что значительно облегчает работу пользователю, не имеющему навыков работы с другими программами. В базе находятся ссылки на документы, ГОСТы.

Для обеспечения защиты от несанкционированного доступа к информации, предусмотрен пароль при входе в программу и пароль на

открытие базы данных, при сбое в сети питания ПК либо аварийном завершении работы программы предусмотрено автосохранение данных.

Программный продукт разработан в среде Delphi 6.0 с использованием СУБД PARADOX. Данная программа позволила уменьшить время и затраты, связанные с внедрением документации СМК в Институте оптики атмосферы. В дальнейшем планируется создание приложения для реализации управления процессами.

В настоящее время программный модуль «Менеджер СМК» прошел тестирование и успешно применяется в ИОА СО РАН, а также получен акт внедрения в научно – исследовательском институте прикладной математики и механики (НИИ ПММ)

ЛИТЕРАТУРА

1. *В.А. Копнов.* Зачем нужна система качества Российским предприятиям // Менеджмент качества и ИСО 9000. 2000. Т. 2. №1. с. 1–14.
2. *М.В. Маликова.* Управление документами системы менеджмента качества // Менеджмент качества и ИСО 9000. 2002. Т. 2. № 1. с. 45–64.
3. *Пособие* для слушателей семинара // Основы организации системы менеджмента качества оборонного предприятия . Вып. № 4. М.: ИиИС ВВТ. 2002.
4. *В.В. Липаев.* Сертификация систем качества предприятий, разрабатывающие программные средства для информационных систем, на соответствие стандартов серии ИСО 9000 // Проблемы качества в сфере образования. 1999. № 4.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ОПЕРАТОРА АСУ ТП ГАЗОПРОВОДА «МЫЛЬДЖИНО-ВЕРТИКОС»

И.Ю. Андреев, аспирант

ГНУ НИИАЭМ, г. Томск, т. 563-751, aiy@niiaem.tomica.ru

В этой статье рассказывается о разработке верхнего уровня АСУ ТП газопровода (ГПр) «Мыльджино-Вертикос», а в частности автоматизированного рабочего места (АРМ) оператора.

Автоматизация технологических процессов является неотъемлемой частью корпоративной информационной системы нефтегазового предприятия. Основными объектами автоматизации являются нефтяные и нагнетательные скважины, групповые замерные установки и узлы коммерческого учета нефти и газа, установки подготовки нефти, промысловые и магистральные нефтепроводы, нефтепродуктопроводы и водоводы, нефтеперерабатывающие установки, системы распределения нефтепродуктов. [1]

Стремительное развитие технологий передачи и обработки информации предъявляет к современным АСУ ТП транспортировки газа новые требования:

- Управление технологическими объектами (процессами) в реальном масштабе времени, в том числе в нештатных ситуациях;
- Возможность интегрирования в многоуровневые информационные системы;
- Оперативное выявление аварийных и предаварийных ситуаций;
- Расширение объема и повышение достоверности технологической информации. [2]

Все эти требования были учтены при разработке системы АСУ ТП газопровода «Мыльджино-Вертикос».

Объект автоматизации представил из себя 8 крановых площадок (КП) и автоматизированную газораспределительную станцию (АГРС). Распределение КП составляет около 100 км.

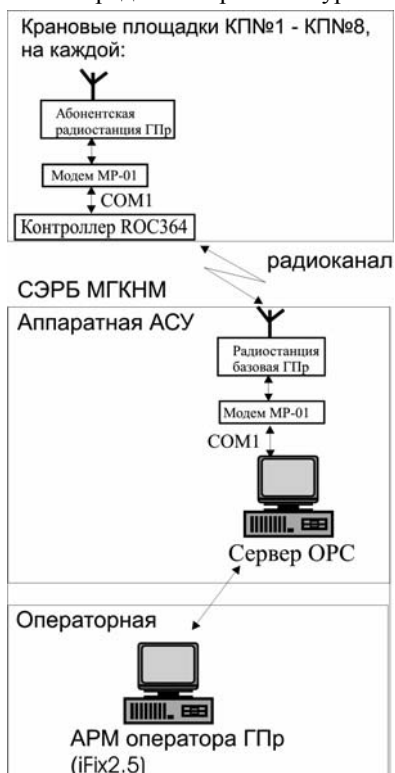
Структура комплекта технических средств верхнего уровня АСУТП ГПр приведена на рис. 1.

Средства реализации – автоматизированные рабочие места на базе ПК типа PC IBM, пакет прикладных программ на базе SCADA iFix2.5, Spartan RocOPC сервер [3].

Функции верхнего уровня реализованные в АРМ:

- Представление всей информации оператору ГПр в удобной, интуитивно-понятной форме;
- Структурированность мнемосхемного представления;
- Сбор и ведение архивов по всем измерительным сигналам;
- Задание режимов и установок алгоритмам управления и блокировок нижнего уровня;
- Отслеживание и индикация информации о критических и предупредительных ситуациях;

Рис. 1. Структура комплекта технических средств верхнего уровня АСУТП ГПр



- Диспетчеризация, выдача информации серверу производственно – диспетчерской службы МКГМ;
- Журнал – режим ведения (просмотра, анализа и редактирования) журнала событий;
- Режим просмотра архива параметров в форме трендового представления.
- Разграничение доступа и функциональности системы в зависимости от прав пользователя.

На рис. 2 представлена мнемосхема КП 5.

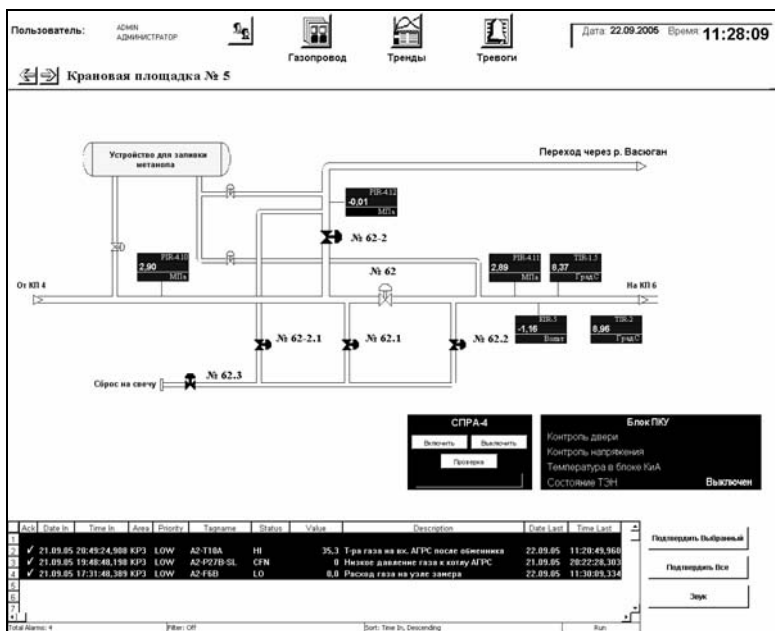


Рис. 2. Эскиз мнемосхемы крановой площадки №5

В результате проделанной работы по созданию АРМ оператора, и автоматизации всего газопровода, была создана АСУ ТП Газопровода «Мыльджино-Вертикос». В настоящее время работает в опытной эксплуатации. Ведется работа по сдаче системы в промышленное использование.

ЛИТЕРАТУРА

1. Журналы «Современные компьютерные технологии». 2002. №2
2. Журналы «Современные технологии автоматизации». 2001. №1
3. АСУ ТП ГПР, Руководство эксплуатации.

ВЕКТОРИЗАЦИЯ ДВУЦВЕТНЫХ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ТРИАНГУЛЯЦИИ

А.А. Чертов, студент гр. 1411 ф-та Информатики

ТГУ, г. Томск, т. 492-260, caa@academ.tsc.ru

Векторизация – это процесс получения отрезков (векторов) по растровому изображению. В простейшем случае на выходе алгоритма векторизации будет набор точек, линий и полигонов, необходимым образом аппроксимирующих исходный растр. Геометрическим объектам могут быть сопоставлены атрибуты, например, для линии – ширина, для точечного объекта – тип условного значка.

Существует несколько подходов к векторизации изображений: методы, основанные на преобразовании Хафа (Hough Transform), методы итеративного утончения, методы, основанные на дистантном преобразовании, различные варианты метода ортогональных направлений и другие. Методы различаются трудоемкостью, устойчивостью к помехам, поведением на развилках и т.п. Не существует универсального алгоритма, который одинаково хорошо бы работал на произвольном изображении.

Предложенный алгоритм состоит из следующих шагов

1) Выделение контуров одноцветных областей. Для контура запоминается цвет области справа и слева. Чтобы избавиться от «ступенчатости» и уменьшить количества точек, контур аппроксимируется другой, более гладкой ломаной (процедура генерализации).

2) Построение триангуляции с ограничениями. На множестве точек, полученных после генерализации контуров, строится триангуляция с ограничениями. В качестве ограничений берутся ребра контуров. В результате каждый треугольник принадлежит строго одной области.

3) Нахождение точечных объектов. В соответствии с некоторыми пороговыми значениями ширины, высоты и/или площади некоторые объекты классифицируются, как точечные. На последующих шагах алгоритма их можно не рассматривать.

4) В оставшейся области строится скелет изображения (рис. 1). Если два смежных по ребру треугольника имеют одинаковый цвет, то ребро, разделяющее их, будем называть невидимым. При построении скелета используются следующие правила:

- Если у треугольника одно невидимое ребро, то в скелет добавляется отрезок, соединяющий середину этого ребра с противолежащей вершиной.

- Если у треугольника два невидимых ребра, то в скелет добавляется отрезок, соединяющий их середины.

- Если невидимых ребер три, то в скелет добавляются отрезки, соединяющие их середины с точкой пересечения медиан.

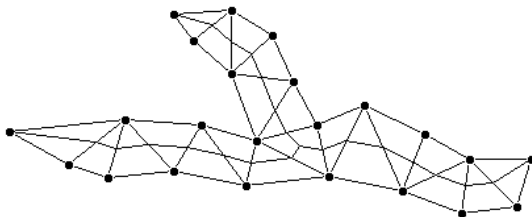


Рис. 1. Скелетная линия

5) Для каждого отрезка скелета оценивается толщина соответствующей линии, как отношение площади треугольника к длине скелетной линии

6) В соответствии со значениями толщины треугольники классифицируются на площадные и линейные. Площадной объект представляется как внешняя граница множества смежных площадных треугольников. Линейный объект представляется как скелетная линия, рисуемая с необходимой толщиной.

Может оказаться так, что все три вершины треугольника будут лежать на одной стороне линии (рис. 2). Это приводит к тому, что образуется нежелательное ответвление на скелетной линии.



Рис. 2. Нежелательное ответвление

Для устранения таких дефектов достаточно удалить все ответвления, которые короче некоторого порога.

Также для скелетной линии характерны небольшие колебания. Для их устранения следует применить дополнительный шаг генерализации.

Описанный алгоритм проводит векторизацию в автоматическом режиме, без вмешательства оператора. Управлять классификацией объектов можно посредством двух параметров – предельного размера точечного объекта и максимальной ширины линии.

ЛИТЕРАТУРА

1. Костюк Ю.Л., Новиков Ю.Л. Графовые модели цветных растровых изображений высокого разрешения // Вестник ТГУ. 2002. № 275, апрель. С.153–160.

2. *Lyu Wenyin, DovDori. From Raster to Vectors: Extracting Visual Information from Line Drawings*[Электронный ресурс]. Режим доступа: <http://research.microsoft.com/research/pubs/view.aspx?pubid=924>, свободный.

ИНТЕГРАЦИЯ БИЗНЕС-ПРИЛОЖЕНИЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ МАРКЕТИНГОМ

В.А. Драганов, аспирант, м.н.с.

ГНУ «НИИ АЭМ при ТУСУР Минобразования России»

e-mail: dva@snc.com.ru

Как известно, практически любая автоматизированная система управления маркетингом (АСУМ) является законченным комплексом программно – аппаратных средств со своей архитектурой и функциональностью, которые в свою очередь зависят от предметной области. Но не зависимо от предметной области у многих АСУМ появляется потребность тесной интеграции с уже существующими бизнес – приложениями. На этом этапе в большинстве случаев сам процесс интеграции вызывает некоторые трудности, так как в одних случаях в архитектуре не была заложена сама возможность внешней интеграции, а в других – не были предусмотрены гибкие механизмы стыковки с новыми приложениями не ориентированными на совместную работу.

Разработанные и внедренные на данный момент системы в своем большинстве только частично снимают проблему интеграции имея примитивные или узкоспециализированные интерфейсы, такие как экспорт/импорт данных, технология СОМ(СОМ+), различные API. Многие мощные АСУМ имеют встроенные модули, реализующие некоторые функции готовых бизнес – приложений. Такой подход, несомненно, выделяет такие системы среди аналогов, но не избавляет их от недостаточной гибкости. Именно невозможность «бесшовной» стыковки и полной автоматизации бизнес-процесса накладывают ограничения на широкое применение некоторых вполне конкурентоспособных систем. Таким образом, все преимущества АСУМ могут быть не востребованы в связи с отсутствием развитого механизма интеграции. Очень важным аспектом выбора АСУМ является минимизация трудозатрат на весь процесс интеграции, внедрения и эксплуатации. Сюда можно отнести и легкость модернизации подсистемы стыковки, а также время на освоение форматов.

Клиенты, вводящие в эксплуатацию новую АСУМ, в большинстве случаев хотят иметь тесную интеграцию с уже внедренными бизнес – приложениями. Поэтому, по мере роста функциональности системы

параллельно растут требования и к подсистемам, одной из которых является модуль интеграции. По причине этого потребовалось решить задачи по реализации типового решения, которое в свою очередь удовлетворяло бы требованиям различного рода автоматизированных систем управления. На основе анализа существующих АСУМ и бизнес – приложений, которые прочно закрепились на рынке, была разработана модель универсального модуля интеграции, который бы обеспечил бесшовную стыковку с большинством имеющихся и вновь появляющимися бизнес – приложениями. В процессе проработки модели была спроектирована архитектура модуля и выявлены основные критерии оценки. За основу в архитектуре были взяты:

- технологии прямого доступа к данным;
- методы межпросессового взаимодействия;
- технология плагинов;
- технология COM(COM+);
- универсальный API;
- интерпретатор макрокоманд

Выбор данных технологий был продиктован широким распространением одних и универсальностью других. Хорошо дополняя друг друга, они образуют мощное ядро, позволяющее без особых трудностей интегрировать практически любое бизнес-приложение в АСУМ. Само ядро подсистемы поддерживает различные источники данных (Oracle, MySQL, ODBC, файлы и т.д.) и имеет встроенный интерпретатор макрокоманд, с помощью которых можно описать алгоритм интеграции или движение потоков данных. В самом простом случае процесс интеграции сводится к выбору конкретного бизнес-приложения и определению требуемой функциональности с помощью визуального интерфейса. Добавление нового приложения также не составляет труда, нужно просто выбрать механизм стыковки. Даже если бизнес – приложение не поддерживает не один из известных механизмов, то в модуле есть возможность применения плагинов, с помощью которых возможно низкоуровневая стыковка. Все эти свойства модуля интеграции обеспечивают его гибкую настройку, широту применения и наделяют АСУМ, в составе которой он функционирует, неоспоримыми преимуществами по сравнению с аналогичными системами, тем самым, снижая уровень трудозатрат до минимума.

Разработанная архитектура модуля интеграции реализована в виде типового решения для АСУМ операционного центра процессинговой компании разработки НИИ АЭМ (г. Томск), который внедрен в ряде региональных операционных центров Западной Сибири. Модуль интеграции протестирован с такими бизнес – приложениями, как MS Office,

1С Предприятие и другими бизнес-приложениями узкого и широкого назначения.

ЛИТЕРАТУРА

1. Месарович М., Мако Д., Такахага И. Теория иерархических многоуровневых систем. М.: Мир, 1973. 344 с
2. Перегудов Ф.И., Тарасенко Ф.П. Основы системного анализа. Томск: Изд-во НТЛ, 1997. 396 с
3. Маклаков С.В. Создание информационных систем с AllFusion Modeling Suite. М: ДИАЛОГ-МИФИ, 2003. 432 с.
4. Гома Х. UML. Проектирование систем реального времени, параллельных и распределенных приложений. М.: ДМК пресс, 2002. 704 с.
5. Энциклопедия SQL. 3-е изд. / Дж. Грофф, П. Вайнберг. СПб.: Питер, 2004. – 896 с.

МНОГОСЛОЙНАЯ АРХИТЕКТУРА В ТЕХНОЛОГИЧЕСКИХ ПРОГРАММНЫХ СИСТЕМАХ

А.В. Фофонов, аспирант

ГНУ «НИИАЭМ при ТУСУР Минобразования России»

г. Томск, fav1481@mail.ru

Создавая программные системы или решая различные задачи, разработчик часто сталкивается с проблемой их «сложности». Типичным подходом помогающим бороться с такой ситуацией является декомпозиция «сложной» задачи на ряд более мелких задач, которые проще решить. Соответственно программная система разбивается на ряд подсистем, каждая из которых обеспечивает выполнение определенной функциональности. Концепция «Расслоения системы» (multi-layer architecture) помогает организовать работу подсистем наиболее эффективным образом. Ее суть заключается в том, что самые важные подсистемы представляются в виде слоев (layers) расположенных друг над другом. Каждый вышестоящий слой использует функции, предоставляемые нижестоящим слоем, однако нижние слои «не осведомлены» о существовании верхних. Такая организация дает ряд важных преимуществ [1],[2]:

- каждый слой представляет собой целостную подсистему, которой легко управлять
- можно разработать много различных вариантов одного слоя
- минимизируются зависимости между слоями
- слои могут быть стандартизованы

- слои могут быть повторно использованы в различных системах.
- Среди недостатков можно отметить [1]:
- возможность каскадных изменений слоев: изменение одного слоя приводит к модификации других
 - падение производительности, за счет необходимости преобразовывать данные при передаче их от одного слоя к другому.

На практике часто встречаются системы, состоящие из трех базовых слоев: «Представление», «Логика предметной области» и «Источник данных». В слое «Представление» собрана функциональность, отвечающая за визуализацию результатов работы объектов «Логике предметной области», а слой «Источник данных» обеспечивает долговременное хранение данных. Такое разбиение на слои позволяет получить системы, поддерживающие несколько различных представлений или умеющие работать с различными источниками данных.

В технологических системах помимо обычных требований визуализации и хранения данных часто присутствуют два дополнительных: распределенность и необходимость взаимодействия с различными устройствами. Эти требования предполагают введение дополнительных слоев: «Коммуникации» и «Устройства». Первый слой должен отвечать за взаимодействие между элементами распределенной системы, а второй – содержать всю необходимую логику для работы с аппаратурой. Выделение таких слоев целесообразно, поскольку позволяет максимально увеличить время жизни системы, за счет возможности управлять ее ключевыми элементами, в случае изменения ряда требований.

Требование распределенности технологической системы означает, что система физически размещается на нескольких узлах вычислительной сети. Следовательно, все слои системы будут распределены по этим узлам в соответствии с ролью назначенной каждому узлу. Обычно выделяют роли «клиент» и «сервер». «Клиент» содержит слой «Представление» и организует взаимодействие системы с пользователем. «Сервер» занимается обслуживанием «клиентов», выполняя их команды и отвечая на запросы. Если для каждого слоя выделить свой узел, то мы получим дальнейшее дробление ролей узлов: «сервер логики предметной области», «сервер устройств», «сервер данных». При этом «сервер предметной логики» будет являться клиентом «сервера данных». Такая архитектура называется многозвенной (multi-tier architecture).

Пример многослойной двухзвенной архитектуры технологической системы, где логика представления вынесена отдельно (архитектура клиент-сервер) представлен на рис. 1.

Организация взаимодействия между слоями системы предполагает передачу данных от одного слоя к другому. Если инициатором обмена

выступает вышестоящий слой, то используется обычный механизм «команд»: объект вышестоящего слоя требует от объекта нижестоящего слоя выполнения каких-либо действий, отправляя ему сообщение-команду. В технологических системах, из-за присутствия различных устройств, часто возникает необходимость организовать обратное взаимодействие, когда инициатором обмена выступает нижестоящий слой. Например, в системе может присутствовать некоторый датчик, который производит периодические замеры в окружающей среде и слой «Устройства» должен сообщить полученные данные слою «Логика предметной области». Для того чтобы организовать такое взаимодействие и при этом не нарушить принципы расслоения используется механизм «издатель/подписчик». При этом объект вышестоящего слоя подписывается на определенные сообщения объектов нижестоящего. Когда происходит ожидаемое событие, объект-издатель уведомляет о нем всех подписчиков.

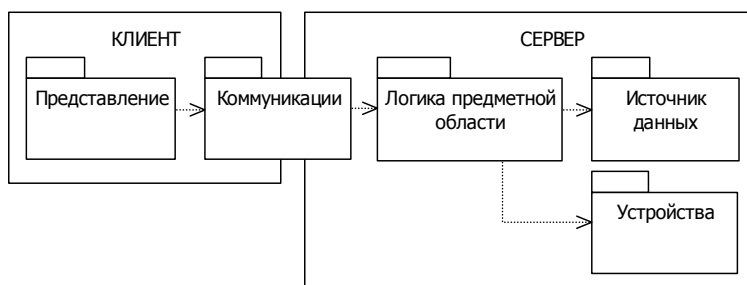


Рис. 1. Многослойная архитектура технологической системы

В заключение стоит отметить, что, несмотря на существующие недостатки, концепция разбиения системы на слои получила широкое распространение. Выделение слоев позволяет повысить гибкость программной системы, и, следовательно, увеличить один из важнейших параметров – время ее жизни.

ЛИТЕРАТУРА

1. Фаулер М. Архитектура корпоративных программных приложений.: Пер. с англ. М.: Издательский дом «Вильямс», 2004. – 544 с.
2. Ксензов М. Рефакторинг архитектуры программного обеспечения: выделение слоев. Режим доступа: <http://www.citforum.ru/SE/project/refactor/>, свободный.

СОЗДАНИЕ СВЕТОДИОДНОГО ТАБЛО С МЕХАНИЧЕСКОЙ ГОРИЗОНТАЛЬНОЙ РАЗВЕРТКОЙ НА БАЗЕ МК АТ89С8252

Е.А. Канский, студент 1 курса гр. УИТС-05;

*н. рук. О.Н. Кузяков, д.т.н., доцент зав. каф. Кибернетических систем
Тюменский государственный нефтегазовый университет (ТюмГНГУ),
г Тюмень, т. (3452) 31-85-18, jeka72@yandex.ru*

Как известно, в настоящее время наука и техника развиваются очень быстрыми темпами. Количество внедряемых изобретений и усовершенствование уже существующих приборов и устройств, облегчающих жизнь человека, поражает воображение. Среди них компьютеры, различная бытовая техника, фото и телевизионная аппаратура, мобильная связь и т.д. Для того чтобы непосредственно участвовать в создании этих устройств, надо хорошо изучать физику в школе. Однако интерес у школьников к изучению физики неуклонно понижается. Среди причин такого положения следует назвать плохую оснащенность кабинетов физики современными техническими устройствами, позволяющим не только поднять у учащихся интерес к изучению физики, информатики, но, и повысить информативность образовательного процесса. В этой связи, нами была сделана попытка изготовить устройство, позволяющее наглядно демонстрировать в ходе уроков физики некоторые явления, в частности, использование светодиодов для получения изображения. Исходя из этого выбор тематики исследования, на наш взгляд, представляется весьма актуальным.

Цель работы

Создать светодиодное табло с механической горизонтальной разверткой на базе МК АТ89С8252 и микросхемы К555ИР22 и проследить его влияние на познавательный интерес учащихся.

Задачи работы

1. Изучение литературы по программированию микроконтроллеров семейства MCS-51.
2. Подбор технической документации для компонентов, используемых при проектировании устройства.
3. Написание управляющей программы, ее отладка и запись в контроллер.
4. Разработка и создания модуля дистанционного управления.
5. Сборка устройства, отладка и испытание.
6. Изучение влияния изготовленного технического устройства на познавательный интерес учащихся.

Использованные в работе теоретические (изучение, анализ литературы, постановка целей и задач работы) и практические (проектирование устройства, эксперименты в реальных условиях, сборка, наладка и

внедрение в образовательный процесс) методы позволили решить задачи исследования.

Описание устройства

Светодиодное табло с механической горизонтальной разверткой представляет собой ряд светодиодов, расположенных перпендикулярно к плоскости вращения и соединенных с управляющим микроконтроллером. Механическая горизонтальная развертка осуществляется путем вращения источника света по окружности с высокой скоростью при помощи электродвигателя. За счет инертности зрения, у зрителя возникает образ цельного изображения. [1]

Изучив литературные источники по проблеме создания устройств на МК и соответствующую техническую документацию, в качестве объекта изучения авторы выбрали микроконтроллер AT89S8252 [2,3], принадлежащий к семейству команд x51.

Разработка устройства включает создание блок-схемы, принципиальной схемы и программы для микроконтроллера [4,5,6].

Блок-схема (рис. 1) содержит следующие элементы: микроконтроллер, который является ядром всего устройства; регистры, служащие для вертикальной развертки изображения; светодиодный модуль, являющийся исполнительным элементом всей системы – источником света; источник питания, обеспечивающий все устройство стабилизированным напряжением 5В; приемник ИК-сигнала, позволяющий управлять табло на расстоянии.



Рис. 1. Блок-схема светодиодного табло

К выходам регистров-защелок K555ИР22 подключено по 8 светодиодов, всего регистров 2. Каждый регистр подключен к шине данных. Для формирования последовательности зажженных светодиодов используется однокристалльная МикроЭВМ AT89S8252-24PI [7,8]. Максимальное разрешение составляет 40x16 точек, при радиусе окружности 13 см. Все устройство, вместе с источником питания смонтировано на вращающейся планке. Электронная часть устройства жестко соединена с вращающейся осью двигателя.

Трансляция исходного ассемблерного файла управляющей программы осуществлялась кросс-ассемблером TASM и заносилась в микроконтроллер способом внутрисхемного программирования с помощью программы AEC-ISP версии 1.0. [9]

Назначение устройства

Светодиодное табло применяется как учебное пособие на уроках физики, которое наглядно отображает явление инертности человеческого зрения, применение сложных полупроводниковых приборов, использование светодиодов в электронике. На наш взгляд, наиболее перспективным применением устройства является использование его в качестве учебного стенда при изучении микроконтроллерных систем. При таком подходе это уже готовая схема со средствами ввода и вывода информации, осуществляемыми с помощью различных типов устройств. Изменение управляющей программы дает возможность учащимся реализовывать свои алгоритмы работы имеющихся средств. Не исключается также добавление новых элементов в схему.

Светодиодное табло, как устройство отображения информации, может служить для вывода как текстовой, так и графической информации. Табло устанавливается стационарно, и может быть использовано в различных сферах: реклама, срочные объявления, вывески магазинов, праздничные вывески, приветствия.

Среди достоинств устройства можно назвать:

- Малое количество излучающих элементов.
- Хорошее качество изображения.
- Возможность увеличения количества излучающих элементов до 64 шт.
- Привлекательность светящегося изображения, особенно в ночное время.

Выводы

На основе изученных теоретических данных был осуществлен оптимальный подбор необходимых компонентов и *создана действующая модель светодиодного табло с механической горизонтальной разверткой на базе МК AT89S8252.*

В ходе проведенного исследования был сделан вывод о том, что светодиодное табло на базе МК AT89S8252 целесообразно использовать в учебном процессе в дисциплинах, связанных с изучением микропроцессорной техники.

ЛИТЕРАТУРА

1. МПК G02В 027/14, G02В 027/26, H04N 013/00, H04N 015/00. Способ формирования изображений и устройства для его осуществления. А.В. Торчигин.
2. Фрунзе А.В. Микроконтроллеры? Это же просто! Т. 1. М.: ООО «ИД СКИ-МЕН», 2002. 336 с.
3. www.atmel.com
4. Лачин В.И., Савелов Н.С. Электроника: Учеб. Пособие. 3-е изд., перераб. и доп. Ростов н/Д: изд-во «Феникс», 2002. 576 с.

5. *Баширов А.* Микроконтроллерная система дистанционного управления. Радио. 2005. № 11. с. 30, 31.
6. *Горошков Б.И.* Элементы радиоэлектронных устройств. Справочник. М.: Радио и связь, 1988. 176 с.
7. Э www.specelservis.ru
8. *Техническая документация «Atmel 8-bit Microcontroller with 8 K Bytes Flash».*
9. www.aec-electronics.com

ПРИМЕНЕНИЕ UML КАК РЕШЕНИЕ ПРОБЛЕМЫ ПРИ ПРОЕКТИРОВАНИИ ВСТРАИВАЕМЫХ СИСТЕМ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

Н.Л. Макеева, студент 1 курса;

Л.А. Кромина, преподаватель-стажер кафедры АСУ

*Кумертауский филиал Уфимского Государственного Авиационного
Технического Университета, республика Башкортостан, г. Кумертау,
т. 8(34761) 4-23-10, natik-love13@mail.ru, Luyda_kr@mail.ru*

Вопрос применения унифицированных методов проектирования программного обеспечения (ПО) при разработке систем цифровой обработки сигналов (ЦОС) долгое время практически не рассматривался. Ранние системы ЦОС разрабатывались на аналоговой элементарной базе, которые выполняли не сложные операции, и имели большую погрешность вычислений. При переходе с элементарной базы на цифровую основу широкое распространение в области ЦОС получили цифровые сигнальные процессоры (ЦСП), которые позволяли перенести вычисления с аналоговой формы на цифровую.

С появлением Unified Modeling Language (UML) и развитых средств проектирования ПО, нацеленных на разработку систем реального времени, процесс освоения новой технологии не будет очень долгим и сложным. UML содержит много концепций, уже знакомых разработчикам, и

позволяет описывать многие аспекты проектируемых систем.

Радиолокационная станция для мониторинга воздушного пространства – это предметная область. Если рассматривать на конкретном примере использование UML-методологии для построения сложной системы реального времени с использованием ЦОС. То предметом разработки будет радиолокационная станция (РЛС) для мониторинга воздушного пространства.

В состав станции входят: антенна, приемопередающее устройство, механизм управления антенной и блок вычислителя. Блок вычислителя, как правило, представляет собой многопроцессорный комплекс, постро-

енный на базе магистрально-модульного стандарта (VME, Compact PCI). На цифровой вычислитель ложатся следующие задачи: – первичная обработка радиолокационной информации – ПОРИ (выполнение алгоритмов фильтрации и спектрального анализа, характеризующихся интенсивными вычислениями и работающих на быстродействующих вычислителях – микросхемах жесткой логики или целочисленных ЦСП; программы на таких устройствах реализуются с использованием логики конечных автоматов); – вторичная обработка радиолокационной информации – ВОРИ (выполнение более сложных алгоритмов для оценки информации, полученной после первичной обработки, таких как формирование графической информации для вывода на дисплей оператора, обнаружение и оценка параметров движущихся объектов; программы представляют собой сложные алгоритмические конструкции с большим количеством условных переходов и выполняются на ЦСП с плавающей точкой);

Программы управления и контроля (предназначены для управления режимами работы РЛС и контроля работоспособности вычислительной системы; выполняются на вычислительном узле с ЦСП или обычным процессором, имеющим доступ ко всем магистралям передачи данных системы).

При первом анализе списка задач видно, что систем представляет собой комплекс программ различной сложности, работающих на ЦСП разной архитектуры и взаимодействующих между собой через различные интерфейсы. Необходимо построить спецификацию системы та, чтобы система легко модернизировалась и была наращиваемой, а спецификация содержала в себе требования, предъявляемые к системам реального времени.

Статическая структура проектируемой системы ПО для узла ПОРИ входит в состав станции наиболее требовательный к ресурсам, и его по не предусматривает использование операционной системы. В задачи узла входят получение оцифрованных сигналов с узла аналого-цифрового преобразователя, получение текущего режима обработки сигналов, выполнение математической обработки и передача обработанных данных на другие узлы для дальнейшего анализа. Данный узел представляет собой многопроцессорную плату, где полученные данные симметрично разбиваются между процессами и параллельно обрабатываются. Для узла ПОРИ строятся три основных множества классов: 1) драйверы устройств; 2) математические функции; 3) алгоритмы управления. Главным классом является класс Плата ПОРИ, включающий в себя остальные посредством агрегативных связей. Математические классы представляют собой своеобразные функции– «обертки» для вызова оптимизированного под конкретный процессор вычислительного кода, созданного разработчиком или поставляемого в виде библиотек вместе с системой программирования. Таким образом, при переносе

се программы на другую вычислительную платформу общая структура программы сохраняется, необходимо только переписать отдельные участки кода. Для удобства множества классов могут быть объединены в пакеты, которые используются в дальнейшем как шаблон для построения модернизированных конфигураций систем.

Декомпозиция системы на классы предоставляет разработчику, в том числе, возможность удобного тестирования отдельных компонентов системы, гибкого изменения и наращивания структуры ПО. К примеру, для добавления в пакет математических функций фильтра высоких частот достаточно создать новый класс путем наследования виртуального класса Фильтр и заполнить виртуальные функции алгоритмами высокочастотной фильтрации.

На основании всего вышеизложенного можно сделать следующий вывод: методология UML позволяет описывать практически все аспекты, необходимые для построения современных систем ЦОС. С применением подобной технологии проектируемая система будет легко модернизироваться и наращиваться, а также отвечать заданным требованиям по производительности и надежности. Использование нотации UML в программах ЦОС является хорошим дополнением к существующим методам. Таким как математическое моделирование, и позволяет разработчику получить законченные математические и программные модели, готовые к реализации.

ЛИТЕРАТУРА

1. *Петров В.П.* Информационные системы. СПб.: Питер, 2003. 688 с.
2. *Лойко В.И.* Информационные системы и технологии в экономике. М.: Финансы и статистика, 2003. 416 с.
3. *Информационно-управляющие системы* / Под ред. Сергеева М.Б. Научно-практический журнал № (1) 14/2005.

ПРОГРАММА ДЛЯ ОБРАБОТКИ ДАННЫХ ДЕФОРМИРУЕМОЙ ТВЕРДОЙ ПОВЕРХНОСТИ

С.К. Миргородский, студент 5 курса ФВС

ТСУСР, г. Томск, e-mail: Mirgorodskiy_Sem@mail.ru

Проблемы деформации твердых тел и локализации пластического течения изучается на протяжении многих десятилетий, но до сих пор находится в стадии, далекой от завершения. В последние годы практически все новые подходы и развиваемые в области физики прочности механики пластичности оригинальные идеи в той или иной мере связаны с анализом причин и особенностей локализации пластического течения, наблюдаемого в процессе деформирования твердых тел.

Задачей данной работы является разработка пользовательского интерфейса программы, дающей возможность построения трехмерного изображения тензора пластической дисторсии деформируемого твердого тела. Файлы, являющиеся основой для построения изображения, получены при помощи метода двухэкспозиционной спекл-интерферометрии, реализуемого в лаборатории физики прочности института физики прочности и материаловедения СО РАН. Данный метод подробно регистрирует поля смещения тензора дисторсии при пластической деформации макроскопического образца. В результате, имеется последовательная серия спеклограмм, охватывающая требуемый участок либо всю кривую деформации. Расшифрованные спеклограммы дают возможность последовательно зафиксировать поведение векторов смещения по всей кривой течения и получить данные о кинетике всех этапов процесса – от упругого деформирования до разрушения образца.

Требования, предъявляемые к программе:

- 1) возможность построения трехмерного изображения;
- 2) осуществление анимационного режима показа процесса деформации;
- 3) возможность автоматического определения длины волны (λ) деформационного процесса.
- 4) создание информационной панели для отображения найденной длины волны для каждого из участков деформации;
- 5) создание информационного окна для показа двумерного графика зависимости напряжения от деформации, отображаемого вместе с анимационным режимом. На графике будет наглядно отображаться текущее состояние процесса деформирования материала;
- 6) формирование отчета.

Основную трудность при выполнении данного этапа работы составило создание анимационного изображения. Для этого в меню введен пункт «Анимация». Для реализации данного пункта были использованы динамические переменные. Перед началом анимации строится массив, состоящий из трехмерных поверхностей, создается список шагов для каждого из участков, где участок является промежутком, соответствующим приращению между соседними спеклограммами. Данный шаг соответствует начальным экспериментальным данным. Значение приращения задается для каждой вершины отдельно. Это связано с тем, что направление движения вершин не одинаково: одна вершина может двигаться вверх, а другая вниз.

При написании программного кода для расчета шага применены следующие правила:

1. Для каждой ячейки матрицы находится разность между значениями координат по оси OZ двух ближайших поверхностей, соответствующих одинаковым координатам по x и y ;

2. Производится нормировка, т.е. максимальная амплитуда делится на некоторое число n (на данном этапе $n = 10$). Полученное значение будет отражать скорость перехода от одной поверхности к другой;

3. Создается дополнительная матрица для записи шагов и полученное значение заносится в ячейку созданной нами матрицы.

После указания пути и начала работы программы, создается массив из трехмерных поверхностей, который необходим как при создании динамического изображения, так и при просмотре в статическом режиме каждой из поверхностей в отдельности. Сам процесс анимации реализован с помощью таймера.

Перед началом определения длины волны, необходимо определить номер центральной линии по оси OY , разделив максимальную координату пополам. Далее определяется шаг, с которым взяты базовые точки, и общий интервал базовых точек.

В данной работе спектральный анализ выполняется с помощью быстрого преобразования Фурье. Данный алгоритм требует, чтобы количество базовых точек было равным числу 2^n . Таким образом, перед началом вычислений дополняем массив, предназначенный для вычисления, дополнительными данными. После заполнения всех необходимых данных вызывается функция быстрого преобразования Фурье.

Результатом выполнения функции являются два вектора, представляющих вещественную и мнимую составляющие комплексного числа. Для точного определения максимума полученных данных необходимо взять модуль комплексного числа. Критерием того, что данная последовательность базовых точек имеет какой-то период, является тот факт, что после выполнения преобразования Фурье, появляется четко выраженный максимум, который легко увидеть, если построить двумерный график зависимости номера точки и результата преобразования. Таким образом, необходимо определить все максимумы полученных данных.

Для определения четко выраженного максимума потребуются два наибольших максимума из всех. Если абсолютная разность этих двух максимумов, выраженная в процентах, больше определенного критического значения, то можно с уверенностью утверждать, что на данном этапе деформации никакой волны нет, и этот этап является переходным. Иначе утверждается, что на данном этапе деформации существует определенный период повторения базовых точек и, следовательно, длина волны.

Для определения максимумов был использован метод золотого сечения, который при работе выполняет небольшое количество вычислений функции, а именно $2 + N$, где N – число шагов выполнения.

Этот алгоритм работает только в случае, когда на определенном отрезке находится только один максимум функции. Следовательно, необходимо дополнить алгоритм так, чтобы он искал все максимумы на данном интервале $[a, b]$.

Доработка алгоритма заключается в следующем:

1. Вычисляется значение функции в точке a ;
2. Вычисляется значение в точке b ;
3. до тех пор, пока промежуточная переменная x не будет больше b , производим вычисления:
 - 3.1. ищем левую границу нового отрезка (т.е. пока функция убывает), увеличивая значение x на заданный шаг поиска;
 - 3.2. ищем правую границу нового отрезка (т.е. пока функция возрастает), увеличивая значение x на заданный шаг поиска;
 - 3.3. находим значение максимума при помощи метода золотого сечения, пока результат не будет меньше заданной точности (10^{-6});
 - 3.4. добавляем в выходной массив новое значение максимума;
 - 3.5. значение x увеличивается на заданный шаг поиска.

Внешний вид программы представлен на рис. 1.

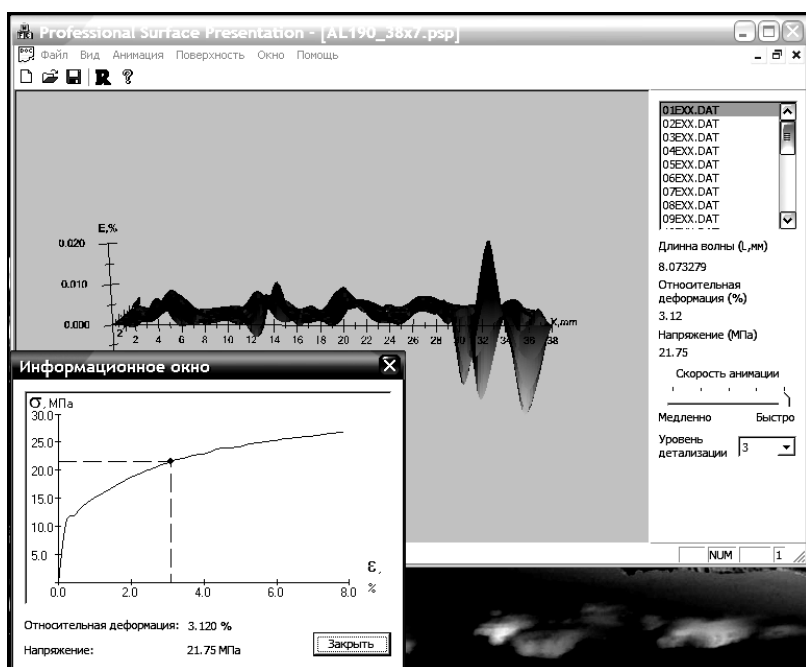


Рис. 1. Внешний вид программы.

Шаг поиска равен 0,2 мм. После выполнения данного алгоритма, на выходе получается вектор, который содержит все максимумы заданной функции.

В настоящее время данный программный продукт проходит тестирование в институте физики прочности и материаловедения СО РАН. Результаты тестирования были представлены в Петербургских чтениях в г. Санкт-Петербурге на базе физико-технического института как часть доклада заместителя директора по науке, профессора, доктора физико-математических наук Зуева Льва Борисовича.

ИСПОЛЬЗОВАНИЕ МНОГОСПЕКТРАЛЬНЫХ ДАННЫХ ПРИБОРА MODIS ДЛЯ ОБНАРУЖЕНИЯ ПОЖАРОВ

А.А. Моисеев, аспирант каф. КСУП

ТУСУР, г. Томск

В данной статье обсуждается возможность использования данных прибора MODIS для обнаружения пожаров. В связи с этим рассмотрим характеристики данного прибора.

Применение данных MODIS, прежде всего, обусловлено главными достоинствами системы – ежедневным всепланетным покрытием съемки, большим числом диапазонов съемки и относительно высоким пространственным разрешением.

В таблице приведено описание основных технических характеристик прибора MODIS.

Описание прибора MODIS

Орбита спутника	705 км, 10:30 нисходящий виток и 13:30 восходящий виток, солнечно-синхронная, околополярная, круговая
Частота сканирования	20,3 rpm
Размеры снимка	2330 км (поперек направления сканирования) на 10 км (вдоль направления сканирования)
Угол обзора системы	110°
Оптический прибор	17,78 см диаметр, неосевой, афокальный (коллимированный), с промежуточной диафрагмой
Частота передачи данных	10,6 Мб/с (максимальная, достигается в дневное время)
Радиометрическое разрешение исходных снимков	12 бит
Пространственно разрешение	250 м (каналы 1 – 2), 500 м (каналы 3 – 7), 1000 м (каналы 8 – 36)

Как уже было отмечено в таблице ширина полосы захвата (2) сканирующего радиометра MODIS (в просторечии именуемого «сканер») составляет около 2300 км. Реально используется средняя часть съемки (5), без краевых сильно искаженных областей (6). Полоса приемлемого качества составляет около 1500 км. Наилучшее качество данных вблизи осевой линии (1). Нарезка на куски (сцены) происходит уже после того как данные будут переданы со спутника (3) на наземную станцию приема (4).

Прибор MODIS производит снимки поверхности земли и океана в различных каналах видимого и инфракрасного диапазонов спектра.

Имеются группы спектральных каналов с пространственным разрешением 250, 500 и 1000 м на пиксель. Описание каналов представлено в [2].

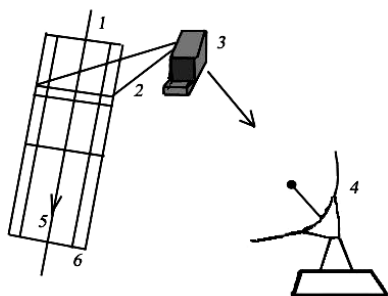


Рис. 1. Геометрия сканирования ППЗ прибором MODIS

На рис. 2 представлена карта, показывающая, какие группы каналов лучше всего подходят для обработки при определенной прозрачности атмосферы.

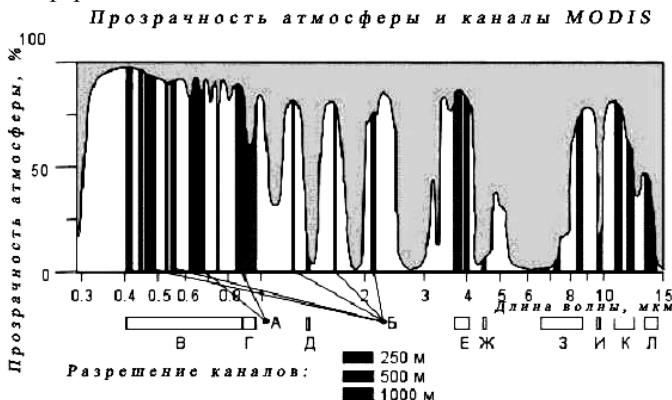


Рис. 2. Прозрачность атмосферы и каналы MODIS

Важной характеристикой прибора MODIS является поведение перекрестного зеркального сканирования. Двустороннее зеркальное сканирование отражает проекцию из 110° поля Земли при каждом шаге

сканирования, эффективно перемещаясь, десять пространственных элементов прибора дают полосу Земли шириной в 10 км в надире. Ширина сканирования увеличивается до 20 км при достижении угла сканирования $\pm 55^\circ$ из-за панорамного так называемого эффекта «бабочки» (рис. 3).

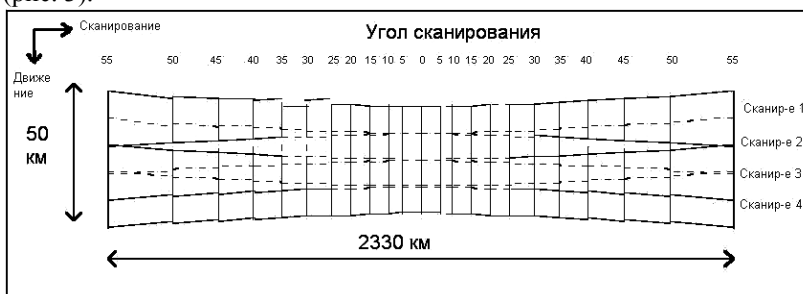


Рис. 3. Панорамный эффект «бабочки»

Этот эффект ведет к перекрытию полос сканирования при углах сканирования более чем 25° (рис. 4) (для разрешения 500 м и 250 м перекрытие возможно при меньших углах сканирования, для разрешения 250 м угол сканирования около 17°).

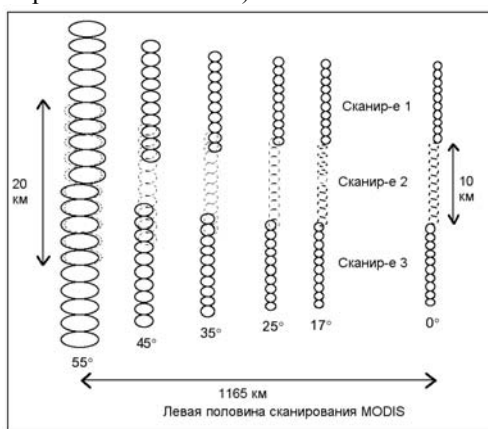


Рис. 4. Рост перекрытия в пределах сканирования

Данные зеркального сканирования измеряются и подаются в поток данных прибора. Затем данные поступают на Землю и обрабатываются различными алгоритмами для решения разных задач. Таким образом, данные прибора MODIS предпочтительнее использовать для решения задачи обнаружения пожаров, нежели данные прибора NOAA спутника AVHRR, которые используются в настоящее время.

ЛИТЕРАТУРА

1. Nishihama M., Wolfe R., Solomon D. MODIS Level 1A Earth Location: Algorithm Theoretical Basis Document Version 3.0
2. Методические рекомендации по приему, архивации, обработке и предоставлению в пользование информации ведомственной системы ДЗЗ МПР России.

ИЗУЧЕНИЕ ВЗАИМОСВЯЗИ ПАРАМЕТРОВ СИГНАЛОВ АКУСТИЧЕСКОЙ ЭМИССИИ С МЕХАНИЧЕСКИМ НАПРЯЖЕНИЕМ В ДЕФОРМИРУЕМЫХ МЕТАЛЛАХ

Е.С. Никитин, аспирант ОППО ТУСУР

ТУСУР, г. Томск, 89039528914, zooms02@mail2000.ru

В СКБ «Акустика» филиала ОППО ТУСУР в ИФПМ СО РАН ведутся исследования по изучению характера локализации источников сигналов (ИС) акустической эмиссии (АЭ) в образцах металлов, подверженных деформации. В связи с этим ставились следующие задачи: получение сигналов АЭ в широком диапазоне частот; запись сигнала АЭ в цифровом виде с высокой частотой дискретизации; привязка времени появления каждого отдельного сигнала АЭ к деформационной кривой нагружения; определение координат (локализация) ИС АЭ в исследуемом материале; изучение характера распределения ИС АЭ по длине образца с течением времени. На рис. 1 представлена схема экспериментальной установки (а) и объекта исследования (б).

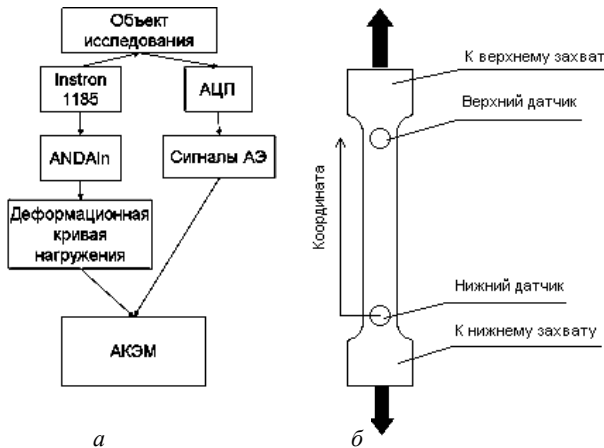


Рис. 1. Схема проведения эксперимента:

а) схема экспериментальной установки, б) объект исследования

Для деформирования образцов использовалась испытательная машина Instron 1185.

Для получения сигналов АЭ были выбраны пьезокерамические датчики с полосой пропускания 0,2–2000 кГц.

Для записи сигналов АЭ был использован прецизионный аналого-цифровой преобразователь **ЛА-н20-12РСІ** с высокой частотой дискретизации (до 50 МГц) и с двумя синхронными каналами.

Отметим, что на данный момент работа проводилась с использованием двухканального АЦП, поэтому локализация возможна только по одной координате. Таким образом, работа проводилась с плоскими длинными образцами (рис. 1, б).

Для привязки времени появления сигналов АЭ к деформационной кривой проводилась запись каждой выборки сигналов АЭ в отдельный файл. В нашем случае деформационная кривая нагружения записывается в отдельный файл при помощи программы ANDA, с указанием времени начала записи и указанием времени для каждого значения деформации.

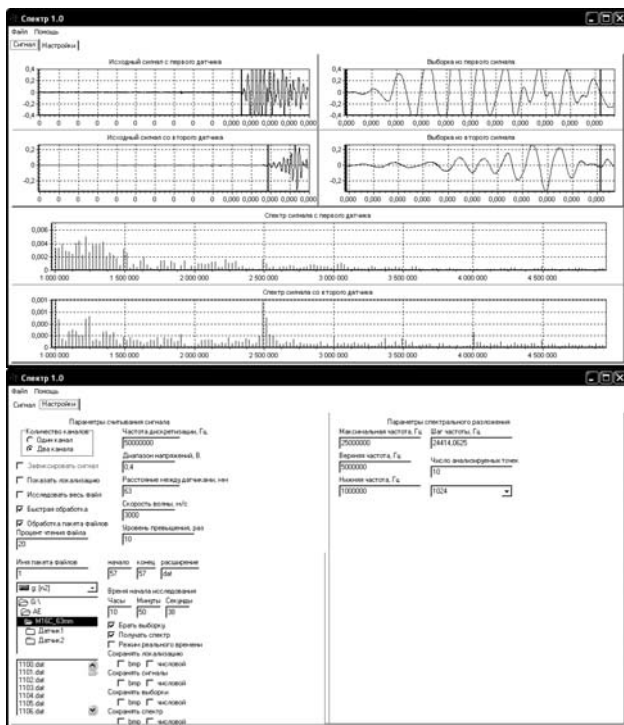


Рис. 2. Интерфейс программы обработки сигналов АЭ

Для локализации ИС АЭ был разработан программный продукт, позволяющий проводить цифровую обработку сигналов АЭ, включающую локализацию и привязку по времени к деформационной кривой нагружения для каждого сигнала АЭ [1]. На рис. 2 представлен интерфейс программного продукта, разработанного для обработки сигналов АЭ.

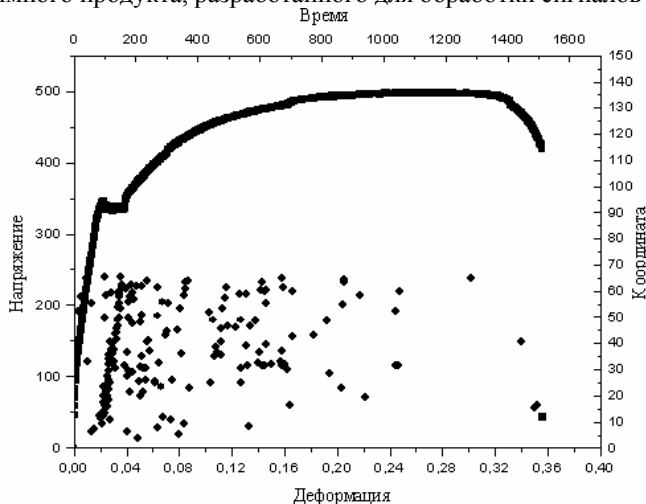


Рис. 3. Взаимосвязь распределения ИС АЭ по длине образца со стадийностью деформационной кривой для стали М16С (1)

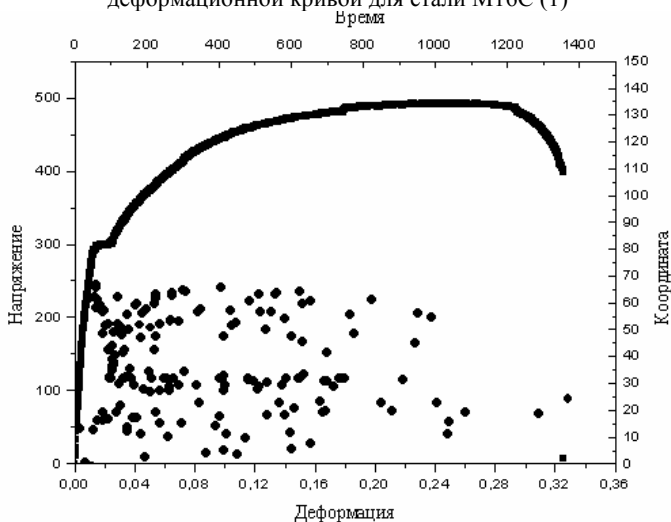


Рис. 4. Взаимосвязь распределения ИС АЭ по длине образца со стадийностью деформационной кривой для стали М16С (2)

После проведения серии экспериментов над образцами из кобальта, стали М16С, стали СТЗСП были получены результаты, представленные на рис. 3, 4, 5, 6.

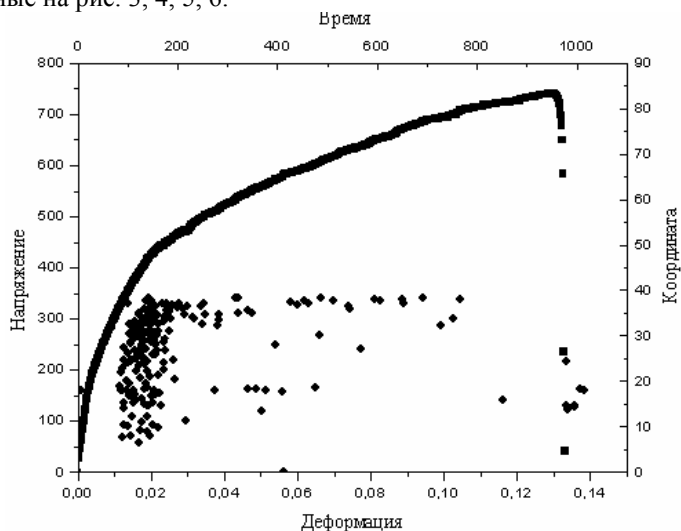


Рис. 5. Взаимосвязь распределения ИС АЭ по длине образца со стадийностью деформационной кривой для кобальта

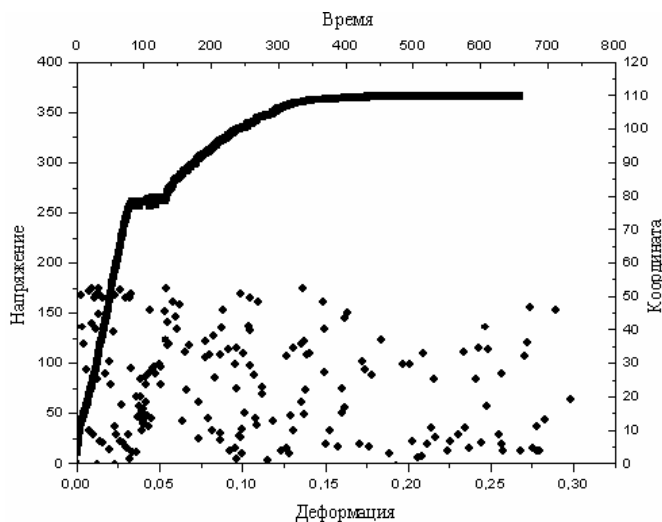


Рис. 6. Взаимосвязь распределения ИС АЭ по длине образца со стадийностью деформационной кривой для стали СТЗСП

По данным локализации ИС АЭ для каждого из представленных на рисунках 3, 4, 5, 6 распределения были построены поверхности, отражающие характер накопления количества ИС АЭ по длине образца с течением времени, которые представлены на рис. 7.

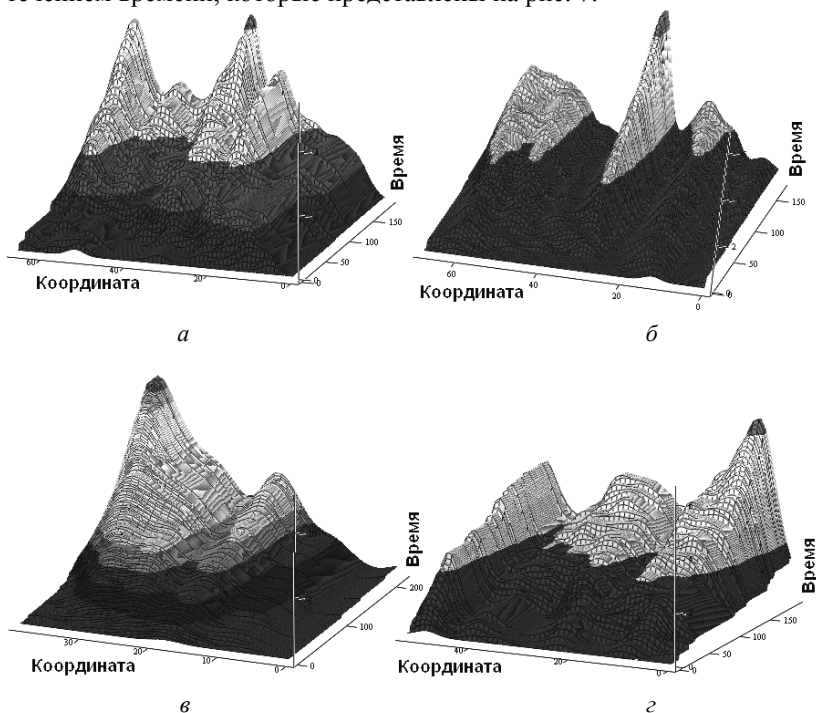


Рис. 7. Распределение накопления ИС АЭ по длине образца с течением времени: а) сталь М16С (1), б) сталь М16С (2), в) кобальт, г) сталь СТЗСП

На рис. 3 наблюдается упорядоченное движение ИС АЭ от нижнего конца образца к верхнему на стадии, соответствующей площадке текучести. Такое движение обусловлено продвижением по образцу фронта локализации деформации, называемого полосой Чернова-Людерса. По наклону распределения координат ИС АЭ была рассчитана скорость движения наблюдаемого объекта ($\approx 0,0003$ м/с), что хорошо согласуется со значениями, полученными другим способом.

На рис. 4 также наблюдается упорядоченное движение ИС АЭ, но уже сразу с двух сторон навстречу друг другу также на стадии, соответствующей площадке текучести. В данном случае мы имеем дело с двумя полосами Чернова-Людерса, движущихся, соответственно, друг навстречу другу.

На рис. 5 такого движения не видно, но в кобальте не наблюдали и полос Чернова-Людерса. Однако можно выделить стадию, на которой резко увеличивается и после которой также резко уменьшается частота появления сигналов АЭ.

На рис. 6 наблюдается картина подобная рис. 3 – на стадии соответствующей площадке текучести наблюдается упорядоченное движение ИС АЭ. В данном случае это также является частным случаем, т. к. иногда появляется несколько движущихся очагов источников сигналов АЭ, что мы также наблюдаем, локализуя ИС АЭ. Также можно видеть, что на всех четырех представленных графиках распределение количества импульсов по времени имеет похожий характер [2], т. е. находится в зависимости от механического состояния материала.

На рис. 7 видно, что распределение ИС АЭ по длине образца с течением времени не является равномерным, наблюдаются максимумы и минимумы. Заметим, что если эксперимент проводился до разрыва, то он происходил в месте, соответствующем одному из максимумов. Например, для распределений *a* и *б* (сталь М16С) разрыв произошел в области наибольших максимумов, в то время как для распределения *в* (кобальт) разрыв произошел в середине образца, т. е. в области меньшего максимума.

ЛИТЕРАТУРА

1. *Никитин Е.С.* Связь параметров разрушения деформируемых металлов с локализацией и спектром источников сигналов акустической эмиссии // *Фундаментальные проблемы новых технологий в 3-м тысячелетии: Материалы 3-й Всероссийской конференции молодых ученых.* Томск: Изд-во Института оптики атмосферы СО РАН, 2006. с. 684–687.
2. *Fisher R.M., Lally J.S.* Microplasticity detected by an acoustic technique. *Can. J. Phys.*, 1967, 45, p. 1147–1159.

ОБНАРУЖЕНИЕ КУСОЧНО-ПЛОСКОСТНЫХ ОБЪЕКТОВ ПО ДАННЫМ ЛАЗЕРНОГО ЗОНДИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ПОВЕРХНОСТНОЙ ТРИАНГУЛЯЦИИ

С.В. Пешехонов, студент 5 курса фак-та Информатики

ТГУ, г. Томск, т. 41-18-27, serpx@mail.ru

В настоящее время для получения цифровых моделей рельефа все большую популярность завоевывает использование зондирующих лазерных систем [1]. В таких системах для получения модели рельефа лазер, расположенный либо неподвижно на земле, либо находящийся на борту летательного аппарата, сканирует поверхность, посылая лучи

и регистрируя время получения отраженного сигнала. Таким образом, фактически, после сканирования получается некоторое облако трехмерных точек, которое, в свою очередь, используется для построения модели поверхности.

Построить модель поверхности Земли и расположенных на ней объектов можно следующим образом:

- 1) вначале построить поверхностную триангуляцию по точкам;
- 2) затем выделить участки земной поверхности и расположенные на ней объекты.

Каждый объект представляется совокупностью кусков поверхностей трехмерных тел из некоторого набора. Известно, что до 95% всех объектов, созданных человеком, состоят из частей цилиндров, конусов, сфер, торов и плоскостей [2]. При этом куски плоскостей наиболее вероятны. Наиболее сложной проблемой является разделение точек на такие группы, по которым можно было бы построить куски поверхностей различных тел. В известных методах это разделение производится, как правило, вручную.

В данной работе предлагается метод выделения плоскостей, основанный на поверхностной триангуляции, построенной на множестве исходных точек. Для обнаружения плоскости на каждом этапе выбирается некоторый нерассмотренный треугольник (рис. 1 слева).

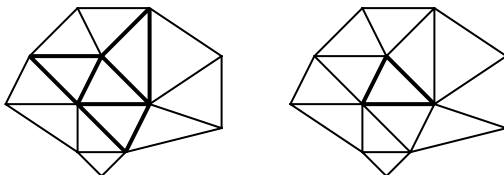
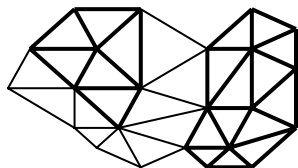


Рис. 1. Выделение кусочно-плоскостного объекта

Далее выбирается некоторое множество связанных с ним треугольников (на рис. 1 справа – 4 треугольника). Связным треугольником называется такой, который либо имеет общее ребро с первым, либо общее ребро со связным треугольником. По точкам, образующим эти треугольники, строится аппроксимирующая плоскость, для чего необходимо вычислить оценку (например, по методу наименьших квадратов [3]) трех числовых параметров, задающих уравнение плоскости в 3-мерном пространстве.

После вычисления параметров, задающих плоскость, начиная от первого треугольника, просматриваются все связанные треугольники и те из них, у которых хотя бы одна точка находится от аппроксимирующей плоскости на расстоянии, большем порога, отбрасываются, а осталь-

ные, помечаются, как принадлежащие плоскостному объекту. После этого параметры аппроксимирующей плоскости уточняются, используя уже все выделенные таким образом треугольники. Далее процесс выделения связанных треугольников продолжается с уже обновленными параметрами для искомой плоскости. Выделенная группа треугольников временно исключается из дальнейшего рассмотрения, после чего делается попытка обнаружения второй аппроксимирующей плоскости среди оставшихся треугольников и т.д. В результате будет получен набор фрагментов плоскостей. На рис. 2 представлен фрагмент поверхностной триангуляции с двумя выделенными плоскостными объектами, один из которых расположен от наблюдателя дальше, чем второй.



Для данного алгоритма задаются следующие управляющие параметры:

Рис. 2. Два выделенных плоскостных объекта, которые располагаются на разных уровнях.

1. Минимальное количество треугольников необходимое для построения первоначальных оценок аппроксимируемых плоскостей (ориентировочно 10).

2. Количество треугольников, достаточное для выделения плоскостного объекта. Зависит от того, насколько большие объекты можно считать полноценными.

3. Допустимая ошибка измерения координат объекта.

Трудоемкость такого алгоритма линейна относительно количества треугольников (а значит и точек). Константа в оценке трудоемкости прямо пропорциональна количеству треугольников, которые составляют порог выделения объекта.

В результате будет получен набор фрагментов плоскостей, с помощью которых можно строить также более сложные объекты, как сфера, цилиндр, конус или тор. На следующем этапе эти объекты могут быть использованы для выделения таких объектов как дома, дороги и пр.

ЛИТЕРАТУРА

1. GeoKosmos. Воздушное лазерное сканирование [Электронный ресурс]: <http://www.geokosmos.ru/news/articles/area/>
2. *Rabbani T., Heuvel F.* Efficient hough transform for automatic detection of cylinders in point clouds // Laser Scanning 2005. [Электронный ресурс]: Материалы конференции. – 2005. – Session 5. <http://www.commission3.isprs.org/laserscanning2005/>
3. *Shakarji C.M.* Least-Squares Fitting Algorithms of the NIST Algorithm Testing System // Journal of Research of the National Institute of Standards and Technology. 1998. V. 103. № 6. P. 633–635 <http://nvl.nist.gov/pub/nistpubs/jres/103/6/j36sha.pdf>

МНОГОФУНКЦИОНАЛЬНАЯ СИСТЕМА ОХРАНЫ И КОНТРОЛЯ ДОСТУПА

А.Н. Попов, студент 6 курса каф. РТС

ТУСУР, г. Томск, aks@70.ru

В настоящее время существует огромное количество систем охраны, противопожарных систем, систем, ограничивающих права доступа на различные объекты. Важнейшей частью таких систем являются сети для сбора данных, обмена информацией, управление исполнительными приборами и устройствами, контроля производственных процессов.

Требования к параметрам отличаются в зависимости от их применения, однако для любой сети важнейшими являются возможность реконфигурации, надежность, адаптивность, помехоустойчивость.

Вот далеко не полный перечень задач, предъявляемых к системам охраны и контроля доступа:

- 1) контроль времени и управление правами доступа персонала в помещения, территории и зоны;
- 2) контроль пожарной безопасности и управление средствами пожаротушения;
- 3) контроль и управление системами охраны;
- 4) управление доступом к производственному оборудованию, контроль состояния и дистанционное обслуживание этого оборудования.

Несмотря на различие, перечисленные задачи существуют и общие требования к параметрам систем охраны и контроля доступа, а именно:

- 1) большая протяженность линии;
- 2) значительное количество разнообразных датчиков, исполнительных устройств и приборов;
- 3) потребность в быстром изменении конфигурации системы, не нарушающем ее работу;
- 4) небольшой объем передаваемых данных;
- 5) относительно низкие скорости передачи данных.

Анализ существующих систем охраны и контроля доступа показал, что наиболее полно предъявляемым к ним требованиям соответствует архитектура сети MicroLAN. Кратко поясним, что архитектура MicroLAN представляет собой информационную сеть, использующую для осуществления цифровой связи одну линию данных и один возвратный (земляной) провод. Таким образом, для реализации среды обмена этой сети могут быть применены дешевые кабели, содержащие неэкранированную витую пару той или иной категории, и даже обычный телефонный провод. При прокладке линий сети MicroLAN не требуются наличие какого-либо специального оборудования, а ограничение максимальной

В качестве ведущего шины используется микроконтроллер фирмы Microchip PIC16F877, который позволяет оперативное перепрограммирование всей системы. Ветвление выполнено на микросхемах DS2409. В каждой ветви размещено до восьми датчиков температуры DS1820 и до четырех управляемых ключей DS2406 (рис. 2).



С помощью этих ключей осуществляется управление сильнотоочной нагрузкой типа вентиль, задвижка, нагревательный элемент. Уникальной особенностью датчика DS1820

Рис. 2. Внешний вид системы

является его возможность работы как термометра или термостата. Используя эти его свойства, он перепрограммировался для выполнения функций пожарной сигнализации в режим термостата на температуру +55 град. Функции доступа выполнялись с помощью ключей таблеток iBUTTON по одному входу на 5 ключей.

Проведены испытание разработанной системы.

ЛИТЕРАТУРА

- 1) www.maxim-ic.com
- 2) www.dalsemi.com
- 3) Яценков В.С. Микроконтроллеры Microchip. Практическое руководство. Москва. Горячая линия – Телеком. 2002. 296 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА СКЛАДСКОГО УЧЕТА МЕДИКАМЕНТОВ ДЛЯ АПТЕЧНОГО ОТДЕЛЕНИЯ НА ПЛАТФОРМЕ «1С: ПРЕДПРИЯТИЕ. ОПЕРАТИВНЫЙ УЧЕТ 7.7»

*А.А. Аксенова, студентка 5 курса ФВС
ТУСУР, кафедра КСУП, г. Томск, anastasiya@sibmail.com*

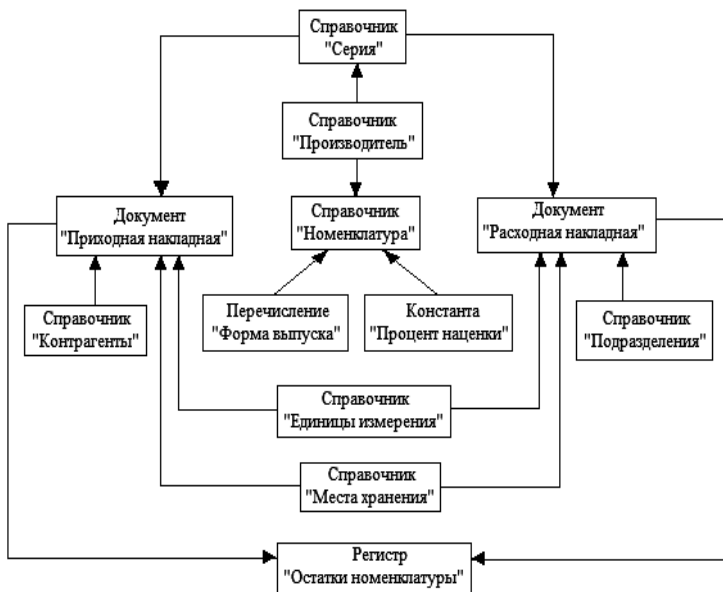
В настоящее время автоматизация деятельности различных предприятий, в том числе и аптек, приобрела глобальные масштабы. Этот процесс представляет собой создание некоего электронного помощника пользователя, так как ручной учет не дает гарантии правильности рас-

четов, вследствие чего, аптека может понести убытки. Кроме того, ручной учет занимает очень много времени.

В связи с этим возникает потребность в автоматизированной системе по ведению складского учета медикаментов. Такая система должна обладать следующими основными возможностями:

- ручная и автоматизированная технология ведения, пополнения номенклатуры и обновления цен;
- механизм расчета цены реализации;
- конфигурация должна учитывать специфику аптечной торговли, прежде всего лекарственными средствами (серийный, суммовый и предметно-количественный учет; групповая классификация);
- кроме того, должны быть основные операции: учет поступления товаров; контроль товародвижение по местам хранения; оперативное отслеживание остатков; ведение взаиморасчетов с поставщиками в разрезе договоров; ведение журнала документов.

В результате работы была создана конфигурация на платформе «1С: Предприятие 7.7» для компоненты «Оперативный учет». Данная конфигурация предназначена для ведения оперативного учета и управления товарными запасами и денежными средствами в аптечных учреждениях, реализующих лекарственные средства и предметы медицинского назначения.



Структура информационной базы

В процессе конфигурирования была сформирована структура информационной базы (см. рисунок), алгоритмы обработки, формы диалогов и выходных документов, печатные формы. Информационная структура спроектирована на уровне предусмотренных в системе «1С: Предприятие. Оперативный учет 7.7» типов обрабатываемых объектов предметной области (константы, справочники, документы, регистры, перечисления, журналы документов и др.) [1, 2].

При работе пользователя в режиме исполнения конфигурации обработка информации выполняется как штатными средствами системы, так и с использованием алгоритмов, созданных на этапе конфигурирования [1, 2].

Использование данной конфигурации позволит значительно повысить эффективность управления, так как она создает для административно-хозяйственных подразделений аптеки единое информационное пространство, тем самым, обеспечивая контроль работы аптеки. Также позволит устранить ошибки при ведении складского учета и снизить затраты времени на заполнение всех необходимых документов, отчетов и т. д.

ЛИТЕРАТУРА

1. *Фирма «1С». 1С:Предприятие 7.7. Конфигурирование и администрирование. Часть 1.* М.: Фирма «1С», 1999. 400 с.
2. *Фирма «1С». 1С:Предприятие 7.7. Конфигурирование и администрирование. Часть 2.* М.: Фирма «1С». 1999. 388 с.

ЗАЩИЩЕННЫЙ РЕЖИМ РАБОТЫ МИКРОПРОЦЕССОРА INTEL

*А.А. Аллянов, студент 5 курса ФВС;
В.В. Одионов, к.т.н., доцент каф. КСУП
ТУСУР, кафедра КСУП, г.Томск*

Начиная с процессора i80286 основным режимом работы микропроцессоров Intel является защищенный режим. Только в защищенном режиме полностью реализуются все возможности заложенные в современные процессоры, как то разделение привилегий, аппаратная поддержка многозадачности, адресация больших объемов памяти и т.д.

Требования, предъявляемые к современным операционным системам, заключаются в поддержке многозадачности, возможности работы с большими объемами памяти, защищенности задач друг от друга. Отсюда естественным образом следует, что все современные операцион-

ные системы работают именно в защищенном режиме. Однако несмотря на такую распространенность, вопросы программирования в защищенном режиме освещены в литературе очень слабо. Причин тому несколько, но основная причина заключается в том, что программисту разрабатывающему программу под конкретную операционную систему достаточно знать лишь архитектуру этой системы (а чаще не требуется и этого – достаточно знать лишь синтаксис языка программирования). Современные ОС скрывают от пользователя особенности аппаратной реализации, предоставляя свои внутренние функции посредством запросов. С одной стороны для пользователя это плюс. Но для программиста знание архитектуры процессора желательно, а для системного программиста – необходимо.

Операционная система выполняет две основные функции: предоставление пользователю вместо реальной аппаратуры некую абстрактную виртуальную машину, имеющую простой интуитивно понятный интерфейс; вторая функция – это управление ресурсами системы: распределение процессоров, памяти, устройств и данных между процессами, конкурирующими за эти ресурсы.

Целью данной работы была разработка учебной операционной системы, работающей в защищенном режиме и обладающей следующими возможностями:

- автономная загрузка
- обеспечение интерфейса с пользователем
- обработка аппаратных исключений
- обработка прерываний от устройств ввода-вывода и дискового.
- демонстрация работы в защищенном режиме посредством запуска нескольких процессов в режиме разделения времени.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА АНАЛИЗА РЕЗУЛЬТАТОВ ВНУТРЕННЕГО АУДИТА СМК В ИОА СО РАН

С.М. Андреев, студент 5 курса гр. 581-2

О.Е. Аркатова, зам. руководителя СлК

Филиал кафедры КСУП в ИОА СО РАН, г. Томск

Рассмотрены вопросы, связанные с построением системы анализа результатов внутреннего аудита СМК. Приведено описание основных модулей программы, описание статистических методов анализа данных.

Внутренние аудиты (проверки) являются высшей формой контроля руководством системы менеджмента качества (СМК) предприятия. Они проводятся для того, чтобы определить соответствие деятельности

и результатов в области качества запланированным мероприятиям, требованиям ГОСТ Р ИСО 9001:2001, а также требованиям, разработанным самой организацией. Результаты внутренних проверок служат основой входных данных для анализа со стороны руководства и позволяют организации декларировать свое соответствие ИСО 9001 [1].

В стандарте ГОСТ Р ИСО 9001:2001 исключительную актуальность имеет процедура оценивания результативности процесса внутреннего аудита по установленным критериям.

С целью облегчения процедуры анализа внутреннего аудита, для службы качества института оптики атмосферы (ИОА СО РАН), разрабатывается компьютерная программа позволяющая автоматизировать процесс анализа результатов внутреннего аудита СМК.

Программа включает в себя базы данных (БД), модуль для анализа данных, модуль графического представления результатов анализа (графики, гистограммы и т.д.), а так же справочную систему по основным несоответствиям и типичными корректирующими действиями.

Базы данных разработаны на основе результатов внутреннего аудита СМК ИОА 2005 года и содержат необходимую информацию для проведения статистического анализа.

Основной задачей при создании программы являются выбор методов анализа информации.

В ходе анализа поставленной задачи и основываясь на рекомендациях ГОСТ Р ИСО 9001:2001, в качестве основных статистических методов анализа данных были выбраны:

- для количественного анализа – диаграмма Парето и гистограмма;
- для качественного анализа – причинно следственная диаграмма (диаграмма Исикавы).

Диаграмма Парето – разновидность столбиковой диаграммы применяемой для наглядного отображения рассматриваемых факторов в порядке уменьшения их значимости. В результате анализа диаграмм Парето выявляют несоответствия, имеющие наибольшую долю (наибольший процентный вклад) и намечают мероприятия по их устранению. Сравнивая диаграммы Парето, построенные по данным до и после улучшения процесса, оценивают эффективность принятых мер.

Гистограмма применяется, когда требуется исследовать и представить распределение данных о числе единиц в каждой категории с помощью столбикового графика.

В общем случае гистограмма используется для:

- отображения картины изменения;
- передачи визуальной информации о поведении процесса;
- принятия решения о том, где сосредоточить усилия и улучшению [2].

В программе гистограммы отображают общую динамику подразделения (количество несоответствие за определенный период и количество принятых мер к разрешению ситуации), так же возможно отображение наиболее часто встречающихся несоответствий как в абсолютном так и в относительном выражении.

Причинно-следственная диаграмма часто называется также диаграммой Исикавы (по имени ее автора), диаграммой «причина-следствие», «рыбья кость», «рыбий скелет». Она позволяет выявить и систематизировать различные факторы и условия оказывающие влияние на рассматриваемую проблему (выявленную при анализе диаграммы Парето). При построении диаграммы выбираются наиболее важные с технической точки зрения факторы. Причины сортируются на наиболее вероятные; на причины, связанные с рассеянностью, и причины, связанные с небрежностью персонала; на причины трудноустраняемые и причины, которые невозможно устранить [3].

Так же программой предусмотрена возможность отображения статистики, как по отдельным подразделениям организации так и по нескольким.

В данный момент ведется разработка модуля анализа данных и их графического представления.

ЛИТЕРАТУРА

1. ГОСТ Р ИСО 9001:2001 Система менеджмента качества. Требования.
2. Сундарон Э.М. Статистические методы контроля и управления качеством. Учебное пособие. Улан-Удэ: Издательство ВСГТУ, 2002. 54 с.
3. Свиткин М.З., Мацута В.Д., Рахлин К.М. Менеджмент качества и обеспечение качества продукции на основе международных стандартов ИСО. СПб, 1999. 401 с.

АВТОМАТИЗАЦИЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ЭЛЕКТРОМАГНИТНЫХ ПРОЦЕССОВ В ЭЛЕКТРОМЕХАНИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЯХ

С.М. Андреев, студент 5 курса

Филиал каф. КСУП ТУСУР в ИОА СО РАН, г. Томск, e-mail: ami@nm.ru

В.И. Андреев, к.т.н., доцент

Томский Государственный Архитектурно-Строительный Университет

Ускоренное проникновение постоянно совершенствующейся полупроводниковой техники в область электромеханики приводит к существенному отклонению от классических гармонических форм кривых токов, напряжений, магнитных потоков и требует изменения и по-

явления конструкций электромеханических устройств, иногда весьма далеких от традиционных.

Так в [1] на основе системного подхода решается задача создания безредукторного привода на примере низкоскоростных электродвигателей вращательного, поступательного и возвратно-поступательного типов, для чего используются многополюсность машины и снижение частоты питающего напряжения, машины с катящимся ротором, машины, работающие на субгармониках магнитного поля и т.п.

В [2] на примере механического затвора лидара предложено совмещать функцию диска затвора с функцией ротора электромеханического преобразователя.

Одна из главных задач современной электромеханики – создание методов исследования как электромеханических систем, объединяющих различные электромеханические преобразователи, электрические, механические элементы и полупроводниковые устройства, так и способов моделирования магнитных полей и изучения процессов в самих электромеханических преобразователях.

Электрическая машина, без всякого сомнения, является ядром и наиболее сложным элементом любой электромеханической системы, и сама может рассматриваться как сложная система, объединяющая в себе электромагнитные, электрические, волновые, тепловые, механические и гидроаэродинамические явления.

Исследования электромеханических преобразователей с целью создания наиболее приемлемой для конкретного применения электрической машины проводят либо экспериментальным путем, либо путем физического (на основе методов подобия) [3] или математического моделирования.

Одним из способов упрощения исследования путем математического моделирования является переход от непрерывных (распределенных) сред к дискретным (сосредоточенным). При этом уравнения Максвелла переводятся в уравнения Лапласа и Пуассона. Затем рассчитываются магнитные потоки частей ферромагнитных сердечников, потокоцепления обмоток электрической машины.

Знание магнитных потоков позволяет определить потери на перемагничивание, магнитные напряжения и по интегральной форме закона полного тока – необходимую магнитодвижущую силу обмоток.

Вектор потокоцеплений обмоток позволяет перейти к решению дифференциальных уравнений, описывающих процессы в электрических цепях, составной частью которых являются обмотки электрической машины.

На этом этапе представляется возможным формирование адаптивной модели с ограниченным набором только тех переменных, которые признаются существенными, что значительно сокращает вычисления.

Этот же принцип лежит в основе всех наиболее эффективных численных методов расчета магнитных полей в электрической машине: методы конечных разностей, конечных элементов, граничных элементов и т.д., обладающие исключительной универсальностью [3].

На основе универсальных численных методов разработаны и широко применяются программные комплексы автоматизированного моделирования электромагнитных процессов, например, MotorPro [4] и ELCUT [5].

Анализ этих двух программных продуктов позволяет сформулировать основные требования к программе, реализующей основные идеи моделирования электромагнитных процессов в электрических машинах:

- в основу должен быть положен наиболее достоверный метод моделирования электромеханических систем;
- выбирать метод решения уравнений необходимо по максимуму скорости вычисления и минимуму погрешности расчетов;
- необходимо обеспечить (например, за счет использования специализированной программы), быстрый ввод графического представления моделируемого объекта.

На основе сформулированных требований предполагается разработать программу, блок-схема которой должна содержать, как минимум, четыре основных блока: блок «Математическая модель», вычислительный модуль, графический редактор, модуль связи с графическим редактором.

В блоке «Математическая модель» содержится математическое описание численных методов моделирования системы.

Вычислительный модуль, отвечающий за решение математической модели, содержит в себе численные методы решения систем уравнений.

Графический редактор обеспечивает отображение результатов моделирования.

Модуль связи с графическим редактором обеспечивает корректное преобразование результатов вычислений в графическую информацию.

Такая организация позволяет обеспечить быстрый ввод и вывод графических данных, а также позволяет использовать широкий спектр математических моделей.

Предлагается разрабатывать систему в среде программирования, относящаяся к классу RAD – (Rapid Application Development – «Средство быстрой разработки приложений») – Delphi. Этот выбор обусловлен не только легкостью процесса разработки программ, но широкими дополнительными возможностями предоставляемыми Delphi.

В качестве графического редактора целесообразно использовать уже готовый продукт, предоставляющий широкий набор инструментов

для работы с графикой. Таким продуктом можно считать систему автоматизированного проектирования конструкторской документации AutoCAD.

Взаимодействие инструмента разработки Delphi и графического редактора AutoCAD осуществляется посредством СОМ технологий. Объектная модель AutoCAD имеет открытый программный код, предоставляемый библиотеками типов (type library) [6], что значительно облегчает программирование приложений взаимосвязанных с AutoCAD.

ЛИТЕРАТУРА

1. *Свечарник Д.В.* Электрические машины непосредственного привода. М.: Энергоатомиздат, 1988. 208 с.
2. *Андреев С.М.* Модернизация механического затвора лидара // Материалы Международной научно-практической конференции. Томск: Издательство Института оптики атмосферы СО РАН, 2004. В 3 частях. Ч. 3. С. 122..
3. *Иванов-Смоленский А.В., Кузнецов В.А.* Универсальный численный метод моделирования электромеханических преобразователей и систем. «Электричество» №7, 2000. с. 24–33.
4. *MotorPro* Introduction, КОМОТЕК Co., Ltd.
5. ELCUT Manual, ПК TOP
6. *Зуев С.А., Полеицук Н.Н.* САПР на базе AutoCAD – как это делается. СПб.: БХВ-Петербург, 2004. 1168 с.

СИСТЕМА МОНИТОРИНГА ПРОГРАММНОГО И АППАРАТНОГО ОБЕСПЕЧЕНИЯ СЕРВЕРНЫХ СТАНЦИЙ. КЛИЕНТСКАЯ ЧАСТЬ

*А.В. Бугреев, студент 5 курса ФВС;
В.В. Одионов, к.т.н., доцент кафедры КСУП
ТУСУР, кафедра КСУП, г.Томск*

Введение в проблемную область. В настоящее время все больше компаний использует сеть Интернет в своих целях. Чем больше компания, тем больше серверных станций она использует. Как правило, в них задействовано один – два системных администратора. Возникает проблема отслеживания, то есть мониторинга работы серверных станций в целом. Внедрение такой системы позволит повысить производительность работы компании и уменьшить время простоя оборудования. В данной работе требуется разработать клиентскую часть системы мониторинга.

Кратко опишем функции клиентской части:

– загрузка настроек

- установление соединения с сервером
- передача данных
- снятие показателей
- хранение показателей в лог-файлах

Структура системы. Система будет состоять из клиентской и серверной части. Это есть клиент – серверное приложение. Клиентская часть устанавливается на сервера, за которыми нужно следить. Эти сервера будем называть контролируемые сервера. Клиентская часть должна снимать и пересылать на серверную часть системы текущую информацию об аппаратной и программной частях контролируемых серверов. Серверная часть предназначена принимать и обрабатывать информацию, получаемую от всех клиентских частей, а также хранить и предоставлять интерфейс для ее (информации) просмотра. Информацию о контролируемом сервере возможно посмотреть локально, т.е. на той же машине, где установлена клиентская часть системы.

Методы решения. Алгоритм работы: запущенная программа читает настройки из конфигурационного файла, производит сбор указанной в конфигурационном файле информации, сохраняет ее в лог-файлы, соединяется с серверной частью системы и передает снятую информацию, через указанное время действия, начиная со сбора информации, повторяются. Клиентская часть представляет собой фоновый процесс без управляющего терминала, поэтому завершать работу клиента нужно при помощи посылки определенного сигнала клиентскому процессу.

В процессе разработки клиент – серверного приложения важной и необходимой задачей является описание протокола взаимодействия клиентской и серверной части, то есть как клиентская и серверная части будут «общаться». Такой протокол часто называют прикладным протоколом. Передаваемые на сервер данные логически состоят из двух частей: служебные данные и снятые показатели. Служебные данные содержат ключевые слова, идентификатор клиентской части и время снятия показателей.

На данном этапе работы приняты решения о выборе структуры системы, инструментария для разработки, определены алгоритмы клиентской части. Разработан прикладной протокол системы. Изучены аналоги разрабатываемой системы.

К дальнейшей работе следует отнести написание комплекта технической документации и реализацию клиентской части системы, а также отладка всего клиент – серверного приложения.

ЛИТЕРАТУРА

1. Куроуз Дж. Ф., Росс Кит В. Компьютерные сети. 2-е издание. Изд. Питер, 2004. 765 с.

АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС ДЛЯ ИЗМЕРЕНИЯ И КОНТРОЛЯ ТОПОГРАФИИ МАГНИТНОГО ПОЛЯ МНОГОПОЛЮСНЫХ МАГНИТНЫХ СИСТЕМ

Р.О. Бурлаков, студент 5 курса ФВС

ТУСУР, кафедра КСУП, г. Томск

Основным элементом бесконтактных двигателей постоянного тока (БДПТ), широко применяемых в различных областях экономики, являются многополюсные постоянные магниты и многополюсные магнитные системы (МПМС) [1].

Оптимизация МПМС является центральным вопросом усовершенствования БДПТ. При этом до настоящего времени остается на стадии постановки задачи ряд серьезных проблем.

Во-первых, не выработано единое мнение о том, какой тип магнитной системы – с осевым или радиальным магнитным рабочим зазором (и, соответственно, направлением намагничивания кольцевого магнита) является предпочтительным. Отсутствует достаточно глубокий анализ эффективности магнитных систем разных видов, слабо изучено распределение поля многополюсных магнитов в его неразрывной связи с параметрами и конструкцией обмоток возбуждения.

Во-вторых, недостаточно изучены технико-экономические вопросы выбора материала постоянного магнита и технологии изготовления элементов ротора.

Для выбора путей решения этих проблем необходимо иметь соответствующую контрольно-измерительную аппаратуру. Она должна позволять подробно изучать распределение поля в рабочем объеме МПМС.

Качество МПМС БДПТ всех видов определяется не только средним значением индукции рабочего поля, но и тем, насколько конструкция отвечает своему главному назначению – созданию заданного закона распределения поля.

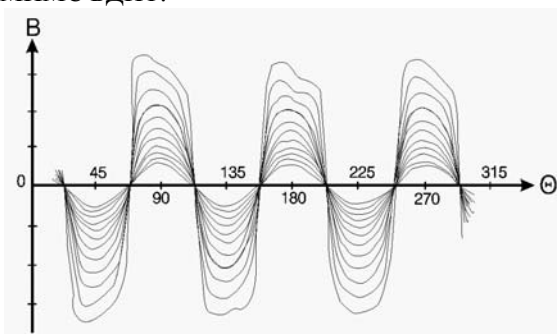
Для БДПТ значение индукции и закон ее распределения должны быть выдержаны с высокой степенью точности, так как от этого зависят основные характеристики устройства. Поэтому контроль топографии поля таких систем является неотъемлемой частью их опытно-конструкторской разработки и технологического процесса производства.

При измерении координатных составляющих магнитной индукции в рабочем объеме следует правильно выбирать траекторию движения измерительного зонда с первичными преобразователями индукции относительно координатных линий МПМС. Магнитное поле многополюсных систем БДПТ является осесимметричным, поэтому для оценки

его асимметрии следует измерить составляющие магнитного поля в функции цилиндрических координат. Для реализации этого был разработан автоматизированный комплекс.

Аппаратная часть комплекса представляет собой систему позиционирования датчика магнитного поля относительно исследуемой магнитной системы (магнитного ротора). В качестве датчика магнитной индукции был выбран датчик Холла, как наиболее оптимальный вариант по стоимости, габаритам, точности и простоте эксплуатации.

Программная часть автоматизированного комплекса предназначена для обработки данных, полученных от аппаратной части. На основании данных от датчика магнитной индукции, полученных при разных значениях угла Θ (угла поворота исследуемой МПМС), программа строит график зависимости магнитной индукции исследуемого объекта от угловых координат (рис.). По построенному графику визуально, либо при помощи дополнительных программ определяется качество исследуемой МПМС БДПТ.



Топография поля 6-полюсной магнитной системы

Разработанный автоматизированный комплекс позволит получать информацию о топографии рабочего поля МПМС БДПТ на этапе конструкторской отработки, что позволит получить заметный выигрыш за счет снижения массы магнитного материала или за счет упрощения конструкции.

ЛИТЕРАТУРА

1. Зайцев Г.Ф. Бесконтактные двигатели постоянного тока. М.: «Солон», 2003. 272 с.

ПРОГРАММА «ДИАГРАММА СМИТА»

Л.Л. Васильев, студент 5 курса ФВС;

М.В. Черкашин, ст. препод. каф. КСУП

ТУСУР, кафедра КСУП, г. Томск

Проблема согласования сопротивлений – одна из основных, с которой приходится сталкиваться разработчику цепей, образованных из отрезков линий передачи. Известно, что при рассогласовании (сопротивление нагрузки не равно волновому сопротивлению) часть энергии падающей волны отражается к генератору. Суперпозиция падающей и отраженной волн приводит к появлению в определенных сечениях линии передачи узлов и пучностей. В результате образуется стоячая волна. При высоком уровне передаваемой мощности это нежелательно, так как в режиме стоячей волны максимумы тока и напряжения могут в два раза превышать их уровень в режиме согласования. Столь значительное увеличение тока и напряжения нередко приводит к пробоем или разрушению диэлектрического заполнения [1].

Нередко волна, отраженная от нагрузки линии, оказывается причиной затягивания частоты генератора, питающего линию. Генератор начинает работать на частоте, несколько отличающейся от требуемой. В приемных устройствах рассогласование с антенной служит источником потерь части энергии, так как не вся принятая энергия поступает на вход усилителя. Тем самым ухудшаются параметры приемного устройства. Бывает весьма полезно контролировать уровень рассогласования, поскольку, например, в маломощных усилителях величины входного сопротивления активных элементов, соответствующие максимуму усиления и минимуму шумов, не совпадают. Преднамеренное рассогласование на входе усилителя нередко улучшает шумовые характеристики при несколько меньшем усилении.

Что необходимо предпринять для достижения требуемого уровня согласования?

Во-первых, следует овладеть методами расчета уровня рассогласования, вызываемого нагрузкой, подключенной к источнику. Во-вторых, необходимо овладеть методами направленного воздействия на уровень отражений, что дает возможность разработчику достигнуть требуемого уровня согласования. Существенную информацию позволяет получать подход, основанный на использовании диаграммы Смита.

Цель данной работы – написание программы расчета СВЧ-цепей с помощью диаграммы Смита.

В программе для представления диаграммы Смита используется графический метод представления коэффициента отражения на плоско-

сти сопротивления (проводимости) нагрузки. Так как относительное сопротивление состоит из активной и реактивной части, представляем коэффициент отражения в декартовой системе координат. При этом выделяя мнимую и действительную часть, получим систему уравнений представляющую семейство окружностей. В результате построения этих окружностей для всех возможных x и r , получается диаграмма Смита [1].

Программа выполняет следующие функции: отображает на экране диаграммы сопротивлений и проводимостей; представляет возможность изменения масштаба и цветовой палитры диаграмм; производить расчет в режиме реального времени, таких параметров, как: сопротивление, проводимость, КСВН (коэффициент стоячей волны по напряжению) и комплексного коэффициента отражения (в полярных координатах, длина равна модулю коэффициента отражения, а угол между радиус-вектором и положительной полуосью – угол коэффициента отражения в градусах), в точке, указанной курсором мыши; представляет ввод данных, как с клавиатуры, так и с помощью мыши; отображает на экране окно, в котором выводятся сведения обо всех введенных точках, отображает на экране окно, в котором строится принципиальная схема согласующей цепи и годограф ее сопротивления (проводимости), с физическими параметрами элементов, представляет возможность загрузки и сохранения данных в текстовый файл в собственном формате.

В качестве среды реализации программы была использована Microsoft Visual C++ 7.0.

Использование данной программы возможно студентами – в учебных целях для ознакомления с методом согласования с помощью диаграммы Смита, а так же в практических целях – разработчиками СВЧ устройств.

ЛИТЕРАТУРА

1. Фуско В. СВЧ-цепи. Москва: Радио и связь. 1990. 288 с.

АВТОМАТИЗАЦИЯ ПРОЦЕССА ИЗМЕРЕНИЯ ФОКУСНЫХ РАССТОЯНИЙ ОПТИЧЕСКИХ ЭЛЕМЕНТОВ

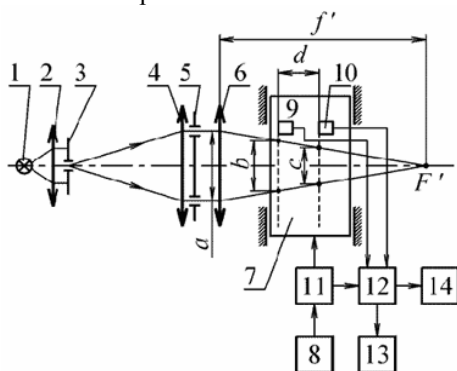
*Д.Н. Вершинин, студент 5 курса
ТУСУР, кафедра КСУП, г.Томск*

В настоящее время в практике физических и цеховых лабораторий приборостроительных предприятий оптического профиля используются, в основном, визуальные методы определения фокусных расстояний оптических элементов [1].

Между тем появилась новая элементная база, особенно в области электроники, которая позволяет автоматизировать процесс определения фокусных расстояний оптических элементов. Это позволяет создать контрольно-измерительные приборы совершенно нового поколения, способные работать в полуавтоматическом или автоматическом режимах. При этом такие приборы являются приборами объективного типа, то есть результаты измерения свободны от субъективных (личных) погрешностей наблюдателя. Данные приборы имеют, как правило, более высокое быстродействие, повышенную точность измерения и сравнительно малые габариты.

Для автоматизации процесса измерения фокусных расстояний предлагается усовершенствовать классическую установку Юдина-Фабри [2].

Структурная схема усовершенствованной установки представлена на рисунке. Работа установки основана на непосредственном измерении угла наклона узких пучков лучей без включения в схему измерения дополнительных оптических элементов, вносящих в результаты измерения дополнительные погрешности.



Усовершенствованная установка для определения фокусных расстояний оптических элементов по методу Юдина-Фабри

Источник света 1 при помощи конденсора 2 параллельным пучком равномерно освещает узкую щель 3, установленную в передней фокальной плоскости объектива коллиматора 4. Объектив коллиматора формирует широкий пучок лучей, из которого щели непрозрачного экрана 5 вырезают два узких пучка лучей, расстояние между осями которых известно с высокой степенью точности. После прохождения контролируемого компонента 6 пучки лучей собираются в его задней фокальной плоскости (в заднем фокусе). Из рисунка видно, что для опре-

деления величины фокусного расстояния при известной величине a необходимо измерить угол наклона пучков лучей α .

Для определения угла α искусственно создаются две секущие плоскости, перпендикулярные оптической оси системы и расположенные на расстоянии d друг от друга. Если измерить расстояния b и c между центрами узких пучков лучей в двух секущих плоскостях, то можно определить искомый угол:

$$\operatorname{tg} \alpha = (b - c) / 2d . \quad (1)$$

Для реализации данного метода используется каретка 7, перемещающаяся перпендикулярно оптической оси системы и несущая на себе два координатно-чувствительных фотоприемника 9 и 10, установленных вдоль направления оптической оси. Расстояние между светочувствительными площадками фотоприемников равно d .

В процессе измерения каретка 7 при помощи электродвигателя 8 перемещается перпендикулярно оптической оси системы. Связанный с электродвигателем или непосредственно с кареткой датчик линейных перемещений 11 непрерывно выдает информацию о величине перемещения каретки от первоначального положения, которая поступает в блок обработки информации 12 (БОИ). В момент, когда энергетический центр узкого пучка лучей совпадет с линией раздела любого фотоприемника (пучок энергетически симметричен относительно линии раздела), в блоке обработки информации 12 запоминается отсчет с датчика линейных перемещений 11. Всего запоминается четыре значения (по два с каждого фотоприемника) и по ним определяются расстояния b и c между следами узких пучков лучей в двух секущих плоскостях.

При известном расстоянии d , которое предварительно вводится в память БОИ, автоматически определяется $\operatorname{tg} \alpha$ по формуле (1).

Если в память БОИ предварительно введено расстояние « a » между центрами узких щелей непрозрачного экрана 5, то значение фокусного расстояния контролируемого компонента определяется по формуле:

$$f' = a / 2 \operatorname{tg} \alpha = ad / (b - c) . \quad (2)$$

В данном устройстве все расчеты производятся в БОИ и результаты могут быть выведены на экран цифрового табло 13 или цифropечатающее устройство 14.

Большим преимуществом разработанного устройства является высокая точность измерения, объективность полученных результатов, большое быстродействие и малые габариты конструкции, независимые от величины измеряемого фокусного расстояния. Все это дает возможность использования установки непосредственно в оптическом цехе и производить стопроцентный выходной контроль линз и склеенных компонентов с выдачей аттестата.

ЛИТЕРАТУРА

1. *Парвулюсов Ю. Б.* Проектирование оптико-электронных приборов. М.: Машиностроение, 1990. 432 с.
2. *Пизюта Б.А., Михайлов И.О.* Новые оптико-электронные приборы для оптических измерений. Сибирская Государственная Геодезическая Академия, 2004. 348 с.

РАЗРАБОТКА БАЗЫ ДАННЫХ «РЕМОНТ» ДЛЯ КОМПЬЮТЕРНОЙ ФИРМЫ «ИНСТАЛ»

О.А. Гайдамака, студентка 5 курса ФВС;

Е.Н. Рыбалка, ст. преподав. каф. КСУП

Томск, ТУ СУР, кафедра КСУП, e-mail: sierra@mail2000.ru

Функционирование любой организационной системы связано с наличием и обработкой различной информации. Фактически информация становится фактором, определяющим эффективность любой сферы деятельности. Поэтому обойтись без информационной системы, обрабатывающей данные, хранимые в базе данных (БД) невозможно. Для разработки информационной системы используется система управления базами данных (СУБД), которая обеспечивает определение, хранение и регламентирование доступа к данным. В настоящее время реляционные СУБД (РСУБД) стали практически промышленным стандартом [1]. В РСУБД данные представлены в виде связанных таблиц. Доказано, что любую структуру данных можно преобразовать в простую двумерную таблицу, над которой можно совершать операции, определенные в алгебре отношений (реляционной алгебре), и обрабатывать данные, хранящиеся в ней, с помощью универсального языка структурированных запросов SQL. Для работы выбран Microsoft Access. В первой (теоретической) части данной работы рассмотрены основные этапы разработки реляционных баз данных, особенности, создание таблиц, форм, отчетов и запросов в Microsoft Access [2].

Поставлена и выполнена задача по разработке базы данных «Ремонт», выполняющей следующие функции:

- Нахождение клиента в базе либо добавление нового;
- Регистрация приема аппаратуры на ремонт;
- Выдача клиенту квитанции о взятии аппаратуры на ремонт;
- Нахождение заказа клиента по номеру квитанции и ФИО;
- Распечатка сопутствующих ремонту документов;
- Регистрация выдачи аппаратуры клиенту;
- Выдача сопроводительного (гарантийного) документа.

Поставлена и выполнена задача о начале разработки и реализации темы дипломного проекта – базы данных «БДКомп», позволяющей вести учет всей деятельности и осуществлять документооборот фирмы «Инстал», занимающейся продажей и ремонтом компьютеров, комплектующих и оргтехники. На данный момент реализованы следующие функции:

- автоматическое внесение прихода товара из таблицы Excel;
- добавление новых клиентов, поставщиков, категорий товара;
- создание нового счета;
- регистрация нового счета (то есть списывание товара со склада и расчет прибыли);
- сохранение нового счета без регистрации (для возможного дальнейшего использования);
- открытие старого счета;
- редактирование старого счета;
- если счет не был зарегистрирован, то регистрация;
- возможность отмены регистрации счета в случае каких либо неожиданных ситуаций (например, не оказалось какого либо товара в наличие, брак, Замена и т.п.).

ЛИТЕРАТУРА

1. *Кренке Д.* Теория и практика построения баз данных. 8-е изд. СПб.: Питер, 2003. 800 с.
2. *Вейскас Дж.* Эффективная работа : Microsoft office Access 2003. СПб.: Питер, 2005. 1168 с.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЦЕНКИ ТЕХНИЧЕСКОГО СОСТОЯНИЯ ПРОМЫШЛЕННОГО ОБОРУДОВАНИЯ

***А.М. Гаськов, студент 5 курса ФВС**
ТУСУР, кафедра КСУП, г. Томск*

В докладе рассматриваются основные вопросы обработки данных полученных в результате измерений и конвертации их в Excel.

Задачи решаемые данным программным продуктом:

- систематизация полученных данных;
- расчет остаточного ресурса трубопроводов;
- создание отчета в Excel;

Программный продукт будет разрабатываться в СУБД MySQL и Delphi6. Недостатками немногих существующих аналогов в первую

очередь является цена, а так же некоторые нюансы неудовлетворяющие потребностям заказчика. СУБД MySQL обладает многими преимуществами. Некоторые из них приведены ниже.

Быстродействие. MySQL – достаточно быстродействующая СУБД. Разработчики склоняются к мнению, что СУБД MySQL является одной из самых быстрых баз данных из имеющихся на современном рынке. В этом можно удостовериться, посетив Web-узел <http://www.mysql.com/benchmark.html>. Эта страница позволяет делать сравнительную проверку производительности на Web-узле MySQL.

Простота использования. MySQL является быстрой и относительно простой в использовании СУБД, которую значительно проще установить и администрировать, чем многие большие системы.

Цена. СУБД MySQL распространяется бесплатно для домашнего использования.

Поддержка языка запросов. MySQL «понимает» команды языка SQL (Structured Query Language – структурированный язык запросов). Этот язык применяется во всех современных СУБД. MySQL также поддерживает интерфейс ODBC (Open Database Connectivity), протокол интерфейса с базами данных, разработанный компанией Microsoft.

Возможности. Сервер позволяет одновременно подключаться неограниченному количеству пользователей. Доступ к серверу СУБД MySQL можно осуществить в интерактивном режиме с помощью различных интерфейсов, позволяющих вводить запросы и просматривать полученные результаты: это программы клиенты, работающие с командной строкой, Web-браузеры или программы-клиенты, работающие в системе X Window. Кроме того, в наличии имеются программные интерфейсы для таких языков, как C, Perl, Java, PHP и Python. Таким образом, можно использовать как готовое клиентское программное обеспечение, так и создавать свое собственное.

Взаимодействие и безопасность. MySQL, предназначена для работы в сети и может быть доступна через Internet, таким образом, с данными можно работать в любой точке земного шара. Но при этом СУБД MySQL снабжена развитой системой защиты от несанкционированного доступа.

Переносимость. СУБД MySQL отлично работает как под управлением самых различных версий UNIX, так и под управлением систем, не использующих UNIX, таких как Windows и OS/2. СУБД MySQL работает как на домашних ПК, так и на мощных серверах.

Открытое распространение. Дистрибуция СУБД MySQL легко доступна. Для этого достаточно воспользоваться Web-браузером. Если вы не понимаете как что-либо работает, просмотрите исходный код. Если вам что-то в работе не нравится, можно внести коррективы.

Ключевой механизм BDE, обеспечивающий работу визуальных компонент баз данных, действует как интерфейс между нашим приложением и самой базой данных. BDE реализован в виде набора системных DLL файлов. Взаимодействие компонентных объектов с BDE никак не специфицирует конкретную базу данных и не зависит от реализации обмена информацией на нижнем уровне иерархии. Именно BDE обращается в свою очередь к драйверам, специфическим для базы данных указанного типа, возвращая нашему приложению запрошенные фактические данные. BDE играет роль, аналогичную контроллеру драйверов ODBC (Open Database Connectivity) производства фирмы Microsoft, изолируя приложения от нижнего уровня взаимодействия с базой данных и увеличивая общую производительность связи за счет использования кэш-памяти. Используя BDE, вы получаете доступ ко всем локальным стандартным базам данных нашего компьютера, к источникам данных ODBC и к SQL серверам баз данных в архитектуре сетевой связи клиент/сервер.

Унифицированная технология BDE применяется во всех продуктах производства корпорации Borland: Чтобы получить доступ к содержимому базы данных, приложению необходимо знать только идентификатор ее `pseeflONHMa(alias)`.

ДЕКОМПОЗИЦИЯ ЗАДАЧИ СИНТЕЗА РЕЧИ

И.В. Горбылев, студент 5 курса ФВС;

В.П. Коцубинский, к.т.н., доцент каф. КСУП

ТУСУР, кафедра КСУП, г. Томск, yazon@km.ru

Общие вопросы создания синтезаторов речи рассмотрены в работах [1, 2]. В данном докладе рассматриваются разложение (декомпозиция) задачи синтеза речи по правилам с точки зрения системного подхода.

Задачей модуля анализа текста, являющегося часть модуля обработки текста, является проведение синтаксического, семантического, пунктуационного и т.п. анализа текста. В результате имеем следующую схему данного модуля (рис. 1):

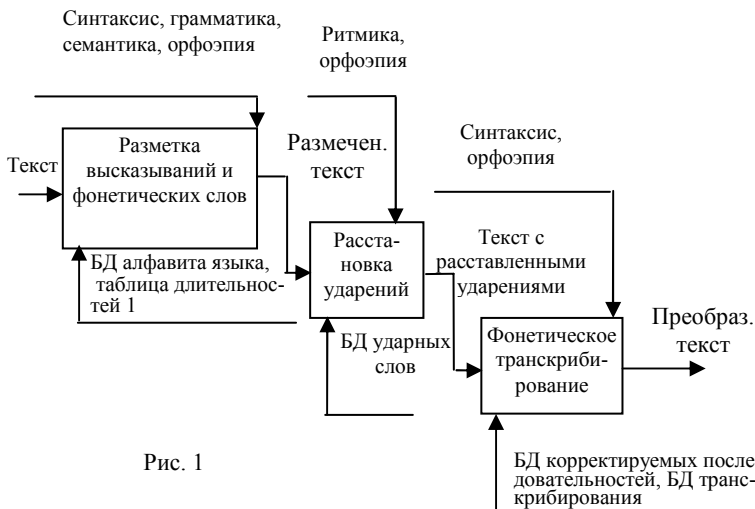


Рис. 1

Рассмотрим теперь непосредственно модуль синтеза речи. На данном этапе система, используя результаты операций, проведенных на предыдущих этапах другими модулями, преобразует текст в речевой сигнал (рис. 2).

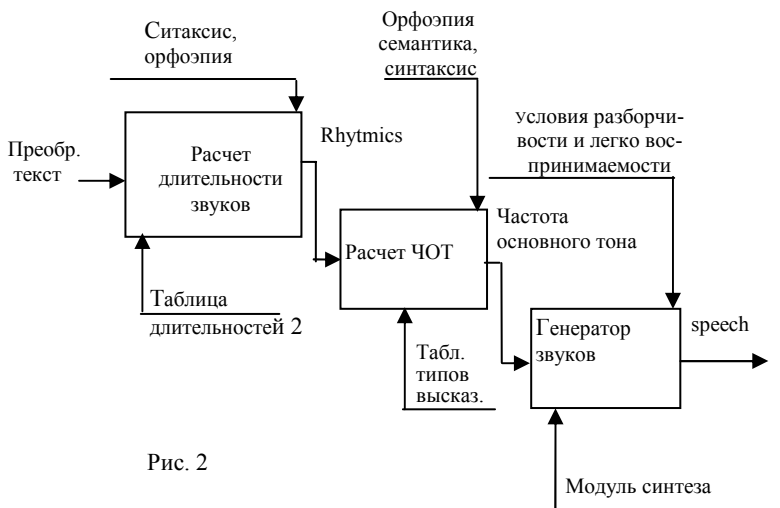


Рис. 2

На различных этапах синтеза речи (как этапах, связанных с анализом входного текста, так и непосредственно на этапе синтеза [1, 2]) модулям требуются базы правил и данных.

Задача ресинтеза речи в настоящее время решена [2]. Необходимо учитывать, что ресинтез основан на решении обратной задачи. Эти решения, как правило, неоднозначны. Поэтому для получения однозначного решения требуется введения дополнительной информации в виде опорных значений, например, по сечениям речеобразующего тракта.

Генерация речевого сигнала по правилам должна быть основана на общих математических соотношениях таким образом, чтобы за счет установки определенных значений параметров получить сигнал с требуемыми характеристиками.

Необходимо учитывать, что при построении моделей речеобразующего тракта даже синтез вокализованных гласных звуков требует анализа обратных связей на уровне голосовых складок [4] это приводит к необходимости решения сложной задачи по определению устойчивости систем в целом.

В работе [4] представлены зоны устойчивых режимов работы модели образования звучной нормальной речи [5]. Режимы, в которых возможны запредельное смыкание голосовых складок, и размыкание, приводят к судорогам в гортани [5] и, возможно, трахеи и мышц грудной клетки, что в свою очередь может привести к резкому возрастанию избыточного давления в легких и, возможно, к уменьшению площади сечения трахеи, т.е. ее емкости. Это переведет устойчивый режим голосообразования в неустойчивый, т.е. к срыву процесса речеобразования. В этой же работе приводятся резонансные характеристики трахеи. Можно предположить, что при нормальном речеобразовании происходит также и управление сечениями и длиной трахеи в зависимости от произносимого звука.

Обратная задача имеет не однозначное решение, это подтверждается необходимостью получить от диктора большое количество параметров перед решением уравнения Новье-Стокса [6], а затем требуемыми для этого вычислительными мощностями. Можно предположить, что не учет влияние обратных связей [7] и устойчивости системы речеобразования делает невозможным создания адекватных синтезаторов речи не зависящих от конкретных дикторов.

ЛИТЕРАТУРА

1. Лобанов Б.М. Микроволновой синтез речи по тексту // Сб. научных трудов «Анализ и синтез речи» / Под ред. Лобанова Б.М. Минск: АН БССР. Ин-т техн. кибернетики. 1991. 86 с. с. 57–73.
2. Леонов А.С., Макаров И.С., Сорокин В.Н. Речевые обратные задачи и ресинтез // XVI сессия РАО. Москва. 10–14 ноября, 2005. Т. 3. с. 28–34
3. Klatt, D. H. Review of Text-To-Speech Conversion for English // J. Acoustic Society of America (JASA). Vol. 82. N. 3. 1987. pp. 737–793.

4. Бондаренко В.П., Коцубинский В.П., Мещераков Р.В. Модель образования звучной речи // XVI сессия РАО. Москва, 10–14 ноября, 2005. Т. 3. с. 80–83.
5. Бондаренко В.П., Коцубинский В.П., Мещераков Р.В. Модель голосового заикания // XVI сессия РАО. Москва, 10–14 ноября, 2005. Т. 3. с. 14–22.
6. Titze I., Story B., Hoffman E. Vocal tract area functions for an adult female speaker based on volumetric imaging // J. Acoust. Soc. Am. 104 (1), 1998, pp. 471–487.
7. Складов, О.П. Хаос и ритм в нормальной речи и при заикании. СПб. 2002. с. 52.

СИСТЕМНЫЙ ПОДХОД К ЗАДАЧЕ СИНТЕЗА РЕЧИ

И.В. Горбылев, студент 5 курса ФВС;

В.П. Коцубинский, к.т.н., доцент каф. КСУП

ТУСУР, кафедра КСУП, г. Томск, yazon@km.ru

В настоящее время на многих научных учреждениях и частных компаниях решается проблема создания систем распознавания и синтеза речи. Эти две задачи являются обратными по отношению друг к другу. Зачастую результаты, достигнутые в одной из областей, могут быть использованы в другой. Синтез речи по правилам до сих пор не решенная задача.

В данной работе рассмотрена общая схема синтезатора речи, проведен анализ необходимой для функционирования системы информации и акцентируется внимание на синтез речи по правилам.

Для решения общей проблемы синтеза речи по тексту необходимо решить целые классы частных проблем, таких, как создание системы автоматического морфологического, системы синтаксического анализа.

Современные системы синтеза речи, по нашему мнению, обладают рядом недостатков:

- неестественность, безэмоциональность речи.
- при компилятивном синтезе речи из отдельных речевых единиц (полуслогов и т.п.) выходной речевой сигнал имеет низкое качество, на границе слияния элементов возникают искажения.
- как правило синтезаторы строятся по какому-либо одному принципу (ограниченный, либо неограниченный словарь; параметрическое, либо волновой метод представления речевой волны), вследствие чего имеет строго ограниченную область применения.

С целью устранения существующих недостатков была предложена несколько видоизмененная модель системы синтеза речи:

- предлагается на вход синтезатора подавать не только сам текст, подлежащий озвучиванию, но и некоторый поток служебной информации, подготавливаемый специально для данного текста.

– поскольку проектирование синтезаторов в программном виде представляет довольно широкие возможности по улучшению гибкости программ, предлагается предусмотреть в программном пакете возможность изменения режима работы синтезатора (например, выбор между синтезом речи при помощи ограниченного словаря, либо компилятивным синтезом речи) – для расширения области применения одного и того же программного пакета.

– далее, поскольку компилятивные синтезаторы нередко страдают тем, что получаемая на выходе звуковая волна обладает низким качеством, предлагается особое внимание уделить модулю «дообработки» речи, с последующим переходом к синтезу речи по правилам.

Исходя из изложенных выше принципов, по нашему мнению, структура синтезатора речи меняется (по отношению к работам [1, 2]) и становится следующей (рис. 1):

Ограничения: обработка текста и служебной информации должна проводиться строго параллельно, преобразование обработанного текста в речь и финальная обработка звука должны идти с достаточно большой скоростью

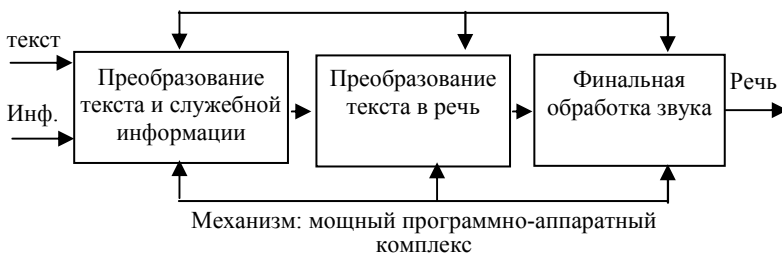


Рис. 1

Если же более детально рассмотреть модуль обработки текста и преобразования его в поток информации. Используем для анализа структур данных принципы положенные в основу программы ERwin. Будучи CASE-средством данная программа позволяет произвести декомпозицию дерева целей и синхронизировать получаемые модели на различных этапах разработки системы. Все это необходимо для создания «понятного» модуля синтеза звуковой волны, что является самой сложной задачей для синтеза речи по правилам. Достаточно вспомнить модули, возникающие на каждом этапе для доработки информации [1, 2]. Учитывая, это получим, следующую схему (рис. 2).

На этапе преобразования текстового потока в выходной текстовый поток, понятный синтезатору, происходит анализ введенной служебной информации. Этот анализ необходим для того, чтобы была возможность учесть на этапе синтеза речи такие параметры, как интонацион-

ные особенности текста, параметры диктора и другую информацию, которая не содержится непосредственно в печатном тексте.

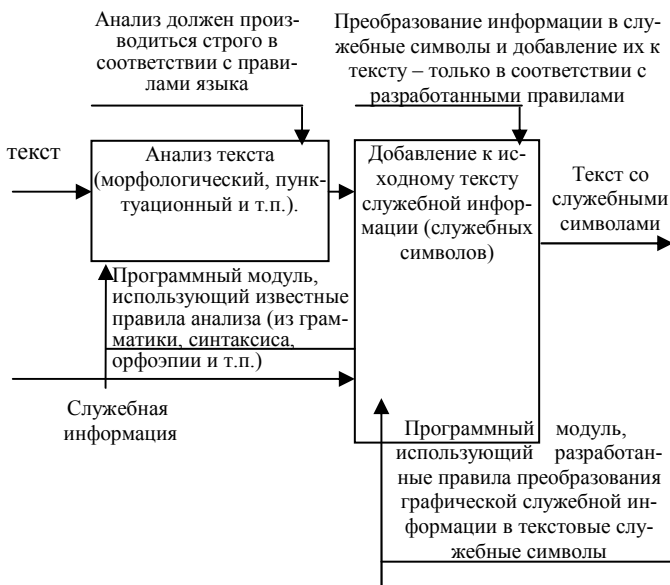


Рис. 2

Предлагается следующий способ представления служебной информации: в интерфейсной форме ввода (или ее аналоге для других устройств, отличных от монитора компьютера) вводить наряду с текстом также служебную информацию в удобной для пользователя форме (графиков, цвета и т.п.), а затем, внутри синтезатора производить преобразование полученной информации в служебные символы в соответствии с правилами преобразования.

Предложенные в данной работе методологический подход к созданию синтезатора речи по правилам, потребует модификаций правила преобразования печатного текста в управление артикуляцией.

ЛИТЕРАТУРА

1. Лобанов Б.М. Микроволновой синтез речи по тексту // Сб. научных трудов «Анализ и синтез речи» / Под ред. Лобанова Б.М. Минск: АН БССР. Ин-т техн. Кибернетики. 1991. 57–73.
2. Klatt D.H., Review of Text-To-Speech Conversion for English // J. Acoustic Society of America (JASA). Vol. 82. N 3. 1987. pp. 737–793.

РАЗРАБОТКА ИНТЕРНЕТ-МАГАЗИНА ПО ПРОДАЖЕ ОТДЕЛОЧНЫХ МАТЕРИАЛОВ

Е.В. Горев, студент 5 курса ФВС;

Т.И. Орлова; Е.Н. Рыбалка, ст. преподав. каф. КСУП

ТУСУР, кафедра КСУП, г.Томск

Совокупный оборот электронной торговли в России составил в 2005 г. более \$1 млрд. долларов. Темп роста электронной торговли в России в 2005 г. составил 38–40%.

Такие данные приводит Национальная ассоциация участников электронной торговли (НАУЭТ). Объем электронной торговли в розничном сегменте вырос в 2005 г. до \$662 млн., а в оптовом сегменте до \$442 млн.

В то же время объем розничного товарооборота через Интернет в России пока составляет менее 1% от общего розничного товарооборота. Для сравнения: в США эта цифра составляет в настоящее время около 15%.

Средний дневной товарооборот (выручка) интернет-магазина в России, по данным НАУЭТ и CNews Analytics составляет \$5,8 тыс. и пока еще отстает аналогичного показателя для предприятий розничной торговли, а вот средняя стоимость одной покупки уже сопоставимы по значениям с таким показателем для традиционных магазинов. Даже если поставить под сомнение эти цифры, то все равно видна тенденция увеличения прибыли за счет продаж через Интернет. Учитывая все вышесказанное, присутствие Интернет-магазина у фирмы в будущем будет неотъемлемой части конкурентоспособности предприятия.

Руководством компании ЗАО «Том-Дом» было принято решение разработать Интернет-магазин, который помимо своего прямого назначения представлял бы компанию в сети Интернет.

Мне было предложено провести исследование типичной схемы работы Интернет-магазина. Коротко о работе Интернет-магазина можно сказать следующее. Пользователь сети Интернет, посетив сайт, имеет возможность просмотреть каталог товаров, выбирая нужные. После того как он определился с заказом, ему предлагается заполнить стандартный бланк заказа. После чего бланк отсылается на сервер и ожидает обработки. Через какое-то время операторы Интернет-магазина связываются с покупателем и подтверждают сделку, оговорив заранее способ доставки товара.

Мне было предложено самостоятельно составить техническое задание Интернет-магазину. После корректировки некоторых пунктов руководителем и рекомендации конкретных программных средств я приступил к разработке концептуальной модели данных [1].

Предложенными программными средствами являются Java Server Page (JSP) и Extensible Markup Language (XML). XML был задуман как гибкий и в то же время формальный метаязык для использования в Интернете. XML метаязык (metalanguage) – это язык, предназначенный для описания других языков. В создаваемом проекте он нужен для обмена данными с сервером, для заполнения базы данных (БД). Кроме того сами данные можно хранить в формате XML документов и работать с ними также как с БД [2].

Технология Java Server Pages (JSP) является составной частью единой технологии создания бизнес-приложений J2EE. JSP – это альтернативная методика разработки приложений, динамически генерирующих ответ на те или иные запросы клиента. Прежде чем JSP документ будет использован, специальная процедура преобразует его в соответствующий сервлет. В свою очередь, сервлет, как правило, пишется на языке Java и реализует определенный интерфейс. Далее, сервлет также не является самостоятельным приложением и функционирует, только будучи помещен в соответствующий web-контейнер [3]. Web-контейнер обеспечивает обмен данными между сервлетом и клиентами, берет на себя выполнение таких функций, как создание программной среды для функционирующего сервлета, идентификацию и авторизацию клиентов, организацию сессии для каждого из них.

ЛИТЕРАТУРА

1. Кренке Д. Теория и практика построения баз данных. 8-е изд. СПб.: Питер, 2003. 800 с.
2. Бен Чанг, Марк Скардина, Стефан Киритцов. Oracle9i XML Handbook. М.: Издательство «Лори». 2003.
3. Брэдли Б. Браун. Oracle 8i. Создание Web-приложений. М.: Издательство «Лори». 2001.

ПРОЕКТ «ЭЛЕКТРОННАЯ КАФЕДРА»

О.А. Гриц, студент 5 курса ФВС

ТУСУР, кафедра КСУП, г.Томск, kcupr@sapr.fet.tusur.ru

Исходными документами «Электронной кафедры» являются учебный план, определяемый им учебно-производственный план и список студентов. Учебно-производственный план содержит всю необходимую информацию о преподаваемых дисциплинах, которые делятся на обязательные и элективные (курсы по выбору).

Необходимость создания программного продукта обусловлена тем, что в связи с постоянным изменением учебного плана, изменением ко-

эффицентом расчета или изменением количества студентов в группе меняется нагрузка преподавателя и приходится рассчитывать величину нагрузки вручную. А это довольно трудоемкий процесс, требующий много времени. Расчет нагрузки преподавателя не для конкретной группы или подгруппы из базы данных, а для нескольких студентов тоже требовал больших временных затрат.

Поведя анализ некоторых автоматизированных систем формирования и обработки документации планирования учебного процесса: Автоматизация учебного процесса в системе дистанционного образования средствами «Lotus Notes» «Электронная кафедра», Автоматизированная система обработки информации Астраханского государственного технического университета. Было выяснено, что существующие системы не подходят в связи со следующими недостатками:

- расчетные коэффициенты могут изменяться. В реализованных системах эта возможность не была учтена.
- рассмотренные системы очень громоздки и содержат слишком много ненужной информации;
- для Автоматизированной системы обработки информации Астраханского государственного технического университета требуется Oracle 7.3.

В ходе работы были выведены формулы для расчета нагрузки преподавателей. Был обоснован выбор программного обеспечения для реализации системы: MySQL 3.23. С учетом особенностей, которого была создана логическая модель системы и создана главная экранная форма.

В ходе работы возникли следующие сложности:

- ненормализованность базы данных;
- реализация возможности изменения коэффициентов нагрузки;
- расчет нагрузки преподавателя не для конкретной группы или подгруппы из базы данных, а для нескольких студентов.

После реализации данная система должна:

- выполнять расчет нагрузки преподавателя;
- производить расчет нагрузки по обеспечивающим кафедрам;
- выполнять расчет нагрузки преподавателя по внебюджетным студентам;
- рассчитывать сводную нагрузку по кафедре;
- производить модификацию расчетных коэффициентов.

Все эти особенности учтены при создании логической модели проектируемой базы данных. Созданный программный продукт позволил существенно упростить работу, связанную с распределением нагрузки по кафедре КСУП ТУСУР.

ОПТИМИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ ПРОДАЖ

С.А. Губина, ТОО «Tandem TVS», Алма-Аты,

Е.Н. Рыбалка, ст. препод. каф. КСУП

ТУСУР, кафедра КСУП, г.Томск, ewgeny@inbox.ru

Повышение прибыли компании в условиях жесткой конкурентной борьбы и увеличения объемов продаваемого товара можно осуществить путем описания процессов продажи товара для выявления недостатков и узких мест процессов продажи и оптимизации существующей работы.

В процессе оптимизации рассматривались бизнес-процессы продажи электронного оборудования в компании ТОО «Tandem TVS». Сложность реализации предлагаемого оборудования заключается в наличии конкурентоспособных торговых марок оборудования с более низкой себестоимостью, а также насыщенностью рынка сбыта в категории предлагаемого товара.

Для продвижения торговой марки оборудования и увеличения объемов продукции были рассмотрены и описаны существующие процессы продаж.

На основе описания процессов продажи и полученных диаграмм был произведен анализ и выявлены следующие недостатки процесса:

- высокая цена реализации оборудования;
- не выгодные условия поставки для клиента;
- длительный срок поставки оборудования, около 6 недель;
- 100% предоплата оборудования;
- ограничение на размещаемый заказ, минимальная сумма заказа;
- отсутствие закупки оборудования под склад, работа только под заказ;
- отсутствие у поставщика сервисного – центра по предлагаемому оборудованию.

Для устранения существующих недостатков было предложено:

- снижение цены на продукцию;
- организация «кредитной линии» для заказчиков;
- устранения ограничения на размещаемый заказ методом соединения нескольких заказов.
- поставка товара на различных условиях в соответствии с Incoterms 2000.

В итоге оптимизации бизнес процессов продаж увеличилось количество заказчиков и объемы продажи оборудования.

В результате реорганизации процессов продаж появилась возможность изучения спроса конечного покупателя на предлагаемую линейку

оборудования для организации процессов закупки оборудования под склад. При закупке товаров под склад существует возможность сокращения сроков поставки оборудования, что в свою очередь увеличивает рынок сбыта продукции и объем продаж. Также при значительном увеличении объемов продаж, поставщик имеет возможность снижения себестоимости оборудования от производителя и организации собственного сервис-центра.

ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА КОМПЬЮТЕРОВ И ОРГТЕХНИКИ НА ПРЕДПРИЯТИИ

Г.М. Гусельников, студент 5-го курса ФВС

ТУСУР, кафедра КСУП, г.Томск

Предметная область. Задача учета компьютерной техники важна по разным причинам:

Во-первых, учет необходим с точки зрения бухгалтерии. И нужно всегда быть готовым к задаче инвентаризации, как лицу, материально ответственному за технику.

Во-вторых, хорошая программа для учета может наглядно представить картину наличия и типов оборудования, имеющегося на рабочих местах. Всегда можно оперативно узнать сроки гарантии какого-то вышедшего из строя устройства и где оно покупалось. Задача планирования и перераспределения техники становится гораздо проще.

Во многом может помочь возможность проследить историю перемещения какого-то устройства по рабочим местам, историю работ по его техническому обслуживанию (ремонт и профилактика), при этом, автоматически запоминается кто вводил/изменял в базу данных эту информацию. Наличие всех этих данных позволяет строить самые различные отчеты (отчет по рабочему месту, паспорт на устройство, перечень всех устройств и прочее).

Особенно актуальной задача учета становится при большом количестве техники в организации. Вследствие того, что данный программный продукт создается впервые, и никакой документации на него не существует, мне было предложено самостоятельно разработать техническое задание (ТЗ) на новый продукт.

Постановка задачи. Необходимо разработать новую информационную систему, с помощью которой можно было бы отследить перемещения компьютерного оборудования по рабочим местам, а также историю работ по его техническому обслуживанию.

В новом программном продукте необходимо предусмотреть:

- возможность удаленного доступа пользователей к системе через сети Intranet/Internet;
- ограничения доступа к информации согласно должностным инструкциям сотрудников;
- обеспечение удобного интуитивно понятного интерфейса пользователя, который позволяют создать современные инструменты разработки Internet/Intranet-приложений;

Необходимость создания удаленного доступа к системе пользователей вызвана тем, что предприятие имеет достаточно большое количество филиалов, которые территориально разнесены как по территории города Томска, так и Томской области.

ИС должна обеспечить выполнение следующих основных функций:

- ведение базы данных по имеющемуся оборудованию;
- полуавтоматическое заполнение базы данных, т.е. импорт данных из программы анализатора оборудования AIDA или ASTRA;
- возможность проследить перемещения компьютерного оборудования по рабочим местам, а также историю работ по его техническому обслуживанию;
- возможность узнать сроки гарантии вышедшего из строя устройства и где оно покупалось;
- поиск устройств или групп устройств по определенному критерию.

Средства разработки. Разработка программной модели системы производится с помощью клиент-серверной технологии ASP (активные серверные страницы). ASP – это мощная технология, разработанная фирмой Microsoft, позволяющая легко разрабатывать сетевые приложения. ASP работает на любой платформе фирмы Microsoft® и Internet Information Server. ASP – это не язык программирования, это внутренняя технология, позволяющая подключать программы к Web-страницам. Основа успеха ASP – простой скриптовый язык (Visual Basic Script или Java Script).

Активные серверные страницы обеспечивают доступ к данным посредством открытого подключения к базам данных (Open Database Connectivity, ODBC).

ODBC представляет собой не зависящую от типа баз данных технологию доступа к данным, и эта независимость особенно полезна в Web-приложениях и облегчает разработку Web-страниц, позволяя прибегать для взаимодействия с базами данных к синтаксису стандартного структурного языка запросов SQL.

Концептуальная модель данных разработана по методологии IDEF1X. Данная методология является способом разработки реляционных баз данных. База данных информационной системы реализована с

помощью СУБД Access. СУБД Access на сегодняшний момент является недорогой и наиболее распространенной СУБД, входящей в пакет офисных программ Microsoft Office. На большинстве офисных компьютеров имеется Office, поэтому нет необходимости приобретать какие-либо другие СУБД.

РАЗРАБОТКА WEB – САЙТА ТУРИСТИЧЕСКОГО АГЕНТСТВА

Н.Н. Даниэльс, студента 5 курса ФВС;

Е.Н. Рыбалка, ст.преподав. каф. КСУП

ТУСУР, кафедра КСУП, г. Томск, daniels@mail2000.ru

Общеизвестен факт, что эффективность прямой рекламы туристических услуг в средствах массовой информации снижается. Поиск альтернативных форм рекламы приводит туристические фирмы к мысли о необходимости собственного присутствия во всемирной компьютерной сети Интернет. Автоматизация и широкое применение Web-технологий становятся одной из актуальнейших задач на сегодня в отрасли туризма.

Работники Турагентства связаны с накоплением большого количества информации о клиентах, турах, отелях и т.п. Чаще всего информация храниться на бумажных носителях. При этом трудно осуществить быстрый отбор нужных данных при оформлении заказа, получении данных о клиенте, туре, рейсах и т.п. Таким образом, автоматизация процесса работы турагентства является нужным и перспективным процессом, разработка АРМ с реализацией возможности выхода в Интернет является актуальной и востребованной задачей в данной отрасли.

Целью данной работы является разработка составных частей АРМ туристического агентства: База Данных, WEB – сайт.

На первом этапе разработки был произведен анализ предметной области. Для описания логики взаимосвязей сущностей использовалась SADT-методология IDEF1x [1]. При этом была разработана следующая структура базы данных (рис. 1).

После разработки и создания базы данных перешли ко второй части работы, а именно реализации WEB – сайта на основе предъявляемых современных требований: легкость доменного имени, запоминаемость фирменного стиля, информативность и интерактивность сайта, реклама торговой марки в сети, увлекательное и полное содержание сайта, чтобы полностью удовлетворить интерес потенциального клиента; быстрая загрузка страниц; художественное оформление, для приятного времяпрепровождения за страницами данного WEB-сайта (рис. 2) [2–6].

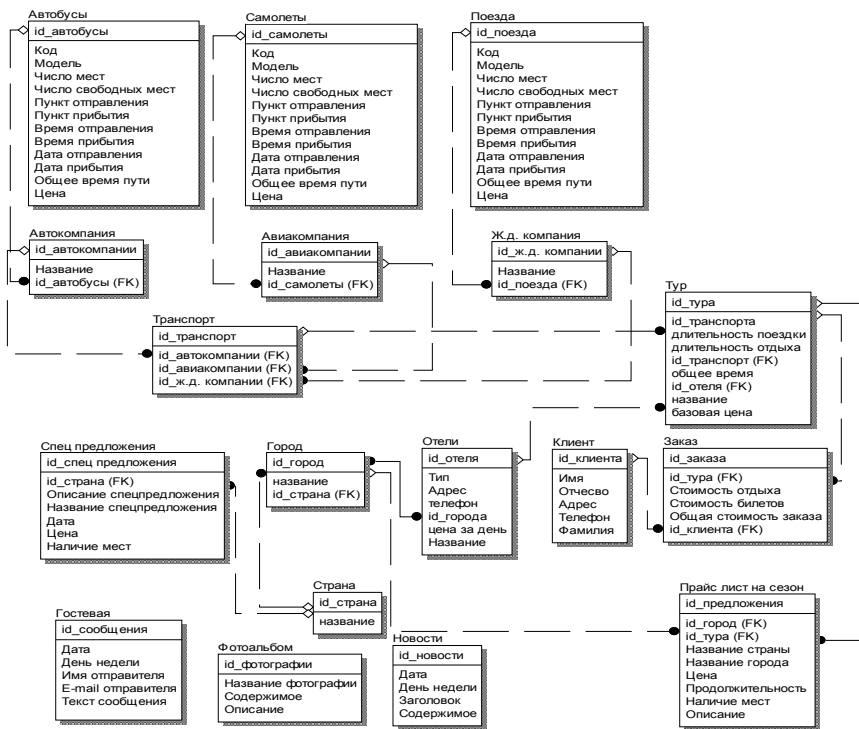


Рис. 1. Логическая модель Базы Данных



Рис. 2. Страница WEB – сайта «РИО – медиа»

Таким образом, была разработана структура Web-сайта, создана база данных для хранения информации, реализованы возможности администрирования сайта, просмотра фотоальбома, расписания авиа- и железнодорожного транспорта, записи и просмотра новостей, ознакомления с новыми специальными предложениями и т.д. Сайт туристического агентства «РИО – медиа» предоставляет полноценную информацию о данном агентстве, а так же позволяет производить редактирование данных. Поддержка данного сайта осуществляется администратором.

ЛИТЕРАТУРА

1. *Federal Information Processing Standards Publication 184. Announcing the Standard for INTEGRATION DEFINITION FOR INFORMATION MODELING (IDEFIX).*
2. *Белунцов В.* Новейший самоучитель по разработке web-страниц. М.: ДЕССКОМ. 2000. 448 с.
3. *Шафран Э.* Создание Web-страниц: самоучитель. СПб.: Питер, 2000. 320 с.
4. *Полянский А.* Хитрости, трюки и секреты создания Web-страниц на базе языка PHP 4.0. М.: «Познавательная книга плюс», 2000. 240 с.
5. *Ковязин А.Н., Востриков С.М.* Мир InterBase. М.: ДЕССКОМ, 2002. 540 с.
6. *Мазуркевич А.М., Еловой Д. С.* PHP – настольная книга программиста. Мн.: Новое знание, 2003. 480с.

УПРАВЛЕНИЕ СЧЕТАМИ ПРОЦЕССИНГОВОЙ КОМПАНИИ

А.Я. Клименко, д.т.н., профессор каф. КСУП;

Ж.Ц. Дашиева, 5 курс ФВС

г. Томск, кафедра КСУП, ТУСУР, т. 913-810-23-18

Особенность бухгалтерских операций процессинговой компании заключается в том, что системе приходится обрабатывать тысячи транзакций, причем обрабатывать необходимо как можно быстрее. Необходимость непрерывной обработки поступающих транзакций и оперативности требует интегрируемости системы бухгалтерского учета в расчетную систему организации. Актуальность разрабатываемой системы определяется тем, что существующие на данный момент автоматизированные системы бухгалтерского учета невозможно интегрировать в другие системы, поскольку обычные автоматизированные бухгалтерские системы слишком самостоятельны. Поэтому перед руководством организации встает вопрос о разработке интегрируемой автоматизированной системы бухгалтерского учета, учитывающей особенности работы организации.

В результате системного анализа предметной области были определены сущности понятия счетов и операций над ними, также выявлены особенности бухгалтерских операций процессинговой компании.

Задача выявления требований к системе очень сложна. И быстро ее решить невозможно. Для конечного формирования требований к разрабатываемой системе были спроектированы четыре модели системы:

- функциональная модель;
- модель прецедентов;
- диаграммы классов;
- логическая модель структуры базы данных системы управления счетами процессинговой компании.

При проектировании функциональной модели были сформированы основные требования к функциональности системы. Далее, при создании диаграмм прецедентов выявлены варианты использования системы для каждого из пользователей (главный бухгалтер, бухгалтер, сотрудник операционного центра, покупатель, продавец). Модель вариантов использования облекает пользовательские требования в законченную форму. Планирование фазы построения осуществляется с учетом реализации на каждой итерации нескольких вариантов использования.

Проектирование диаграмм классов отображает структуру разрабатываемой системы. Диаграммы классов показывают статическую структуру понятий, типов и классов. Понятия отражают представления пользователей о реальном мире; типы отражают интерфейсы компонентов программного обеспечения; классы отражают реализацию компонентов программного обеспечения.

В ERWin была разработана логическая модель структуры базы данных системы. На данном этапе были определены сущности модели, их атрибуты и связи между ними.

Реализация подсистем управления счетами процессинговой компании подразумевает выполнение следующих пунктов:

- выбор инструментальной среды разработки;
- формы документов и визуализации;
- архитектура модулей;
- тестирование подсистем.

Выбрана среда разработки программного продукта (Visual FoxPro 8.0), поскольку данная среда дает легкий доступ к данным, удобный интерфейс пользователя и формирует отчеты. Поскольку в базе данных разрабатываемой системы будет содержаться конфиденциальная информация, к организации доступа к данным, хранению и возможности восстановления информации уделено особое внимание.

Заключение. Большое внимание при разработке системы управления счетами процессинговой компании было уделено моделированию системы. Для создания программных приложений реалистического масштаба необходимо заниматься их моделированием с помощью спе-

циальных инструментов. Инструменты моделирования позволили интерактивно просматривать и редактировать модели, быстро находить в них нужную информацию, лучше понимать создаваемую систему. Результатом работы является создание системы управления счетами процессинговой компании, самостоятельно проводящая проводки по счетам, формирующая отчеты по проделанным операциям. Система интегрируется в расчетную систему компании.

ЛИТЕРАТУРА

1. *Бабаев Ю.А.* Бухгалтерский учет: Учебник. М.: Юнити-ДАНА, 2001. 361 с.
2. *Баженова И.Ю.* Visual FoxPro 6.0. М.: Диалог-МИФИ, 2000. 416 с.
3. *Якобсон А., Буч Г., Рамбо Дж.* Унифицированный процесс разработки программного обеспечения. СПб.: Питер, 2002. 496 с.
4. *Рамбо Дж., Якобсон А., Буч Г.* UML: Специальный справочник. СПб.: Питер, 2002. 656 с.
5. *Скотт К.* UML: Основные концепции.: Пер.с англ. М.: Издательский дом «Вильямс», 2002. 144 с.

АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО ВРАЧА АНЕСТЕЗИОЛОГА-РЕАНИМАТОЛОГА

*А.В. Долин, студент 5 курса ФВС; С.В. Авдеев, д.м.н., руководитель
РАО НИИ онкологии ТНЦ СО РАМН;*

*М.И. Андреев, к.т.н., зам. зав. филиалом каф. КСУП в ИОА СО РАН
ТУСУР, кафедра КСУП, г. Томск, serg_avdeev@mail.ru,
mlnlmax@mail.ru, ami@nm.ru*

Задача накопления, обработки и распространения (обмена) информации стояла перед человечеством на всех этапах его развития. В течение долгого времени основными инструментами для ее решения были мозг, язык и слух человека.

Положение в корне изменилось с появлением электронных вычислительных машин (ЭВМ).

Принципиально новый шаг был совершен, когда от применения ЭВМ для решения отдельных задач перешли к их использованию для комплексной автоматизации тех или иных законченных участков деятельности человека по переработке информации.

Решающее значение для эффективности систем подобного рода имеет то обстоятельство, что они опираются на автоматизированные информационные базы. Это означает, что в памяти ЭВМ постоянно сохраняется информация, нужная для решения тех задач, на которые рассчитана система. Она и составляет содержимое информационной базы соответствующей системы.

Хранение информации в памяти ЭВМ придает этой информации принципиально новое качество динамичности, т.е. способности к быстрой перестройке и непосредственному ее использованию в решаемых на ЭВМ задачах.

При переходе от автоматизации отдельных процессов предметной области к созданию автоматизированных информационных систем требуется не только взаимоувязка приложений, но и качественно новый подход к организации данных. Этот подход состоит в использовании единого хранилища – базы данных.

С переходом к концепции БД, данные становятся неким общим ресурсом, целостность которого необходимо защитить от разрушений при сбоях оборудования, при некорректных обновлениях, от НСД и т.п.

С целью обеспечения возможности взаимодействия человека с ЭВМ в интерактивном режиме появляется необходимость реализовать в рамках АСУ так называемое АРМ – автоматизированное рабочее место.

Преимущества такой автоматизации в медицинском учреждении очевидны:

- уменьшается время регистрации пациента, следовательно, увеличивается общая пропускная способность учреждения;
- заполнение форм может происходить с использованием настраиваемых шаблонов и справочников, что значительно сокращает время заполнения карты;
- возможность быстрого поиска необходимой информации за счет адресного доступа к ней;
- отпадает необходимость в работе с множеством различных бумажных бланков, карт, выписок и т.п.;
- возможность проанализировать необходимые данные и представить их в виде отчетов или графиков;
- настраиваемый доступ к информации;

Разрабатываемое автоматизированное рабочее место (АРМ), позволяющее организовать ввод, хранение и обработку информации о пациентах НИИ онкологии ТНЦ СО РАМН, должно удовлетворять следующим требованиям:

- возможность формально описать историю болезни в виде привычной для медиков амбулаторной карты;
- возможность описать функциональное состояние пациента, динамику изменения наблюдаемых параметров;
- получение статистических отчетов по основным направлениям деятельности;
- дружелюбный интерфейс пользователя.

Эти задачи можно осуществить при помощи создания единого хранилища – базы данных и использования средств СУБД.

На сегодняшний день известно более двух десятков форматов данных СУБД, однако наиболее популярными, исходя из числа проданных копий, следует признать dBase, Paradox, Interbase, FoxPro и Access. В качестве формата базы данных для разрабатываемой системы был выбран популярный формат компании Microsoft – Access. К преимуществам данного формата можно отнести поставку драйвера Microsoft Jet 4.0 OLE DB Provider в стандартной комплектации пакета Microsoft Office. Ядро Jet может рассматриваться как диспетчер данных, на основе которого строятся СУБД, такие как Microsoft Office. Используя технологию OLE, Access может взаимодействовать с другими продуктами программного пакета Microsoft Office.

В качестве среды реализации был выбран язык визуального программирования Delphi, предоставляющий необходимые ресурсы для создания приложения, необходимого для работы с базой данных.

Delphi – язык и среда программирования, относящаяся к классу RAD– (Rapid Application Development – «Средство быстрой разработки приложений») средств CASE -технологии. Delphi сделала разработку мощных приложений Windows быстрым процессом. Приложения Windows, для создания которых требовалось большое количество человеческих усилий например в C++, теперь могут быть написаны одним человеком, использующим Delphi. Выгоды от проектирования APM в среде Windows с помощью Delphi:

- устраняется необходимость в повторном вводе данных;
- обеспечивается согласованность проекта и его реализации;
- увеличивается производительность разработки и переносимость программ.

В ходе преддипломной практики были изучены основные понятия СУБД, ее назначение, требования к программному обеспечению и используемым языкам.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПТИЧЕСКОГО КАНАЛА ЛИДАРА

Д.С. Елистратов студент, 5 курса ФВС;

М.И. Андреев, к.т.н., с.н.с., доцент

Филиал каф. КСУП в ИОА СО РАН, г. Томск, e-mail: Super@sibmail.com

В [1, 2] математическая модель оптического приемо-передающего канала лидара не учитывают целый ряд его конструктивных особенностей, что вполне обоснованно для решаемых там задач.

При автоматизации процесса юстировки лидара [3] возникает задача определения допустимых угловых отклонений лазерного луча, при

которых не нарушаются требуемые условия функционирования лидара, например, исключение возможной засветки фотоприемника сигналом ближней зоны в процессе юстировки.

Для решения этой задачи требуется математическая модель оптического приемо-передающего канала лидара, учитывающая как можно больше конструктивных факторов, с целью определения их взаимосвязи с областью допустимых угловых отклонений лазерного луча.

На основе геометрических соотношений [4,5,6] разработана математическая модель оптического канала лидара, связывающая в единую систему такие конструктивные факторы как: γ – угол расходимости; α – угол наклона поворотного плоского зеркала в плоскости XOZ ; d – диаметр пучка лазерного излучения в плоскости XOY , проходящий через точку A , общую с плоскостью поворотного зеркала; d_{ni} – диаметр пучка на высоте H_i с учетом γ ; b – расстояние между оптическими осями передающей и принимающей оптическими системами лазера; D – диаметр приемного зеркала; F – фокус приемного зеркала; D_6 – диаметр бленды; H_6 – высота бленды; $H_{\min}$ и $H_{\max}$ – максимальная и минимальная высота зондирования соответственно; $\theta_{\min}$ и $\theta_{\max}$ – максимальный и минимальный угол перехвата излучения отраженного от i -го слоя атмосферы находящиеся на высоте $H_{\min}$ и $H_{\max}$ соответственно.

Разработанная математическая модель оптического канала лидара может быть применена для создания программного продукта, который, в свою очередь, может быть эффективно использован при автоматизированной юстировке вновь строящихся и модернизирующихся лидарных станций наземного базирования.

ЛИТЕРАТУРА

1. Зуев В.В., Ельников А.В., Бурлаков В.Д. Лазерное зондирование средней атмосферы / Под общей ред. чл.-кор. РАН В.В. Зуева. Томск: ООО Изд-во «РАС-КО», 2002. 352с.
2. Межерис. Лазерное дистанционное зондирование / Пер. с англ. М.: Мир, 1987. 550 с.
3. Тышкевич А.В., Андреев М.И. Модернизация юстировочного узла аэрозольного лидара Сибирской Лидарной Станции. // Научная сессия ТУСУР 2005: Материалы Всероссийской научно-технической конференции, г. Томск, 26–28 апреля 2005 г. Томск: Издательство ТУСУРа, 2005. С/ 325–326 с.
4. Ильин В.А., Позняк Э.Г. Аналитическая геометрия. М.: Наука, 1988. 223 с.
5. Кравцов Ю.А., Орлов Ю.А. Геометрическая оптика. М.: Мир, 1980. 304 с.
6. Бутиков Е.И. Физика для углубленного изучения. М.: Санкт-Петербург, 2000. 336 с.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ МОНОЛИТНОГО ПОЛЕВОГО ТРАНЗИСТОРА

Р.Г. Жулин, студент 5 курса ФВС

ТУСУР, кафедра КСУП, г. Томск

Цель работы разработать модуль для расчета параметров математической модели монолитного полевого транзистора, в которой будет реализован расчет S -параметров транзистора по его геометрическим размерам и режиму по постоянному току.

В настоящее время идет быстрый рост развития технологий, в том числе и технологий для приема и передачи информации. Достижения в полупроводниковой электронике позволяют системам приема и обработки информации работать с частотами до 100 ГГц. СВЧ-транзисторы используются для создания различных радиоэлектронных устройств. На основе этих приборов создаются усилители, генераторы, преобразователи и умножители частот и т.д., параметры которых должны удовлетворять заданным требованиям. До частоты 10 ГГц при проектировании широкополосных усилителей используются, как правило, биполярные транзисторы, на более высоких частотах – полевые транзисторы [1].

Начальным этапом разработки СВЧ-устройства по заданным требованиям технического задания является схемотехническое проектирование. На этом этапе проводятся сравнения нескольких возможных вариантов построения СВЧ-устройства, выбор оптимального по заданному критерию варианта и расчет полной принципиальной схемы устройства. Жесткие требования на характеристики СВЧ-устройств, сложные эквивалентные схемы активных элементов (АЭ) – все это приводит к необходимости использовать ЭВМ. Однако успех применения ЭВМ при проектировании СВЧ-устройств во многом зависит от правильного выбора структуры и параметров математической модели элементов [2].

Задаче построения математической модели СВЧ-транзистора (физической эквивалентной схемы – ФЭС) и посвящена данная работа. В ходе работы реализован программный модуль, осуществляющий расчет параметров монолитного транзистора по заданным геометрическим размерам и режиму по постоянному току. Модуль войдет в состав системы автоматизированного проектирования СВЧ-устройств, разрабатываемого на кафедре КСУП. Это позволит ускорить процесс разработки и повысить эффективность данной системы проектирования.

В качестве среды реализации программы была выбрана система MATLAB 6.5. Система MATLAB вобрала в себя не только передовой опыт развития и компьютерной реализации численных методов, накопленный за последние три десятилетия, но и весь опыт становления ма-

тематики за всю историю человечества. Около миллиона легально зарегистрированных пользователей уже применяют эту систему. Ее охотно используют в своих научных проектах ведущие университеты и научные центры мира.

MATLAB выполняет сложные и трудоемкие операции над векторами и матрицами. Также MATLAB обладает богатыми средствами работы с графической информацией. Теперь пользователю не нужно заниматься рутинным программированием процедур, реализующих изображения графиков (линий уровней, поверхностей). Данные возможности в системе MATLAB можно реализовать с помощью двух-трех функций. Кроме того, среда MATLAB 6.5 поддерживает все средства построения графического пользовательского интерфейса, которые необходимы для удобного и свободного управления программой [3].

ЛИТЕРАТУРА

1. *Текшев В.Б.* Проектирование СВЧ транзисторных усилителей с использованием ЭВМ. Учебное пособие. М.: МЭИ, 1983. 77 с.
2. *Хотунцев Ю.Л.* Полупроводниковые СВЧ-устройства (Анализ и синтез). М.: Связь, 1978. 80 с.
3. *Потемкин И.И.* Инструментальные средства Matlab 5_X. Москва 2001/2002.

ИНСТРУМЕНТАЛЬНАЯ СИСТЕМА СОЗДАНИЯ ТРЕНАЖЕРОВ ПО КУРСАМ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И МОДЕЛИРОВАНИЯ СИСТЕМ

Д.А. Звонков, 5 курс ФВС

ТУСУР, кафедра КСУП, г. Томск, т. 89234022980, perun@ms.tusur.ru

Современный уровень развития информационных технологий позволяет студенту изучать лекционный материал, выполнять практические индивидуальные задания, используя персональный компьютер, в том числе и дома, в удобной обстановке.

Г.Н. Решетниковой, доцентом каф. КСУП было предложено создать несколько тренажеров по курсам вычислительной математики и моделирования систем [2]. Суть тренажеров сводится к тому, что параллельно изучения лекционного материала студент смог бы наблюдать результаты работы изложенных методов. При этом он может опробовать описанный метод на различных наборах исходных данных и сравнить разные методы решения одной и той же задачи. Для решения поставленной задачи необходимо реализовать методы, изложенные в курсе и создать банк исходных данных для этих методов.

Мною было предложено создать инструментарий для реализации описанных методов, объединения их с лекционным материалом и создания тренажеров по математическим дисциплинам.

Многу было проведено исследование языков программирования [4, 5] и специализированных математических сред [6, 7], с помощью которых могли бы быть реализованы поставленные задачи. В ходе исследования было выявлено, что существующие языки программирования не дают необходимых возможностей для реализации. Специализированные математические среды имеют сложности с интеграцией с банком исходных данных, кроме того, использование этих сред приведет к необходимости использования их же студентом, что будет довольно накладно для студента, и к тому, что студенту будут доступны исходные коды реализованных методов, что нежелательно. По результатам исследования были сделаны выводы о необходимости создания своего математически ориентированного языка программирования и виртуальной машины, с возможностью встраивать программы в тренажеры и интеграцией с банком данных.

Виртуальная машина. Виртуальные машины можно разделить на стековые и регистровые. Регистровые виртуальные машины для хранения операндов и результатов операций используют регистры, а стековые – стек. Основными преимуществами регистровых виртуальных машин перед стековыми являются меньший объем программы и большие возможности оптимизации кода программы. Преимуществами стековых виртуальных машин являются простота трансляции в коды виртуальной машины и возможность использования многооперандных команд виртуальной машины, что может быть удобно в некоторых специфических случаях. Учитывая математическую специфику виртуальной машины, предлагается использовать стековые виртуальные машины.

Для реализации отдельных задач возможно гораздо удобнее будет использовать включаемые модули в виде dll библиотек, в которых будут реализованы специфические команды обработки данных. Поэтому предлагается использовать двухбайтовые команды, где первый байт представляет собой идентификатор включаемого модуля, а второй – номер команды. Естественно возможна ситуация, когда число необходимых операций превысит 256, тогда для одного включаемого модуля возможно регистрация нескольких идентификаторов модулей, но в этом случае необходимо выделить несколько функций интерпретаторов команд.

Все данные представлены в виде байтовых последовательностей переменной длины. Первый байт в этой последовательности является идентификатором типа данных. Естественно, что для стандартных типов данных, чья длина постоянна, таких как целое не отрицательное число, целое число, вещественное число, дробное число, комплексное число, булев тип, длина последовательности может не указываться. А для таких данных, как вектор или матрица, указатель длины последовательности просто необходим. Представление данных в виде последова-

тельностью байтов может быть удобна для работы включаемых модулей, использующих специфические типы данных и форматы их представления.

Состав виртуальной машины

- Загрузчик – производит загрузку программы в память программы, подключение встраиваемых модулей в интерпретаторе команд, регистрация методов виртуальной машины во встраиваемых модулях.

- Память данных – используется для хранения исходных и конечных данных, глобальных переменных и др.

- Память программы – память программы содержит список команд.

- Интерпретатор команд – интерпретатор команд анализирует текущую команду и передает ее код соответствующему модулю.

- Стек данных – содержит временные данные. Используется для передачи данных в вызываемые функции и операции, и для хранения возвращенных результатов.

- Стек командных адресов – содержит адреса точек возврата из функций.

- Блок регистров и флагов – содержит указатель на вершину стека, флаг ошибки, регистр кода ошибки, флаги трассировки и счетчик текущей команды.

- Помимо арифметических команд ядра, соответствующих встроенным функциям языка программирования следует реализовать так же специфические команды, такие как:

- команды обмена данных (передача данных между стеком, памятью данных, регистрами и флагами);

- команды переходов, в том числе безусловного перехода, условного перехода, вызова функций и возврата из них;

- команды разметки (команда *trace* для построчной трассировки, команда *stop* для завершения программы и команда *skip* – пустая команда).

Требования к языку программирования

Необходимо реализовать типы данных, которые часто встречаются в математике, такие как целые, вещественные, дробные и комплексные числа, вектора и матрицы.

Необходимо так же разработать список операторов, который будет приближен к тем операторам, которые используются в описании математических формул на бумаге. Те действия, которые не поддаются операторной форме записи, необходимо реализовать в виде встроенных функций, которые будут транслироваться в одну команду виртуальной машины. В операторной или функциональной форме следует реализовать основные арифметические операции, операции с комплексными числами, операции векторно-матричного аппарата.

Необходимо предусмотреть возможность описания пользователем собственных функций и возможность рекурсивного вызова пользовательских функций. Так как для разных задач порой необходимы одни и те же пользовательские функции, то необходимо реализовать возможность подключения функций, описанных в других файлах.

В некоторых специфических задачах может возникнуть ситуация, когда проще будет описать новые встраиваемые функции и расширить математическое ядро виртуальной машины. Для этих целей необходимо реализовать возможность использования включаемых модулей.

Язык программирования не предполагает операторов ввода или вывода данных. Вместо этого пользователь описывает переменные, которые программа получает на вход, и какие передает на выходе. А ввод и вывод этих данных осуществляется за средствами программы, запустившей данную программу. Это позволит использовать не только введенные пользователем исходные данные, но и загружать их из банка исходных данных. В качестве возвращаемого результата могут так же выступать директивы визуализации полученных данных (построить график, диаграмму с использованием полученных данных), которые будут выполняться средствами библиотеки визуализации.

Реализация вышеописанных инструментов позволит создавать аналогичные тренажеры не только по данным дисциплинам, но и по другим математическим, физико-техническим и экономическим дисциплинам.

ЛИТЕРАТУРА

1. *Борисов, С.И.* Варианты организации тренажеров обучению задач // Материалы региональной научно-методической конференции «Современное образование: интеграция учебы, науки и производства», Томск, изд-во томского гос. ун-та систем управления и радиоэлектроники ТУСУР, 2003. с. 85–86.
2. *Решетникова Г.Н.* Моделирование систем: учебное пособие / Г.Н. Решетникова; Федеральное агентство по образованию, Томск. гос. ун-т систем упр. и радиоэлектроники. Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2005. 261 с. 1
3. *Ахо, Альфред В.* Теория синтаксического анализа, перевода и компиляции. В 2 т. Пер. с англ. / Альфред В. Ахо; В. Ахо. М.: Мир, 1978. Т. 1: Ахо, Альфред В. Синтаксический анализ/ Альфред В. Ахо, Джеффри Д. Ульман. М.: Мир, 1978. 612 с.
4. *Архангельский А. Я.* Программирование в C++ Builder 6. М.: ЗАО «Издательство БИНОМ», 2004 г. 1152 с.
5. *Хомоненко А. Д. и др.* Delphi 7 / Под общ. ред. А.Д. Хомоненко СПб.: БХВ-Петербург, 2003. 1216 с.
6. *Дьяконов В. П.* MATLAB 6/6.1/6.5 + Simulink 4/5. Основные применения. М.: СОЛОН-Пресс, 2004. 768 с.
7. *Губинский Д.А., Турбина Е.С.* Вычисления в MathCAD 12. СПб.: Питер, 2006. 544 с.

ПРОГРАММНЫЙ МОДУЛЬ «НЕЧЕТКИЕ МНОЖЕСТВА»

А.А. Изюмов, студент 5 курса ФВС;

Н.Ю. Хабибулина, ст. преподав. каф. КСУП

ТУСУР, кафедра КСУП, г. Томск

Знания не всегда могут быть описаны точно – часто встречаются так называемые «нечеткие знания». Люди повседневно решают проблемы и делают заключения в среде «нечетких знаний», а для того чтобы интеллектуальные системы обладали такими возможностями как гибкость, широкий кругозор, адаптируемость, необходимо представление и использование нечетких знаний.

Очевидной областью внедрения алгоритмов нечеткой логики являются всевозможные экспертные системы, в том числе:

1. нелинейный контроль за процессами (производство);
2. самообучающиеся системы (или классификаторы), исследование рискованных и критических ситуаций;
3. распознавание образов;
4. финансовый анализ (рынки ценных бумаг);
5. исследование данных (корпоративные хранилища);
6. совершенствование стратегий управления и координации действий, например сложное промышленное производство.

Чаще всего для отображения и использования нечетких знаний используются процедуры фаззификации/дефаззификации. Основой процедуры дефаззификации является использование функции принадлежности переменной некоторому нечеткому множеству.

На рис. 1 и 2 приведены наиболее популярные виды функций принадлежности, а также способ их задания в разрабатываемом программном модуле. Для построения трапецевидной функции необходимы 4 точки, для колоколообразной – 3.

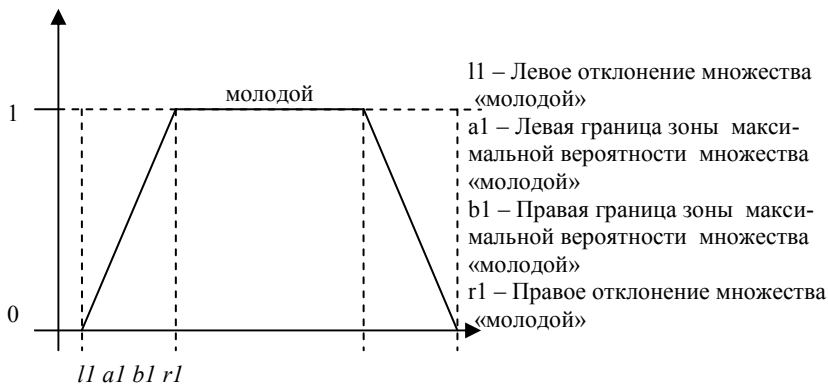


Рис. 1. Трапецевидная функция принадлежности

В ходе разработки модуля «Нечеткие множества», были решены следующие задачи:

- Модуль реализует работу с двумя типами функций принадлежности: колоколообразной (рис. 2) и трапециевидной (рис. 1);
- Количество множеств не ограничено;
- Каждое множество может иметь свое собственное имя, что облегчает процедуру дефазификации;
- Каждое множество внутри системы множеств может иметь свое собственное отклонение;
- Для каждого типа функции принадлежности, пользователь данного модуля может рассчитать вероятность попадания заданного значения переменной в систему множеств;
- Модуль оборудован собственной графической подсистемой – каждую систему множеств можно вывести одним из трех способов: построить график колоколообразной функции принадлежности, трапециевидной, или оба графика одновременно;
- Модуль имеет возможность загрузки и сохранения системы множеств, для их повторного использования (используется свой собственный внутренний формат хранения – единый двух типов функции принадлежности);

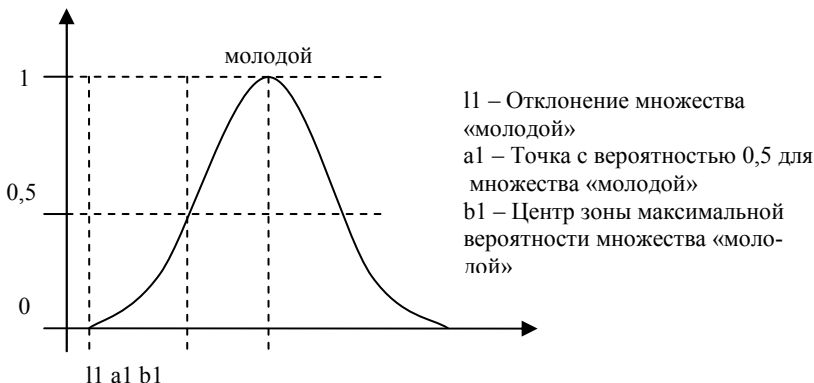


Рис. 2. Колоколообразная функция принадлежности

Основной целью данной разработки является ее интеграция в существующий программный комплекс создания и поддержания работоспособности гибридных экспертных систем. Кроме того, данный программный модуль используется в генераторе поясняющих и тестирующих задач, который является составной частью разработанной автоматизированной обучающей системы по курсу «Прикладные методы искусственного интеллекта».

ПРОГРАММНЫЙ МОДУЛЬ «НЕЙРОННЫЕ СЕТИ»

А.А. Изюмов, студент 5 курса ФВС

ТУСУР, кафедра КСУП, г.Томск

Первой попыткой создания и исследования искусственных нейронных сетей считается работа Дж. Маккалока (J. McCulloch) и У. Питтса (W. Pitts) «Логическое исчисление идей, относящихся к нервной деятельности» (1943 г.), в которой были сформулированы основные принципы построения искусственных нейронов и нейронных сетей. В ней предлагалась схема компьютера, основанного на аналогии с работой человеческого мозга.

Большим прорывом в области нейроинтеллекта стало создание нейрофизиологом Френком Розенблатом в 1962 г. модели однослойной нейронной сети, названной персептроном. Она была использована для такого широкого класса задач, как предсказание погоды, анализ электрокардиограмм и искусственное зрение.

За последние десятилетия теория о нейроинтеллекте приобрела новое дыхание. Было предложено много интересных разработок, таких, например, как когнитон, способный с высокой достоверностью распознавать достаточно сложные образы (например, иероглифы) независимо от поворота и масштаба изображения. Автором когнитона является японский ученый К. Фукушима (K. Fukushima).

Основной целью данной работы является разработка программного модуля, реализующего основные функции нейронной сети. Необходимость данной разработки связана с необходимостью расширения функций существующего программного комплекса создания и поддержания работоспособности гибридных экспертных систем в области использования нейронных сетей. Кроме того, данный программный модуль используется в генераторе поясняющих и тестирующих задач, являющегося составной частью автоматизированной обучающей системы по курсу «Прикладные методы искусственного интеллекта».

В ходе разработки модуля «Нейронные сети», были решены следующие задачи.

- Реализован метод обучения нейронной сети на основе алгоритма обратного распространения ошибки.

- Возможно задавать различные критерии для остановки процесса обучения, в том числе, процесс обучения можно искусственно прерывать, а затем продолжить.

- Количество слоев в сети – 100.

- Количество нейронов на одном слое не ограничено.

- В сети могут присутствовать скрытые слои.

- Каждый слой сети имеет свое собственное название.
- Значения обучающей выборки можно нормализовать.
- Реализована возможность настраивать шаг сети (чем он меньше, тем больше времени сеть будет тратить на обучение и тем более возможно ее попадание в окрестность локального минимума ошибки).
- Реализована возможность загрузки обучающей выборки из файла (используется свой собственный формат хранения).

В экономике и бизнесе обычно применяют нейросети, мощность которых ограничена примерно 100 входами. Этого чаще всего хватает для описания того или иного поведения финансового рынка или другого сложного нелинейного процесса. Разработанный модуль «Нейронные сети», реализует все возможности, необходимые для решения задач любой сложности.

АВТОМАТИЗИРОВАННАЯ ОБУЧАЮЩАЯ СИСТЕМА ПО ТЕМАМ «НЕЧЕТКИЕ МНОЖЕСТВА» И «НЕЙРОННЫЕ СЕТИ»

А.А. Изюмов, студент 5 курса ФВС;

Н.Ю. Хабибулина, ст.преподав. каф. КСУП

ТУСУР, кафедра КСУП, г.Томск

Целью данной разработки является создание автоматизированной обучающей системы по темам «Нечеткие множества» и «Нейронные сети», рассматриваемым в процессе изучения дисциплины «Прикладные методы искусственного интеллекта». Структура разработанного программного продукта представлена на рисунке.

Основными составляющими частями являются: блок интерфейса, блок тестирования и блок администрирования.

Блок интерфейса отвечает за отображения лекционного материала и представления его в форме, удобной для отображения. Использование для отображения лекций формата *.mht позволяет легкой модификации самого материала любым текстовым редактором.

Блок тестирования предназначен для проверки качества усвоения лекционного материала. Цель этого блока – визуализировать процесс тестирования, обеспечить вывод вопросов разных типов.

Блок администрирования предоставляет администратору программного продукта возможность изменять важнейшие функции управления базой вопросов.

Реализована работа с графическими (когда варианты ответа представляют собой картинки) и текстовыми вопросами двух основных типов: закрытых (когда пользователю необходимо выбрать из предлагае-

мых вариантов ответов) и открытых (когда пользователю необходимо ввести значение): закрытый (на основе компонента TCheckBox) – «1», открытый (на основе ввода в компонент TEdit) – «2», графический закрытый – «3», открытый вопрос на нечеткие множества – «4», закрытый вопрос на нечеткие множества – «5», открытый вопрос на нейронные сети – «6», закрытый вопрос на нейронные сети – «7». Сами вопросы хранятся в зашифрованных модулем шифрования файлах с расширением *.txt.

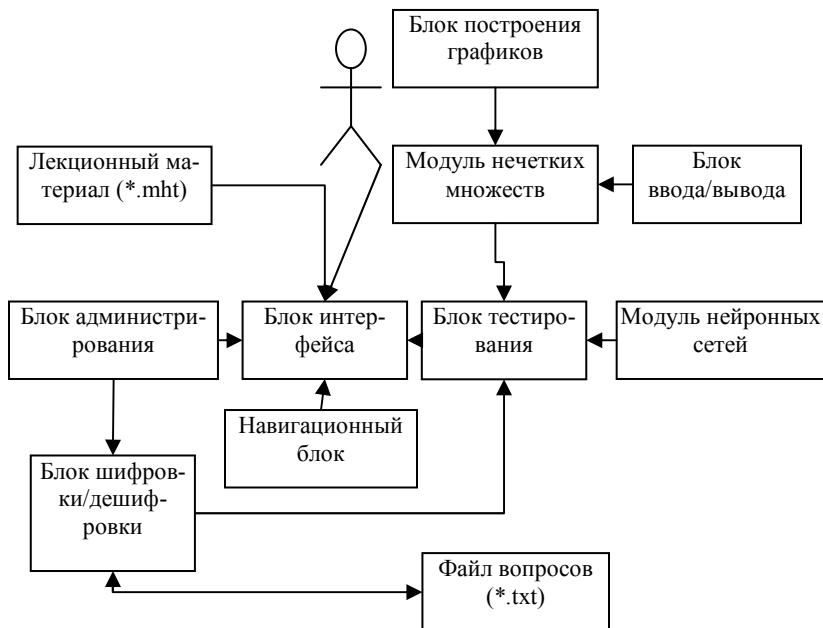


Рис. 1. Структура разработки

Подключение к АОС модуля нечетких множеств обеспечивает программный продукт всем необходимым инструментарием для работы с нечеткими знаниями, а модуля нейронных сетей – для работы с нейросетями.

Вопросы по теме «Нечеткие множества» и «Нейронные сети» генерируются автоматически при каждом запуске тестирующего блока, причем при каждом запуске случайным образом генерируются основные числовые значения вопроса. Студент выполняет задание, параллельно этому программный продукт также получает правильный ответ, далее эти значения сравниваются и выставляется оценка по вопросу.

Таким образом исключается возможность «заучивания» правильных вариантов ответа.

Оценивание полученных ответов происходит с учетом трудности вопроса и частичности полученных ответов. При запуске модуля тестирования осуществляется подсчет максимума баллов по следующей формуле:

$$\text{Макс.балл} = \sum_{\substack{\text{число} \\ \text{вопросов}}} (\text{число прав.ответов}) * (\text{сложность вопроса})$$

Таким образом, варьированием сложности вопроса достигается нормирование базы по «стоимости», т.е. для пользователя становится не критичным ответить на все вопросы – он может ответить на самые легкие и получить оценку «удовлетворительно», или ошибиться в некоторых местах и получить «хорошо».

Разработанный формат хранения базы вопросов универсален – и оставляет возможность модификации самих вопросов, а также подключаемых данных.

Данные внутри файлов вопросов зашифрованы уникальным алгоритмом (с повышенной криптоустойчивостью), что исключает возможность подбора алгоритма дешифрования на основе лингвистического анализа.

Разработанная АОС – удобное средство обучения студентов, призванное облегчить преподавателю процесс преподавания дисциплины «Прикладные модули искусственного интеллекта». С помощью несложных модификаций, АОС легко переписать для любой другой дисциплины, для которой необходимо использовать нечеткие знания и нейросети.

СИСТЕМА АВТОТРЕКИНГА ДЛЯ СИСТЕМ БЕСПРОВОДНОЙ ОПТИЧЕСКОЙ СВЯЗИ *А.А. Исаенко, студент 5 курса ФВС; И.А. Столбов, аспирант ТУСУР, кафедра КСУП, г.Томск*

В настоящее время системы беспроводной оптической связи (СБОС) считаются одной из перспективных коммуникационных технологий [1]. Эти системы получают все большее распространение в качестве альтернативы существующей медной и волоконно-оптической инфраструктуре в местах, где прокладка кабеля невозможна или затруднена.

К основным проблемам эксплуатации СБОС являются высокие требования к точности совмещения и стабилизации оптических осей

источника и приемника системы [2]. Колебания зданий, на которых установлены СБОС, вибрации основания передатчика, флуктуации показателя преломления атмосферы на трассе распространения отклоняют лазерные пучки от направления на приемник. В связи с этим становится актуальной задача адаптивного наведения лазерных потоков передатчика на приемник абонента в процессе работы СБОС.

Проблему ухода лазерного пучка от оптической оси приемника обычно решают путем увеличения угла расходимости этого пучка. В результате такого подхода приходится значительно повышать мощность источника лазерного излучения, что ведет к лишним энергозатратам.

Для нормального функционирования каналов связи осуществляемых узким пучком необходимо применять автоматические динамические системы наведения и слежения (системы автотрекинга).

Большинство известных способов автотрекинга СБОС основано на том, что для компенсации ухода луча механически перемещается вся система [3]. Такой способ автотрекинга является неэффективными, так как приходится применять мощные и очень точные системы позиционирования, стоимость которых значительно превышает стоимость самой СБОС.

Наиболее перспективным решением автотрекинга является использование оптико-механических компенсаторов, которые в настоящее время активно применяются в телевизионных системах оптической стабилизации изображения [4]. Однако установка компенсаторов в приемную часть системы, как это делается в телевизионном оборудовании, является неэффективным решением, так как вызывают значительные аберрации в приемном тракте.

Наиболее оптимальным решением является установка оптико-механических компенсаторов в оптический тракт излучателя. Так как в лазерных СБОС диаметр оптической системы лазера значительно меньше диаметра оптической системы приемника, то и габаритные размеры компенсаторов для лазера будут меньше требуемых размеров компенсаторов приемника. А это значит, что для управления компенсаторами лазерного пучка потребуются менее мощные приводы, чем для управления компенсаторами приемника, или для управления позиционированием всего устройства СБОС.

Для решения задачи динамического наведения лазерных потоков передатчика на приемник абонента в процессе работы СБОС предлагается реализовать систему автотрекинга следующим образом (рис. 1).

В оптическую схему лазера устанавливаются два оптических клина. Шаговые двигатели ШД1 и ШД2, управляемые микроконтроллером посредством силовых драйверов, вращают клинья, угловые координаты

которых отслеживаются микроконтроллером с помощью датчиков ДУ1 и ДУ2. В зависимости от выбора геометрических и кинематических параметров (углы при вершинах клиньев, показатели преломления, скорости и направления вращения) можно получить самые разнообразные виды развертки (строчную, эллиптическую, спиральную, по сложной кривой) [5].

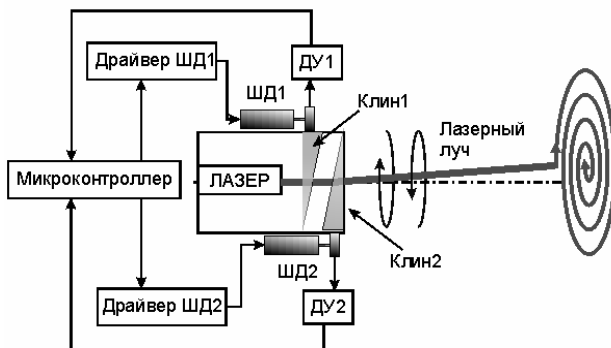


Рис. 1. Структура системы автотрекинга

Система может использоваться как для наведения, так и для удержания на одной линии оптических осей источника и приемника.

В режиме поиска и наведения система осуществляет сканирование в области приемника по траектории «Архимедова спираль».

В режиме удержания соосности передатчика и приемника (автотрекинг) приемник при помощи двухкоординатного датчика положения отслеживает максимум сигнала с передатчика, и при его смещении СБОС передает на противоположный конец канала информацию о том, на сколько необходимо сместить пучок, чтобы вернуть максимум на место (свести оси). Система автотрекинга смещает пучок и ждет следующего сигнала от приемника.

Таким образом, предложена система автотрекинга, которая по сравнению с известными аналогами способна более эффективно выполнять задачи совмещения и стабилизации оптических осей источника и приемника СБОС.

ЛИТЕРАТУРА

1. Милинкус Б.М. Атмосферная лазерная связь. Информост – Радиоэлектроника и телекоммуникации, 2001. №5 (18). с. 17–23.
2. Клоков А.В. Беспроводные ИК-технологии, истинное качество «последней мили». Технология и средства связи, 1999, № 5. с. 40–44.
3. <http://www.canon.com/bctv> – Технология автотрекинга систем беспроводной оптической связи Canobeam DT-50 фирмы Canon.

4. http://www.625net.ru/archive/arc_2004.htm#8_04 – Оптическая стабилизация изображения в телевизионных объективах. Березенцева Л.М.
5. Парвулюсов Ю.Б. Проектирование оптико-электронных приборов. Москва: Машиностроение, 1990. 432 с.

УЛЬТРАЗВУКОВОЙ ДОПЛЕРОВСКИЙ НЕИНВАЗИВНЫЙ ИЗМЕРИТЕЛЬ СКОРОСТИ КРОВОТОКА

***И.Х. Каримов, студент 5 курса ФВС; А.В. Ковинов, аспирант
ТУСУР, кафедра КСУП, г. Томск***

Уже давно в медицине существует проблема регистрации и измерения низкоскоростных кровотоков, таких как: венозных кровотоков в сосудах головы и конечностей, измерение кровотоков по малым артериям – латеральные кровотоки (микрохирургия, трансплантация и др.), измерение перфузии (кровоснабжения) тканей. В качестве отдельной задачи можно выделить проблему измерения кровотоков в открытых при операции сосудах малого сечения.

Применяемые в настоящее время доплеровские ультразвуковые комплексы не позволяют проводить такие измерения из-за ограничения на минимальную регистрируемую скорость. Данное ограничение возникает в связи с необходимостью фильтрации мощных низкочастотных составляющих в спектре принимаемого УЗ сигнала, возникающих вследствие отражения излучаемого сигнала от колеблющихся с частотой сердечных сокращений стенок сосудов.

В предположении, что граничная частота фильтра составляет 200 Гц из формулы для доплеровского сдвига частоты F_d следует, что прибор, работающий на частоте 8 МГц, в угле 30° , может обнаружить кровоток со скоростью не ниже 2 см/с. Такое значение минимальной скорости, по меньшей мере, вдвое больше величины, характерной для кровотока в малых артериях и венах, и на порядок превышает скорость кровотока в капиллярах и венах.

Единственным решением поставленной задачи является создание высокочастотных доплеровских комплексов, т.к. только таким способом можно преодолеть ограничение на минимальную измеряемую скорость. Например, для прибора, работающего на частоте 20 МГц, значение минимальной регистрируемой скорости составляет 0,1 см/с, что позволяет проводить измерения низкоскоростных кровотоков. Для сравнения приведена таблица скоростей кровотока в различных сосудах.

Главная проблема, которая встает на пути разработки аппаратуры такого класса, – быстрое возрастание коэффициента затухания ультразвука в тканях человеческого тела пропорционально частоте колеба-

ний. Так, затухание в мягких тканях составляет в среднем 0,7 дБ см – 1 МГц, т.е. на частоте 8 МГц затухание ультразвука при обследовании сосуда, расположенного на глубине 1 см составит 11 дБ, в то время как величина затухания ультразвука частотой 20 МГц при исследовании того же сосуда составит около 30 дБ, т.е. амплитуда принимаемого сигнала на частоте 20 МГц будет на порядок меньше, чем у 8 МГц канала при тех же параметрах передатчика.

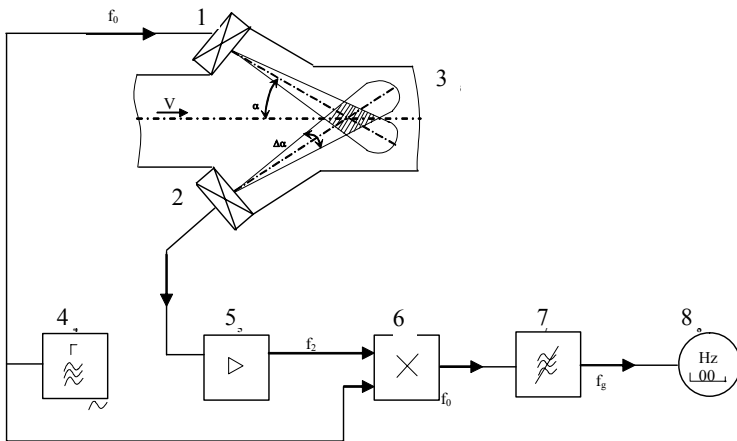


Рис. 1. Функциональная блок схема измерителя. 1 – излучатель, 2 – приемник, 3 – рабочая камера (кровеносный сосуд), 4 – генератор 20 МГц, 5 – малошумящий усилитель, 6 – фазовый детектор, 7 – НЧ-фильтр, 8 – дисплей

Технические характеристики прибора

Рабочая частота	20 МГц	
Диапазон скоростей	0,1–10 см/с	
Зависимость затухания от частоты	1 МГц	0,7 дБ/см
	8 МГц	11 дБ/см
	20 МГц	30 дБ/см
Ошибка измерения	2%	
Диапазон расстояний до объема, где измеряется скорость	1–10 мм	
Размеры рабочей поверхности датчика	10 × 10 мм	

Вместе с тем, с ростом частоты, увеличивается и доля отраженного кровотоком ультразвука, поскольку в случае релеевского рассеяния (размер рассеивателя – в нашем случае эритроцита 7,2×2,2 мкм – много меньше длины рассеиваемой волны) мощность рассеянной волны пропорциональна четвертой степени частоты.

Система обработки выполняет следующие функции:

- измеряет среднюю скорость кровотока и индицирует результат;
- определяют знак доплеровского смещения частоты, а, значит, и направление кровотока.

Рассматривая проблему в целом можно прийти к выводу о том, что на сегодняшний день еще не существует технических возможностей для создания прибора с более высокими параметрами.

ЛИТЕРАТУРА

1. *Энергетическая доплерография – новая диагностическая технология визуализации кровотока.* // В сб.: Новые диагностические технологии. Организация службы функциональной диагностики. Москва. 1996. С. 32 (со авт. В.П. Куликов).

СПЕЦИАЛИЗИРОВАННЫЙ ГРАФИЧЕСКИЙ РЕДАКТОР ДЛЯ ВВОДА СХЕМ СВЧ-УСТРОЙСТВ

*А.Ю. Квашин, студент 5 курса ФВС, Л.И. Бабак, к.т.н., доцент
ТУСУР, кафедры КСУП, г. Томск*

Реализован программный модуль, представляющий собой графический редактор для ввода схем СВЧ-устройств с учетом ограничений, накладываемых языком описания этих схем – SRL. Разработан метод представления и хранения СВЧ-цепей, позволяющий вывести нарисованную цепь на экран монитора и сохранить готовую цепь в формате языка SRL, не беспокоясь о нарушении правил этого языка.

На кафедре КСУП ТУ СУР реализован ряд программ, в которых имеется ввод схем СВЧ-устройств в текстовом виде на языке SRL. Пользователю приходится описывать схему в текстовом редакторе, что является неудобным в случае больших и сложных схем. Данный редактор должен стать частью этих программ и упростить ввод СВЧ цепей, дав пользователю возможность визуального контроля над ними.

При работе над редактором был разработан способ представления цепей схемы в программе. Каждая цепь представляет собой отдельный объект, который, в свою очередь так же, может быть представлен из нескольких объектов [1–3], которые в свою очередь таким же образом могут состоять из объектов и так далее. Элемент – «Активный блок» представляет собой описание самого элемента и массива цепей, входящих в состав этого активного блока. Редактор имеет следующие основные функциональные возможности: рисование последовательной и параллельной цепей, объединение нескольких цепей в одну схему, рисо-

вание «Активного блока» с последующим добавлением его в общую схему и сохранение схемы в формате языка SRL.

ЛИТЕРАТУРА

1. *Поляков А.Ю.* Методы и алгоритмы компьютерной графики в примерах на Visual C++. СПб.: БХВ – Петербург, 2002. 416 с.
2. Разработка приложений на Microsoft Visual C++ 6.0. Учебный курс / Пер, с англ. 2-е изд. М.: Издательско-торговый дом «Русская редакция», 2001. 704 с.
3. *Боровской И.Г.* Технология разработки программных систем (Ч. 3. Microsoft Visual C++). Учебное пособие // Томск, ТУ СУР, 2000. 140 с.

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА «НАХОЖДЕНИЕ ЭКСТРЕМУМОВ МНОГОЭКСТРЕМАЛЬНЫХ ФУНКЦИЙ ПРИ ПОМОЩИ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ»

***С.В. Китлер, студент 5 курса ФВС
ТУСУР, кафедра КСУП, г.Томск***

Целью работы является разработка программного обеспечения вычислительного практикума по дисциплине «Системный анализ и методы принятия решения». Основная задача – разработка программного комплекса «Решение задач многоэкстремальной оптимизации при помощи генетических алгоритмов».

Оптимизация в широком смысле слова находит применение в науке, технике и в любой другой области человеческой деятельности. Это могут быть задачи проектирования, задачи распределения ограниченных ресурсов, задачи определения оптимальной траектории летательного аппарата и т.п. Подобные задачи часто встречаются в ряде прикладных областей при моделировании реальных процессов: теории управления, моделировании физических явлений, анализе данных и других областях, где необходимо получить наилучший результат целевой функции на множестве некоторых ограничений.

В силу широты класса многоэкстремальных функций задача глобальной оптимизации в общем случае является неразрешимой, т.е. нельзя гарантировать, что решение задачи будет получено за конечное число шагов. Даже некоторые из разрешимых задач могут попасть в класс неразрешимых, т.к. число шагов, необходимых для получения решения, может быть чрезмерно большим. Для того чтобы решить задачу, помимо непрерывности функции цели, необходимы некоторые дополнительные условия ее гладкости. Таким образом, специфика задачи глобальной оптимизации заключается в многоэкстремальности функции цели и неразрешимости в общем случае.

Развитие методов глобальной оптимизации стимулируется не только актуальностью или сложностью этих задач, но и развитием вычислительной техники. В настоящее время параллельные и векторные суперкомпьютеры рассматриваются как один из основных инструментов для проведения исследований в различных научных и прикладных дисциплинах. Всего лишь несколько лет назад параллелизм рассматривался как редкая и экзотическая область вычислений, интересная, но не предназначенная для «простых» пользователей. Анализ тенденций развития прикладных приложений, архитектур вычислительных систем, сетей показывает, что эта точка зрения уже неверна. Параллельные компьютеры не только перестали быть редкостью, но и становятся, в связи с развитием многоядерных архитектур, повседневным орудием исследования. Проблемам параллельных вычислений в задачах глобальной оптимизации, а также различным подходам к распараллеливанию алгоритмов глобальной оптимизации в настоящее время придается большое значение.

Для решения задачи глобальной оптимизации не существует универсального по эффективности алгоритма. Поэтому при разработке специфических методов глобальной оптимизации в первую очередь учитывают свойства целевой функции и рассматриваемого класса задач, для которого разрабатывается метод.

Методы глобальной оптимизации можно разделить на две категории: детерминированные и стохастические. Детерминированные методы получают глобальное решение посредством исчерпывающего поиска на всем допустимом множестве. Поэтому большинство детерминированных методов теряют эффективность и надежность с возрастанием размерности задачи. Более того, чтобы гарантировать успех, такие методы требуют выполнения дополнительных предположений, наложенных на функцию цели. Детерминированные методы не используют стохастики.

Стохастические алгоритмы позволяют уйти от проблем детерминированных алгоритмов. Стохастический подход присутствует не только в разработке и анализе алгоритма, но и используется в решении базовых проблем, например, при определении условия остановки.

Исторически первым методом глобальной оптимизации является метод Монте-Карло, на базе которого был создан метод мултистарта. В методе мултистарта из множества X случайно или детерминировано выбирается некоторое подмножество из N точек. Последовательно из каждой точки запускается алгоритм локального спуска, и из полученного множества локальных решений выбирается наилучшее. В чистом виде метод мултистарта не является эффективным, т.к. одно и то же

локальное решение может быть найдено не один раз. Мультистарт – это обобщенный подход: большинство эффективных методов глобальной оптимизации основано на идее метода мультистарта – запуска стандартных локальных алгоритмов из множества точек, равномерно распределенных на множестве X . Таким образом, метод мультистарта можно назвать прототипом таких методов.

В последнее время значительное распространение получили методы моделирования обжига и контролируемого случайного поиска. Основная идея метода моделирования обжига исходит из физики процесса замерзания жидкостей или рекристаллизации металлов в процессе обжига. Целевая функция здесь является аналогом равновесия термодинамической системы и видоизменяется путем добавления случайных величин. Процесс повторяется достаточное число раз для каждой температуры, после чего температура понижается и весь процесс происходит снова до состояния полной заморозки.

Алгоритм контролируемого случайного поиска является методом прямого поиска. Алгоритм начинает работу на множестве S начальных точек, равномерно распределенных на допустимом множестве задачи. Многократно образуются новые испытываемые точки, которые замещают подмножество W худших точек из множества S в случае, если они лучше. Алгоритм останавливается, когда все полученные значения функции достаточно близки.

При решении задач функциональной оптимизации стали широко применяться генетические алгоритмы (ГА). Они основаны на генетических процессах биологических организмов: биологические популяции развиваются в течение нескольких поколений, подчиняясь законам естественного отбора и принципу «выживает сильнейший». ГА получили широкое распространение для решения задач поиска и оптимизации в самых разнообразных областях науки и техники.

Генетические алгоритмы – это вычислительные модели, которые представляют собой семейство алгоритмов поиска, основанных на механизмах природной селекции и генетики, и имеющих дело с набором (популяцией) возможных решений задачи (испытаний), которые подвергаются циклическому воздействию трех основных «генетических» операторов – селекции, скрещивания и мутации. Существенная особенность этих алгоритмов заключается в кодировании потенциального решения некоторой проблемы в виде простой хромосомо-подобной структуры данных. К набору таких хромосом собственно и применяют операторы рекомбинации с тем, чтобы сохранить критическую информацию.

Работа генетического алгоритма начинается с генерирования некоторой (как правило, случайной) популяции хромосом, каждой из кото-

рых соответствует точка в пространстве поиска. Затем происходит оценка этих структур (расчет целевой функции для каждой хромосомы) и распределение между ними репродуктивных возможностей таким образом, чтобы хромосомы, представляющие лучшее решение исходной проблемы, получили больше шансов, для «воспроизводства» чем хромосомы, соответствующие худшими решениями. Качество решения обычно определяется по отношению к текущей популяции.

Будучи вероятностными, генетические алгоритмы, не являются еще одним вариантом случайного поиска, поскольку при отборе новых точек с ожидаемыми более хорошими характеристиками, они эффективно используют предыдущую информацию.

Важной особенностью генетических алгоритмов является то, что они обеспечивают сходимость к глобальному оптимуму. В отличие от классических градиентных методов оптимизации при реализации генетических алгоритмов не требуется ставить ограничения на гладкость целевой функции. Более того, они позволяют находить оптимум даже в случае, разрывной целевой функции.

Так же важным свойством ГА является естественный внутренний параллелизм. При этом, по сравнению с градиентными методами, различие во времени расчета целевой функции при различных значениях ее параметров не оказывает влияния на эффективность распараллеливания. Эти времена могут отличаться на порядки – например, если можно определить, что точка в пространстве поиска не отвечает наложенным ограничениям, не вычисляя целевую функцию или вычисляя ее только частично.

Создаваемая программа будет ориентирована на подготовку специалистов, использующих современные компьютерные технологии выбора оптимальных вариантов при исследовании или проектировании процессов, изделий, приборов, конструкций различной природы.

Изучение предлагаемой программы позволит пользователям получить знания в области математических моделей, методов и программных средств принятия оптимальных решений.

ИНТЕРАКТИВНАЯ СИСТЕМА ВЫБОРА КОНДЕНСАТОРОВ И АВТОМАТИЧЕСКАЯ УСТАНОВКА ИХ НА СХЕМУ ЭЛЕКТРИЧЕСКУЮ ПРИНЦИПИАЛЬНУЮ

А.С. Климович, студент 5 курса ФВС;

*А.А. Пономарев, инж.-программист 1 кат. ФГУП «НПЦ «Полюс»
ТУСУР, кафедра КСУП, г.Томск*

В процессе разработки электронных блоков, проектирования или модернизации их отдельных частей, проекта в целом, конструкторам и

разработчикам постоянно приходится обращаться к различным документам, таким как технические условия (ТУ), стандарты предприятия (СТП), и, в частности, работать с документами на электро-радио изделия (ЭРИ) для определения параметров ЭРИ и его записи в документации, выявление ограничений на использование ЭРИ в соответствии со стандартами предприятия.

Вследствие чего при разработке печатных плат возникает множество факторов понижающих скорость проектирования и качество изделия. Следовательно, есть необходимость создания программы, которая помогала бы ускорить и упростить процесс выбора полного наименования ЭРИ, а также исключить подавляющее количество ошибок человека.

На основе проведенного анализа было разработано техническое задание, где сформулированы задачи и требования к программному комплексу.

Программа содержит информацию обо всех используемых на предприятии конденсаторах в соответствии с их ТУ от завода-производителя элементов. Описание каждого типа конденсатора должно храниться в отдельном программном модуле.

Программный комплекс реализован в среде Windows и выполняет следующие функции.

- Оболочка программного комплекса содержит закладки для каждой разновидности конденсаторов, что обеспечивает легкое нахождение требуемого элемента.

- В автоматическом режиме формируется запись наименования конденсатора.

- Копируется сформированное наименование элемента в буфер обмена.

- Происходит вывод подробной информации о выбранном конденсаторе.

- Взаимодействует с системой Schematic P-CAD2002, позволяя автоматически устанавливать на схему выбранный элемент и прописывать в его атрибуты сформированное наименование.

- Программа имеет возможность представлять наименование как на русском так и на латинском языках. Запись на русском языке необходима для корректировки текстовых документов. Запись латиницей необходима для записи атрибутов конденсатора в Schematic, так как уже есть разработанные ранее программы автоматического формирования перечня элементов и ведомости покупных изделий, работающих с атрибутами на латинском.

В данный момент времени написана часть программы, обрабатывающая закладки конденсаторов серии K52-11, K52-10 с автоматическим формированием полной записи конденсатора. На рисунке 1 пред-

ставлено основное окно конденсатора серии K52-11, одной из выбранных закладок.

КонденсаторВыбор												
K10-17a	K10-17b	K10-47a	K10-47b	K15-20b	K50-29	K50-68	K52-9	K52-10	K52-11	K53-22	K53-25	K73-16
Конденсатор K52-11 (инв.№9080) О.Ж.0.464.234ТУ												
Номинальное напряжение В												
Номинальная емкость мкФ												
6,3 В	16 В	25 В	32 В	50 В	63 В	100 В	Видео разм.					
С 150	С 100	С 68	С 47	С 33	С 22	С 15	1					
С 330	С 220	С 150	С 100	С 68	С 47	С 33	2					
С 680	С 470	С 330	С 220	С 150	С 100	С 68	3					

Рис. 1. Вид основного окна с активной закладкой на конденсатор K52-11

Разрабатываемая программа поможет разработчикам электронных схем избежать ошибок в файле схемы и, соответственно, в таких документах, как перечень элементов и ведомость покупных изделий. Следовательно, при ее использовании во время проектирования снижаются временные затраты на разработку и материальные затраты в процессе производства.

КОРПОРАТИВНАЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА РЕКЛАМНОЙ КОМПАНИИ

Е.В. Коркач, студент 5 курс ФВС

Н.Ю. Хабибулина, ст. препод. каф. КСУП

ТУСУР, кафедра КСУП, г.Томск, jonny1984@mail.ru

Эффективность построения и использования корпоративных информационно-аналитических систем стала чрезвычайно актуальной задачей, особенно в условиях нынешней рыночной конкуренции.

Критериями оценки эффективности могут служить снижение стоимости реализации информационно-аналитической системы, соответствие текущим требованиям и требованиям ближайшего времени, возможность и стоимость дальнейшего развития и перехода к новым технологиям.

На сегодняшний день оперативность предоставления информации тесно связана с понятием «интернет».

Постепенно уходят в прошлое времена, когда люди перелистывали увесистые бумажные справочники в поисках нужной информации. Возьмем, к примеру, менеджера по рекламе, которому необходимо

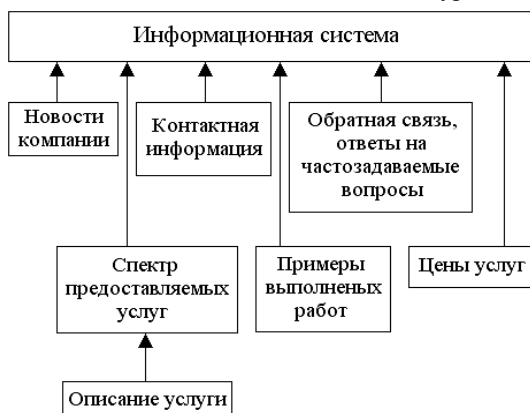
срочно изготовить сувениры с фирменной символикой. Алгоритм его действий сегодня будет выглядеть примерно так: набрать в строке одной из поисковых систем соответствующее словосочетание, просмотреть полученный список организаций, затем зайти на сайт каждой из приглашенных компаний в целях изучения ассортимента, прайс-листа, условий работы с клиентами и т.п. И только после всех этих операций грамотный менеджер позвонит в пару-тройку фирм, чтобы что-то окончательно выяснить, уточнить и договориться о чем-то конкретном в процессе телефонной беседы.

Основной целью работы является разработка информационно-аналитической системы рекламной компании.

Для достижения данной цели были сформулированы следующие задачи:

- разработать структуру базы данных информационно-аналитической системы;
- разработать структуру web-сайта;

На сегодняшний день на рынке услуг, предоставляемых компанией-заказчиком, сайты компаний-конкурентов схожи между собой. Информационные системы таких фирм в интернет принято называть «сайтами-визитками». Для информационного сайта разработана структура, изображенная на рис. 1.



формационные системы таких фирм в интернет принято называть «сайтами-визитками». Для информационного сайта разработана структура, изображенная на рис. 1.

Рис. 1. Структура информационного сайта

Информационная система представляет собой базу данных с интегрированным web-интерфейсом. База данных содержит информацию достаточную для представления рекламной фирмы на рынке соответствующих услуг. База данных спроектирована таким образом, чтобы удобно хранить и корректировать данные компании. Физическая модель базы данных (КВ уровень) представлена на рис. 2.

В результате проделанной работы разработана структура информационно-аналитической системы. Элементы построены по типу «сайта-визитки». В соответствии со спроектированной структурой разработана модель базы данных. Ее пополнение происходит с помощью спе-

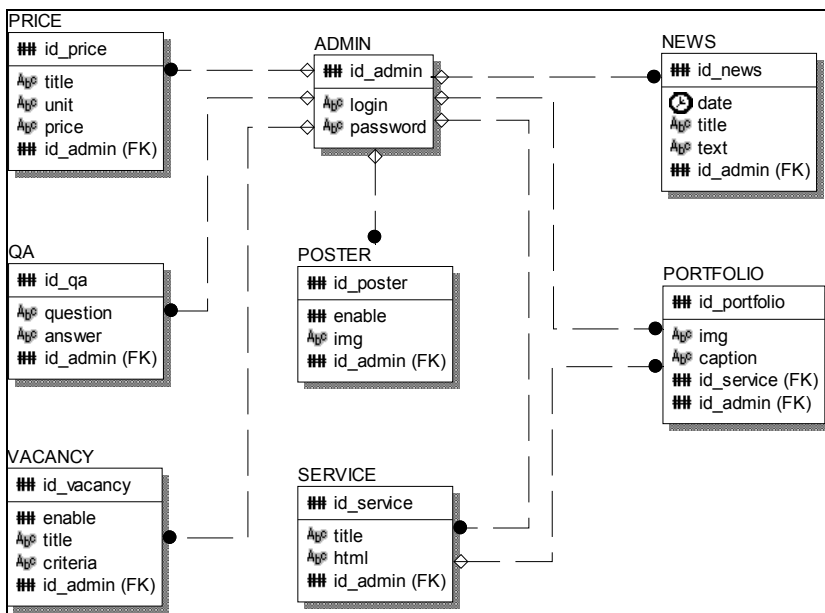


Рис. 2. Физическая модель базы данных (КВ уровень)

циально разработанной администраторской страницы. В аналитической части сайта реализована возможность рассчитать стоимость разработки предлагаемых рекламных продуктов.

РАЗРАБОТКА СИСТЕМ АТМОСФЕРНОЙ ОПТИЧЕСКОЙ СВЯЗИ

*О.П. Коротин, студент 5 курса ФВС
ТУСУР, кафедра КСУП, г.Томск*

Системы атмосферной оптической связи (CAOC), в зарубежной литературе известные под названием FSO – Free Space Optical, получают все большее распространение в качестве альтернативы существующей медной и волоконно-оптической инфраструктуре в местах, где прокладка кабеля невозможна или затруднена [1]. К преимуществам подобного рода систем можно отнести высокие скорости передачи информации, которые невозможно достичь при использовании любых других беспроводных технологий; простота инсталляции, а также отсутствие необходимости получать лицензии и платить за использова-

ние частотного диапазона. Более широкое применение беспроводных оптических систем сдерживается их зависимостью от погодных условий.

Атмосферные оптические линии реализуют двухточечные соединения: данные передаются между двумя оптическими терминалами, в каждом из которых имеются отдельные приемник и передатчик, как правило, с разнесенными оптическими трактами – во избежание возможных помех и переотражений.

Построение всех САОС практически одинаково – интерфейсный модуль, модулятор излучателя, оптическая система передатчика, оптическая система приемника, демодулятор приемника и интерфейсный блок приемника [2].

Все САОС по технологическому признаку можно разделить на две группы [3]. Одна группа использует полупроводниковые ИК-диоды (с излучением с поверхности), а вторая группа использует для излучения полупроводниковые ИК лазерные диоды (с излучением с торца перехода). Главное различие систем сказывается на их главных характеристиках – скорости и дальности передачи. Первая группа – это в основном короткоходные системы до 1,5 км со скоростями до 20 Мбит/с. Вторая группа – обеспечивает дальности передачи до 3...15 км, в зависимости от погодных условий и требований к качеству канала, со скоростями до 155 Мбит/с (коммерческие системы) или до 10 Гбит/с (опытные системы).

В качестве приемников излучения в САОС применяются *p-i-n*-фотодиоды (на скоростях до 100 Мбит/с), либо лавинные фотодиоды (на скоростях выше 100 Мбит/с).

Определившись с типом излучателя и оптической схемой САОС необходимо определить минимально требуемую мощность излучателя. Для этого производится расчет оптического канала связи. При этом необходимо учитывать особенности распространения оптического излучения в атмосфере.

Основными факторами, влияющими на распространение оптического сигнала в атмосфере, являются [4]:

- молекулярное (релеевское) рассеяние света;
- аэрозольное рассеяние;
- молекулярное поглощение;
- турбулентные явления в атмосфере;
- нелинейные эффекты распространения;
- фоновые помехи от посторонних источников в атмосфере.

Учет при расчете оптического канала всех приведенных выше факторов – весьма сложная задача. Для этого необходимо составить физическую модель атмосферы. Проблемой составления физической модели атмосферы занимается в частности Институт Оптики Атмосферы СО РАН [5].

Для повышения эффективности разрабатываемых САОС можно предложить следующие рекомендации:

1) При расчете канала связи необходимо учитывать статистику метеорологической дальности видимости (МДВ) для региона, в котором будет применяться САОС.

2) Для борьбы с влиянием атмосферных явлений (дождь, снег, турбулентность) следует использовать:

- несколько лазерных диодов (не менее двух) в источнике излучения, а также несколько приемных оптических антенн в приемнике;
- ИК-светодиод и лазерный светодиод в паре.

3) Для повышения дальности приема в условиях тумана и смога необходимо:

- повышать энерговооруженность луча, т.е. интенсивность светового потока в луче;
- повышать мощность излучателя;
- снижать расходимость лазерного излучения.

4) Для повышения качества приема необходимо включать в состав разрабатываемой САОС:

- систему корректировки эллиптичности пучка лазера;
- оптику, имеющую минимум аберраций, максимум пропускающую рабочее излучение, способную точно фокусировать излучение на чувствительной части фотодиода;
- устройство, позволяющее с высокой точностью корректировать угол расхождения луча;
- систему корректировки чувствительности лавинного фотодиода в зависимости от температуры;
- автоматическую систему корректировки взаимной ориентации приемника и источника.

ЛИТЕРАТУРА

1. *Милинкус Б.М* Атмосферная лазерная связь. Информост – Радиоэлектроника и телекоммуникации. 2001. № 5 (18). с. 17–23.
2. *Гауер Дж.* Оптические системы связи: Пер. с англ._М.: Радио и связь, 1989. 504 с.
3. *Клоков А.В.* Беспроводные ИК-технологии, истинное качество «последней мили». Технология и средства связи. 1999. № 5. с. 40–44.
4. *Зуев В.Е.* Распространение лазерного излучения в атмосфере. М.: Радио и связь, 1981. 288 с.
5. <http://www.iao.ru/> – сайт Института оптики атмосферы.

ПРОГРАММНЫЙ КОМПЛЕКС МОДЕЛИРОВАНИЯ ТЕПЛОВЫХ И ДЕФОРМАЦИОННЫХ ПРОЦЕССОВ ПРИ ИНДУКЦИОННОМ НАГРЕВЕ ОСЕСИММЕТРИЧНЫХ СОПРЯЖЕННЫХ ТЕЛ

А.В. Крахмаль, студент 5 курса ФВС; Е.В. Крохмаль, к.т.н.

ТУСУР, кафедра КСУП, г.Томск

Программный комплекс «Термический анализ» позволяет решать прикладные задачи, возникающие при индукционном нагреве сопряженных осесимметричных тел, а именно: моделирование тепловых процессов при индукционном нагреве; моделирование деформации поверхностей касания сопряженных тел при неравномерном тепловом поле; моделирование усилия прессы, необходимого для разъединения сопряженных тел; оптимизация профиля мощности индукторной системы для разъединения сопряженных тел.

С помощью данного программного комплекса решены практические задачи получения оптимального профиля мощности и компоновки индукторов для разъединения сопряженных осесимметричных тел, а именно, задачи ослабления напряженного состояния перед распрессовкой цельнокатаного железнодорожного колеса и расчета профиля мощности индуктора для съема этого же колеса без использования прессового усилия.

Разработанный программный комплекс успешно эксплуатируется для проведения численных экспериментов и расчета индукторных систем в ФГНУ «НИИ АЭМ», г. Томск. С его помощью был разработан ряд промышленных образцов установок индукционного нагрева для разъединения сопряженных тел, эксплуатируемых на предприятиях РФ.

Комплекс состоит из трех программ: программы управления библиотекой свойств материалов, моделирования тепловых и деформационных процессов и программы локальной оптимизации профиля мощности. «Термический анализ» имеет открытую структуру для модификации и наращивания функциональных возможностей, так как при разработке и реализации была использована СОМ-технология, которая позволяет отключать и менять отдельные компоненты программ комплекса во время выполнения без перекомпиляции или перекомпоновки приложений.

Не смотря на успешное использование данной реализации программного комплекса «Термический анализ» при решении прикладных задач, можно выделить ряд недостатков, основным из которых является – время, затрачиваемое на расчет теплового поля. Этот недостаток обусловлен используемым методом приближенного решения уравнения теплопроводности – явной разностной схемой.

Такое положение дел затрудняет использование методов глобальной оптимизации, требующих большого числа вычислений целевой

функции. Поэтому, в течение преддипломной практики, был рассмотрен метода переменных направлений. Метод реализован в виде расчетного компонента температурного поля программного комплекса.

Для тестирования моделирования теплового поля с помощью разработанного компонента необходимо результаты работы программы сравнить с результатами аналитических расчетов, коммерческих программ и физического эксперимента.

В дальнейшем, после проведения тестирования реализации метода, развитие программного комплекса «Термический анализ» может быть направлено на достижение следующих целей.

- Пополнение программ оптимизации, в частности, целесообразно включение эффективных методов глобального поиска. Это позволит пользователю выбрать наиболее подходящий для решения поставленной задачи метод оптимизации.

- Решение других задач индукционного нагрева, в том числе моделирование нагрева с периодической и методической загрузкой индуктора, моделирование закалки и т.п.

Реализация перечисленных функций значительно расширит возможности комплекса.

БАЗА ДАННЫХ ДОЛЖНИКОВ КРЕДИТНОГО ОТДЕЛА СТРАХОВОЙ КОМПАНИИ ООО «СК КОМЕСТРА-ТОМЬ»

*Д.В. Кригер, студент 5 курса ФВС; А.В. Кригер, программист
информационного отдела компании ООО «СК» Коместра-Томь»
ТУСУР, кафедра КСУП, г.Томск*

Важнейшим отделом страховой компании «Коместра – Томь» является кредитный. При выдаче кредита всегда есть опасение, что клиент не вернет кредит [1]. Конечно, в цивилизованных странах возврата кредита можно потребовать через суд, но во многих ситуациях кредиторы не идут этим путем. А ведь не возврат кредита – это прямые потери компании, которые вполне могут сказаться и на зарплате работников, а то и привести к банкротству компании (либо закрытию всего кредитного отдела, и, как следствие, потери весомой ветви бизнеса).

Кредитные операции – одна из самых доходных статей деятельности компании (после страховых операций[2]). За счет этого источника формируется основная часть чистой прибыли, отчисляемой в резервные фонды и идущей на выплату окладов сотрудникам, расширению компании. Поэтому предотвращение не возврата, уменьшение риска не возврата кредитов – это важнейшая задача кредитного отдела.

Целью моей работы является разработка базы данных должников кредитного отдела.

На сегодняшний день в Томске имеется единственный проект по созданию базы данных должников по кредитам (его можно найти в Интернете <http://blacklist.tsk.ru>), этот проект был реализован в 2004 году компанией «Консультант-Плюс». Тут имеется возможность поиска должников у двух компаний: «Консультант», «Уиллис-Компьютеры», также представлена вся информация о лицах, которые когда-либо нарушали процесс возврата кредита данных компаний. Этот проект имеет ряд недостатков, главный из которых его стоимость. Чтобы зарегистрироваться и пользоваться этой базой данных, юридическое лицо должно заплатить 20 000 рублей, плюс ежемесячные обновления этой базы стоят порядка 5 000 рублей. Даже в том случае, если доступ к этой базе будет куплен, сама база данных останется чужой.

К функциям разрабатываемой базы данных относится:

- ввод и хранение данных должников кредитного отдела страховой компании;
- поддержка большого числа пользователей;
- разделение пользователей на роли по различным критериям (администратор, агент, сотрудник-страховщик, брокер, физическое/юридическое лицо и т.д.);
- возможность выборки данных по различным срезам и построение на основе них визуальных отчетов (графиков, диаграмм);
- возможность сохранения выборок в excel-файл;
- возможность синхронизации (загрузка-выгрузка) данных информационной системы с данными сторонних производителей (например, с программой 1С-бухгалтерия);
- возможность автоматизации нескольких дочерних компаний в одной базе данных.

К особенностям системы можно отнести наличие удобного пользовательского интерфейса, легкость установки клиентского приложения, простота администрирования системы. Регистрация новых пользователей и назначение им необходимых ролей, исходя из их непосредственной деятельности в компании, происходит несколькими нажатиями кнопки мыши.

Сервер Базы данных был выбран Oracle: т.к. уже имеется некоторый опыт по разработке систем, основанных на работе с БД этого типа. Физически база данных Oracle – не более чем набор файлов на диске. Расположение этих файлов несущественно для функционирования (хотя важно для производительности) базы данных.

Логически база данных – это множество пользовательских разделов Oracle, каждый из которых идентифицируется именем пользователя (с паролем), уникальным в данной БД.

Существуют три основные группы файлов на диске, составляющие базу данных.

1. Файлы базы данных
2. Управляющие файлы
3. Журнальные файлы

Наиболее важные из них – файлы базы данных, где располагаются собственно данные. Управляющие и журнальные файлы поддерживают функционирование архитектуры. Для доступа к данным БД все три набора файлов должны присутствовать, быть открытыми и доступными Oracle. Если эти файлы отсутствуют, обратиться к базе данных нельзя, и администратор базы данных должен будет восстанавливать часть или всю БД, используя файлы резервных копий (если их сделали). Все эти файлы двоичные.

В моей работе положено начало разработке базы данных должников кредитного отдела страховой компании «СК «Коместра-Томь», основанной на модульном принципе. Такая база получается гибкой и легкой в поддержке и доработке. Написание новых модулей и внедрение их в общий рабочий процесс системы становятся практически незаметным для пользователя, повышается его скорость работы. Структура базы данных легко читаема и изменяема.

ЛИТЕРАТУРА

1. *Брункевич Ю.А.* Кредитные операции. М.:»Эком», 2004. 198 с.
2. *Алексеева В.П.* Банковское дело. М.: ООО «ТИД «ДС», 2003. 243 с.

РАЗРАБОТКА КОММУНИКАЦИОННОГО ДРАЙВЕРА ДЛЯ КОНТРОЛЛЕРА CONTROLLOGIX 5500

И.В. Кузнецов, студент 5 курса ФВС

ТУСУР, кафедра КСУП, г.Томск

В промышленном производстве, на предприятиях сферы услуг и т.д. зачастую возникают задачи сопровождения некоторого объекта различной индивидуальной информацией, используемой в производственном процессе либо для учета при хранении и транспортировке. В качестве объекта может быть возвратная тара, предмет обработки или сборки в поточном производстве, паллеты, и т.д. В технологическом процессе вышеупомянутые объекты снабжаются какими-либо отмет-

ками, этикетками, паспортами, прикрепленными документами, несущими информацию об индивидуальных качествах объекта (сорт, тип, цвет, вес, размеры и т.д.) либо о пути прохождения объектом технологического процесса (способ обработки, цвет окраски, номенклатура деталей для дальнейшей сборки и т.д.).

В условиях автоматизированного производства рано или поздно возникает необходимость автоматизации этого самого информационного сопровождения, а именно автоматизации закрепления за объектом некоторого набора данных и в дальнейшем считывания и обработки этой информации.

Зачастую для этих целей используется система штрих кодов. Но у нее есть существенные недостатки: малый объем информации, высокая стоимость и большие размеры принтера с автоматическим аппликатором, расходные материалы, загрязнение этикетки

Этих недостатков лишена система радиочастотной идентификации объектов на основе специальных меток (RFID).

Носителем информации в RFID системе является метка со встроенной энергонезависимой памятью (электрически стираемой ПЗУ, статической ОЗУ с батарейной подпиткой) и схемой коммуникации по радиоканалу. Питание схемы коммуникации внутри метки осуществляется от контроллера идентификации посредством электромагнитного поля, наведенного антенной, т.е. в общем случае метка не содержит источника питания, что выгодно сказывается на ее эксплуатационных характеристиках. Внешне метки бывают самыми разными от цилиндра размером со средней величины шуруп или плоской таблетки до этикетки размеров кредитки. Объем памяти от нескольких десятков байт до нескольких килобайт. Контроллер идентификации с антенной осуществляет как чтение, так и запись информации в метке.

На объекте автоматизации, (производство электродов ОАО «Саяногорский Аллюминиевый Завод»), используется автоматическая сортировка с использованием системы RFID OMRON V700.

Управляющий контроллер – отвечает за механическую часть, то есть он посылает команды устройствам, управляющими механизмами направления движения конвейера, исходя из информации передаваемой ему устройствами идентификации.

Однако контроллер не может сам физически подключиться к устройству радиоидентификации используемой в сортировке, так как он не может напрямую посылать команды контроллеру RFID, в виду того, что он не может физически подключиться к данному устройству. Следовательно, необходим модуль, способный работать с устройствами, которые невозможно подключить напрямую к шине Controllogix, и использующими другие протоколы связи. Для этого используется модуль

1756-ADM, модуль позволяет пользователю разрабатывать программы на языке С для поддержки передачи данных на один из трех последовательных портов, также как если бы пользователь передавал численные и символьные данные или команды между Controllogix процессором и 1756-ADM модулем. Иными словами модуль позволяет связываться с устройством (-ми) стороннего производителя подключенного через интерфейсы RS-232, RS422 или RS-485, через команды шины Backplane Controllogix используя драйвер-транслятор написанный пользователем.

Поэтому целью данной работы является разработка и реализация коммуникационного драйвера для контроллера ControlLogix5500, который позволит ему связываться с RFID системой OMRON V700. Применение данного программного продукта позволит автоматизировать процесс сортировки электродов и, соответственно, увеличит производительность производства алюминия.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА В СТРОИТЕЛЬНОЙ КОМПАНИИ

*А.Н. Кунтаев, студент 5 курса ФВС;
Е.Н. Рыбалка, ст. преподав. каф. КСУП
ТУСУР, кафедра КСУП, г.Томск*

С одной стороны в связи с повсеместным развитием компьютерной техники появилась возможность автоматизировать многие процессы. С другой стороны, в связи со стремительным ростом экономики и благосостояния граждан увеличилась потребность в индивидуальном жилье. Строительством такого жилья занимаются множество фирм. Для повышения конкурентоспособности возникает объективная необходимость автоматизировать систему учета в строительной компании [1].

На рынке программного обеспечения для такого рода специализированных фирм в отличие от магазинов компьютерных фирм присутствует не такое большое количество программ [2-4]. Однако, даже существующие системы зачастую не удовлетворяют желаниям и возможностям заказчиков в полной мере. Как правило, такие системы являются либо дорогостоящими продуктами, что препятствует их использованию предприятиями среднего бизнеса, либо узкопрофильными, что идет вразрез с требованиями заказчиков, объединить все лучшее и необходимое в одной программе. Отсюда следует вывод о целесообразности создания собственной программы, менее универсальной, но сравнительно дешевой и лишенной указанных недостатков. Такая программа, как правило, способна удовлетворить потребности заказчиков в полной мере.

Цель данной работы – проектирование и реализация автоматизированной информационной системы учета в строительной компании. Будущая программа должна учитывать все особенности конкретной фирмы, а также требования, предъявляемые, пользователем.

В настоящее время на данном предприятии уже используется подобная программа, но возможности фирмы давно превосходили те, под которые настраивалось программное обеспечение. Для улучшения работы фирмы возникла необходимость разработки более новой программы. Данная программа должна выполнять все основные функции для обеспечения полноценной работы фирмы.

Кроме того, программа должна обладать следующими возможностями.

- Ведение информации по всем поставщикам. Это список всех поставщиков, с которыми работает фирма в данный момент.

- Мониторинг всех объектов с ведением отчетности. Здесь подразумевается ведение материально-технической базы для каждого объекта с возможностью необходимого обновления.

- Возможность приема заказов в цехах. Обслуживание клиентов непосредственно в цехах. Обсуждение всех деталей заказа ведется с главным специалистом в цеху (он также является единственным пользователем программы).

- Разработать клиентское приложение для управления складом.

- Формирование необходимых отчетов, как стандартных, так и с произвольной выборкой.

- Автоматическое формирование бланков договоров.

- Учет оборудования компании. На каких объектах находится то или иное оборудование фирмы.

- Разработать помощник для расчета сметы на строительство и отделку зданий.

- Возможность вывода документов на печать.

Программа должна иметь интуитивно-понятный интерфейс [2-4], сочетающий в себе простоту и функциональную гибкость, а также вобрать в себя основные достоинства аналогичных программ [5].

На данный момент произведен предварительный этап проектирования информационной системы – выявлены требования и информационные потребности будущих пользователей, описана логика взаимосвязей сущностей. Последующие этапы предусматривают непосредственное создание кода, тестирование, внедрение системы, а также составление сопроводительной технической документации.

ЛИТЕРАТУРА

1. Мартин Дж. Организация баз данных в вычислительных системах. С-П.: Парус, 1999. 125 с.

2. Александровский А.Д., Шубин В.В. Delphi – опыт практического применения. Москва: Издательство ДМК, 2000. 240 с.
3. Андерсен В. Microsoft Access – Проблемы и решения. Москва: Издательство Эком, 2001. 384 с.
4. Харитонова И. Office Access 2003. СПб.: Питер, 2004. 464с.
5. Кренке Д. Теория и практика построения баз данных. 8-е изд. СПб.: Питер, 2003. 800 с.

АЛГОРИТМЫ И ПРОГРАММЫ ТИПОВОГО РЕШЕНИЯ ЗАДАЧ УПРАВЛЕНИЯ СПРАВОЧНИКАМИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

А.В. Ледовских, студент 5 курса ФВС;

А.Я. Клименко, д.т.н., профессор каф. КСУП

ТУСУР, кафедра КСУП, г.Томск

Цель работы: типовое решение задачи управления справочниками автоматизированных систем обработки информации, то есть разработка программного продукта который позволял бы отображать плоские таблицы на древовидную структуру. В процессе выполнения работы были изучены пакеты BP Win 4.0, Rational Rose, ER Win. Результатом работы является разработанная: функциональная модель, модель прецедентов, логическая модель, модель диаграммы классов. Был разработан программный продукт, являющийся инструментом для работы со справочниками. То есть предоставляет пользователю следующие функциональные возможности: редактирование данных, экспорт, импорт данных, навигацию по справочникам. Реализована возможность отображения плоских таблиц на древовидную структуру. На этапе моделирования были определены требования к системе, введены ограничения на функциональную модель, разработан и реализован интерфейс программного продукта.

Интерфейс пользователя, который осуществляет передачу информации от пользователя к программе, реализовывался в среде разработки Delphi. Данный выбор обосновывается на следующих преимуществах данной среды:

Delphi – язык и среда программирования, относящаяся к классу RAD – «Средство быстрой разработки приложений»); Delphi сделала разработку мощных приложений Windows быстрым процессом, а также кнопки, объекты с данными, меню и построенные диалоговые панели с помощью которых можно обеспечить ввод данных просто несколькими нажатиями кнопок мыши, не прибегая к программированию.

В ходе работы применялись различные паттерны проектирования для конкретного отображения узлов древовидной структуры на плоские таблицы.

КОМПЬЮТЕРНЫЙ ТРЕНАЖЕР ДЛЯ ОБУЧЕНИЯ ОРИЕНТИРОВАНИЮ ПО СРЕДСТВАМ ЛАЗЕРНОЙ НАВИГАЦИИ

О.Ю. Линник, студентка 5 курса ФВС;

И.А. Столбов, аспирант ТУСУРА

ТУСУР, кафедра КСУП, г.Томск

Современная информационная революция радикально меняет не только материальное, но и духовное производство – производство знаний. Физическим носителем информационных технологий, их инструментом является компьютер, без использования которого невозможно представить сколько-нибудь содержательного интеллектуального труда. Владение компьютером рассматривается как обязательное качество готового к труду специалиста во многих сферах человеческой деятельности. Необходимым требованием, предъявляемым сегодня к специалистам в области экономики, техники, ряда других отраслей человеческой деятельности, является профессиональное владение персональным компьютером, что в свою очередь требует глубоких знаний в области компьютерных технологий, определенных навыков и специфического стиля мышления.

Тренажерная подготовка специалистов нашла применение в авиации, судовождении, ракетно-космической технике, т.е. в тех областях, где обучение на натурном объекте связано с большими затратами, а подчас и с опасностью возникновения аварийных ситуаций.

Применение тренажеров, т.е. объектов, в той или иной степени воспроизводящих натурный объект эксплуатации, позволяет обучающемуся персоналу получить навыки эксплуатации и наиболее эффективного использования оборудования, что дает возможность в дальнейшем, в условиях нормальной эксплуатации избежать многих осложнений и аварийных ситуаций.

Судовождение на внутренних водных путях, при современных габаритах судов «река-море» и пассажирских, требует искусства почти ювелирного. Особенно в узких фарватерах, при входах в шлюз. Сейчас достижения электроники, космической и оптоэлектронной техники предоставляют судоводителям целый арсенал навигационных средств для безопасности плавания. Характерная черта – универсальность этих систем, возможность использования и на реке, и на море. Это относится к спутниковой навигации, к маякам.

Маяк – не просто источник света, а источник узкого луча, в границах которого должен держаться ведущий судно моряк или производящий посадку пилот. А чтобы яркость такого луча была достаточной, понадобились мощные энергоемкие лампы и громоздкие фокусирующие системы. Поэтому весьма полезным для навигации стало появление лазеров, способных в отсутствие фокусирующих систем создавать узкий и яркий луч.

Преимущества лазерных средств навигационного оборудования (ЛСНО) по сравнению с основанными на традиционных источниках света хорошо известны: узкая спектральная полоса лазерного излучателя значительно увеличивает заметность излучения на фоне других огней и обеспечивает большую дальность видимости, особенно днем, в сумерках и при других неблагоприятных условиях. Эффективность внедрения маяков определяется уменьшением потерь от аварий, связанных с плохой видимостью существующих средств навигации, так и от простоя судов из-за плохих метеоусловий.

Компьютерный тренажер обучения ориентированию поможет обеспечить высокую подготовку персонала, тем самым уменьшить число аварий и катастроф. Аналогов данной разработки еще не существует, но правительство выделило более 1000000 евро на разработку и внедрение таких тренажеров.

Существует не мало способов построения маяков. Самый распространенный двухцветный двухпостовой маяк изображен на рис. 1.

При таком построении образуются три зоны ориентирования. В I зоне судоводитель наблюдает проблески зеленого цвета только левого маяка, во II – проблески красного цвета правого маяка, в III – центральной зоне проблески обоих маяков. При этом если судно находится на оси створа, проблески в центральной зоне наблюдаются одновременно, при смещении от заданного направления синхронность следования огней нарушается и первым наблюдается проблеск маяка, в сторону которого произошло смещение. Т.о. направление следования огней указывает на направление смещения от осевой линии створа, а временной интервал между проблесками позволяет судить о величине отклонения от заданного курса следования.

Алгоритм определения положения корабля в конусе маяков.

$$k_1 = \operatorname{tg} \alpha_1, k_2 = \operatorname{tg} \alpha_2.$$

Y задается по условию (расстояние до маяков).

Проверка попадания корабля в конус зеленого маяка:

Если $(Y > k_1 \cdot gx)$ и $(Y > k_2 \cdot gx)$, то корабль в зеленом конусе.

И возможно его пора зажечь.

Красный маяк работает аналогично и одновременно с зеленым.

Условия для зажигания маяков.

1. Маяк еще не зажигался за данный проход луча.
 2. Угол обзора корабля с маяка меньше угла сканирующего луча.
- Если условие выполнилось, то зажигается маяк на 100 мс.

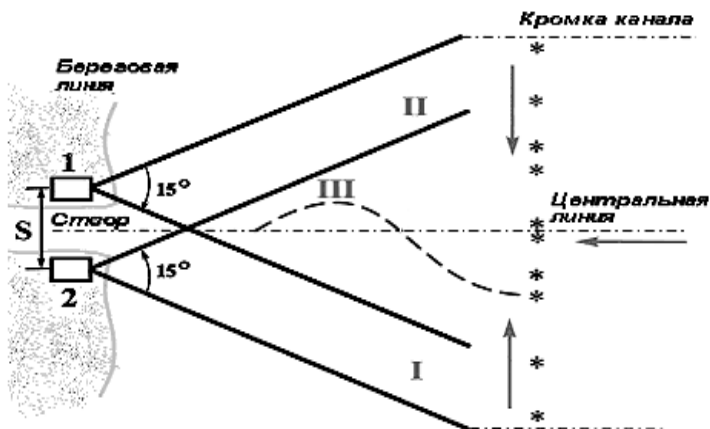


Рис. 1. Схема формирования двухцветного двухпостового маяка

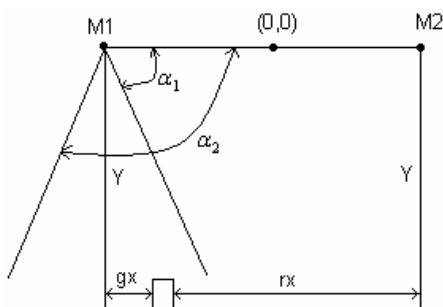


Рис. 2. Положение корабля в конусе маяков

Угол сканирующего луча определяется с помощью функции, которая возвращает угол сканирующего луча маяков на данный момент времени. Для определения момента времени вызывается функция операционной системы TimeGetTime, которая возвращает время работы ОС в миллисекундах.

$$f(t) = \frac{\text{mod} \frac{t}{T} \cdot \alpha}{T} - \frac{\alpha}{2},$$

α – угол раствора маяков, t – время (мс), T – период сканирования (мс).

ЛИТЕРАТУРА

1. Зуев В.Е., Пересыпкин В.И., Фвдеев В.Я. Лазерные навигационные устройства. Москва: «Радио и связь», 1987. 162 с.
2. Зуев В.Е., Пересыпкин В.И., Фвдеев В.Я. Лазерные устройства для обеспечения судовождения. Новосибирс: Наука, 1985. 128 с.
3. Олихов И.М. Мобильная лазерная трехцветная навигационная система – надежность в экстремальных ситуациях. Электроника: НТБ, 1999. №3.

РАЗРАБОТКА ПРОГРАММЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ТРАНЗИСТОРНЫХ СВЧ-УСИЛИТЕЛЕЙ НА ОСНОВЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ

*И.Г. Лощилев, студент 2-го курса ФВС; А.В. Нефедьев, инженер;
Л.И. Бабак, к.т.н., доц. каф. КСУП*

ТУСУР, кафедра КСУП, г. Томск. E-mail: cursor@ms.tusur.ru

Рассматривается разработка новой версии программы структурного синтеза транзисторных СВЧ-усилителей GeneAmp. Реализован новый интерфейс и расширены функциональные возможности программы.

Проектирование транзисторных СВЧ-усилителей является длительным и трудоемким процессом, требующим опыта разработчика. Повысить эффективность проектирования позволяет применение программ структурного синтеза усилителей на основе генетических алгоритмов (ГА).

В [1] была описана первоначальная версия программы автоматизированного проектирования СВЧ-транзисторных СВЧ-усилителей GeneAmp, реализованная в среде Visual C++. Программа позволяет выполнить структурный синтез (определение схемы и значений элементов) СВЧ-усилителей по заданным требованиям к характеристикам.

В основе программы лежит ГА. Проектировщик задает структурную схему усилителя, требования к характеристикам, ограничения на топологии корректирующих (КЦ) и согласующих цепей (СЦ), диапазоны номиналов элементов. Результатом работы программы является принципиальная схема усилителя.

Испытания программы показали хорошие результаты, однако она имела следующие недостатки:

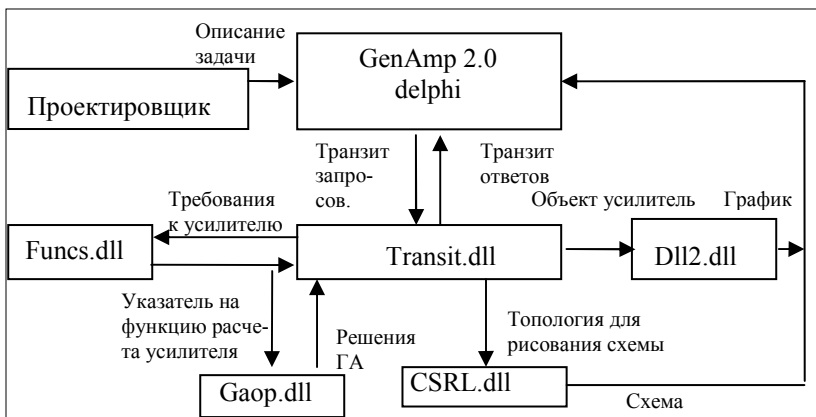
1. Неудобный интерфейс не давал возможности разработчику наглядно задавать требования к топологии усилителя, КЦ и СЦ.

2. Реализация программы в виде однооконного приложения ограничивала функциональные возможности и, в частности, не позволяла проектировщику одновременно наблюдать таблицы, графики характеристик и схемы синтезированных усилителей.

В связи с этим была начата разработка новой версии программы, свободной от указанных недостатков. Однако создание качественного интерфейса на Visual C++ является достаточно сложной задачей и требует большого количества времени, которое превышает время, затрачиваемое на написание собственно алгоритмов проектирования.

Для преодоления указанной трудности было решено написать интерфейс новой версии программы на языке Delphi 7, который является удобным для такого рода задач. Так как язык Delphi 7 сильно уступает C++ в скорости выполнения вычислительных алгоритмов, расчетная часть программы, реализованная на C++, была взята из первоначальной версии и преобразована в dll-библиотеки, которые вызываются во время работы программы. На рисунке и в таблице приведено краткое описание распределения задач между dll-библиотеками.

Описанный комбинированный принцип построения программы позволил в сравнительно короткие сроки реализовать новую более функциональную версию. Однако, в процессе работы стали видны некоторые недостатки этого подхода, такие как сложность в отлавливании ошибок и нахождении причин явлений, связанных с невозможностью использовать функцию debug (приходится использовать отчеты о работе отдельных модулей в текстовых файлах). Эти сложности являются платой за скорость разработки.



Блок-схема связей главной программы и модулей

Краткое описание модулей

Название	Назначение модуля
Transit.dll	Реализует связь Delphi и C++
Gaop.dll	Классический и мутационный ГА [2]
Funcs.dll	Модуль расчета характеристик усилителя
CSRL.dll	Рисование принципиальной схемы по описанию
DLL2.dll	Графики характеристик усилителя

При создании новой версии программы *GeneAmp* были выполнены следующие работы:

1. Реализован новый интерфейс как программы в целом, так и диалогов задания топологии усилителя в частности. В верхней его части изображен диалог, который позволяет проектировщику быстро и наглядно задать топологию СВЧ-усилителя.

2. Программа реализована как многооконное приложение, проектировщик может выбрать любое из полученных решений в таблице результатов и просмотреть его схему и графики характеристик.

3. В разработанной программе наряду с классическим ГА использован новый более эффективный мутационный ГА [2].

Испытания новой версии программы показали ее эффективность [2].

ЛИТЕРАТУРА

1. *Нефедьев А.В., Бабак Л.И.* Программа автоматизированного проектирования транзисторных СВЧ-усилителей при помощи генетических алгоритмов. В сб. «Научная сессия ТУСУР-2005». Томск. 2005. с. 300–303.
2. *Лощилов И.Г., Бабак Л.И.* Автоматизированный структурный синтез транзисторных СВЧ-усилителей с использованием мутационного генетического алгоритма. В наст. сборнике.

АВТОМАТИЗИРОВАННЫЙ СТРУКТУРНЫЙ СИНТЕЗ ТРАНЗИСТОРНЫХ СВЧ-УСИЛИТЕЛЕЙ С ИСПОЛЬЗОВАНИЕМ МУТАЦИОННОГО ГЕНЕТИЧЕСКОГО АЛГОРИТМА

И.Г. Лощилов, студент 2-го курса;

Л.И. Бабак, к.т.н., доц. каф. КСУП

ТУСУР, кафедра КСУП, г. Томск. e-mail: cursor@ms.tusur.ru

На примере задачи структурного синтеза транзисторных СВЧ-усилителей дан сравнительный анализ работы классического и мутационного генетических алгоритмов.

Одним из эффективных подходов к проектированию транзисторных СВЧ-усилителей является структурный синтез на основе генетических алгоритмов (ГА). В [1] описана новая версия программы автома-

тизированного проектирования СВЧ-усилителей *GeneAmp*, в которую включены как классический, так и мутационный [2] ГА. В настоящей статье описаны особенности реализации и дан сравнительный анализ работы этих алгоритмов применительно к задаче синтеза транзисторных СВЧ-усилителей.

Начальным этапом при проектировании является задание ограничений на топологию, характеристики и значения элементов усилителя. Далее в процессе работы ГА генерируются бинарные строки (особи), соответствующие различным решениям (схемам усилителя). В эти строках бинарно закодированы переменные, описывающие типы, способы включения и значения элементов усилителя. В принципе длина переменной не ограничена, как и длина бинарной строки, это зависит от способа кодирования. Далее проверяется соответствие бинарных строк (решений) поставленным ограничениям.

Общее описание классического и мутационного ГА приведено в [2]. В интерфейсных формах отражены основные параметры этих алгоритмов. Отметим, что мутационный алгоритм в качестве составной части включает в себя классический ГА. В процессе работы мутационного алгоритма классический ГА может срабатывать с вероятностью *Crossover probability* в каждом поколении.

В мутационном ГА также поддерживаются многоточечный и универсальный кроссоверы. Новыми и наиболее интересными являются параметры *MaxVariable* и *Freq (%)*. В [2] был описан мутационный алгоритм, в котором всего одна особь, и все ее переменные подвергаются мутации в каждом поколении. В данной же реализации параметр *PopNum* определяет количество популяций, а *PopSize* – количество таких вот мутируемых особей-индивидуальностей, которые находятся в каждой из популяций. Эти особи, как и раньше, мутируют в каждом поколении, однако теперь их несколько и иногда с вероятностью *Crossover probability* они могут скрещиваться, именно тогда и вызывается классический ГА. Также возможны миграции между популяциями с вероятностью *migr prob*.

Рассмотрим, как выглядит мутация для особи-индивидуальности. К примеру, пусть в нашей бинарной строке закодировано 40 переменных, тогда значение параметра *Max Variable=20* означает, что мы находим некоторое случайное значение *k*, лежащее в диапазоне от 1 до 20. Это *k* – количество переменных, которые подвергнутся мутации. Причем количество точек мутации в переменной тоже определяются величиной, которая именуется *Freq*. Точнее, количество точек мутации для переменной равно случайному *z* из диапазона 1... *Freq* (в нашем примере *z = 1*). Таким образом, в данном случае выберется не более чем двадцать переменных (переменная может выбираться более 1 раза), в каждой из которых будет инвертирован один бит.

Тестирование алгоритмов было выполнено в программе *GeneAmp* на примере структурного синтеза однокаскадного усилителя на полевом СВЧ-транзисторе диапазона 2–10 ГГц. Требования к характеристикам усилителя приведены в табл. 1.

Таблица 1

Требования и характеристики усилителя

Характеристики	G , дБ	ΔG , дБ	F , дБ	$ S_{11} $, дБ	$ S_{22} $, дБ
Требования	12,00	1,00	2	–9,63	–9,63
Визуальное проектирование	12,10	0,59	1,90	–10,55	–10,82
Генетический алгоритм	11,87	0,27	2,04	–10,10	–19,90

Для ГА были заданы следующие параметры:

1. Мутационный ГА: 4 популяции по 20 хромосом, вероятность миграции 30%. Панмиксия. Двухточечный кроссовер. Вероятность подключения классического ГА (кроссовер) 30%. Вероятность мутации в нем 3%. Max Variable =3. Freq=1;

2. Классический ГА: 10 популяций по 50 хромосом, вероятность миграции 100%. Панмиксия. Двухточечный кроссовер. Вероятность мутации 3%.

Для мутационного ГА большое количество хромосом в популяции было взято для стабильности, так как при их малом числе увеличивается вероятность «застревания» в локальных экстремумах.

Таблица 2

Результаты сравнительного тестирования ГА

Всего тестов: 10	Классический ГА	Мутационный ГА
Положительных ($\Phi > 1e-18$)	6	10
Отрицательных ($\Phi < 1e-18$)	4	0
Среднее время работы (сек.)	11 (6 результатов)	3,3
Среднее кол-во вычислений целевой функции	~45,000	~12,500

Результаты сравнения ГА приведены в табл. 2. Успешность синтеза оценивалась по величине целевой функции Φ , которая при выполнении всех требований к характеристикам усилителя является положительной, а в противном случае – отрицательной. Из таблицы видно, что мутационный ГА превосходит классический как в скорости (примерно в 3–4 раза), так и в качестве (вероятности) нахождения решения.

В табл. 1 и на рис. 1 приведено сравнение результатов проектирования усилителя с помощью «визуальной» методики и мутационного ГА. При близких полученных характеристиках усилителей время проектирования с использованием интерактивного визуального подхода составляет около 1 дня, а с помощью ГА – несколько секунд.

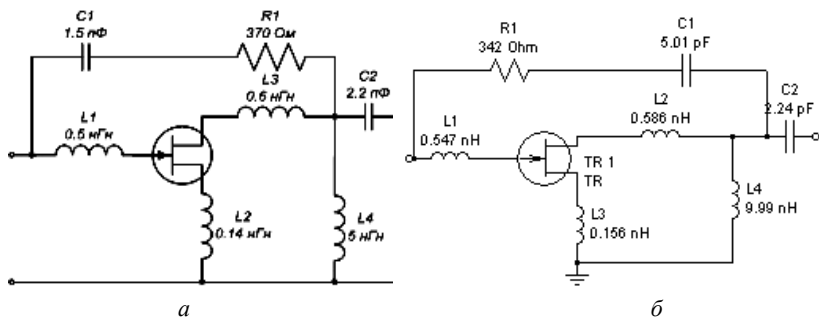


Рис. 1. Схемы усилителей, спроектированных визуальным методом (а) и ГА (б)

Недостатком мутационного ГА является большее количество настроек, некоторая сложность в их подборе для каждой новой задачи. Однако путем нескольких перезапусков эти недостатки обычно окупаются найденным хорошим решением за более короткое время.

Следующим этапом в разработке данной программы может быть добавление еще одного ГА, который будет использовать кодирование в реальных числах. Авторы считают, что такой алгоритм может дать ощутимый эффект и улучшить характеристики усилителей.

ЛИТЕРАТУРА

1. Лоцилов И.Г., Бабак Л.И., Нефедьев А.В. Разработка программы автоматизированного проектирования транзисторных СВЧ-усилителей на основе генетических алгоритмов. В наст. сборнике.
2. Лоцилов И.Г., Бабак Л.И. Генетические алгоритмы бинарного кодирования, основанные на мутации. В сб. «Электронные средства и системы управления», Ч. 2, Томск, 2005, с. 132–136.

АВТОМАТИЧЕСКАЯ ОПТИЧЕСКАЯ ЛОКАЦИОННАЯ СИСТЕМА

П.В. Максименко, студент 5 курса ФВС
ТУСУР, кафедра КСУП, г. Томск

В последнее время активно ведется внедрение атмосферных оптических систем связи (АОСС) в различные сферы деятельности, в том числе и в военную сферу. Такие средства связи используются для формирования линий связи между участками, разделенными водными преградами, железнодорожными развязками, в зонах с активными радиопомехами. АОСС

Предполагается, что при развертывании воинских подразделений на новом месте дислокации часть АОСС (центральные или штабные) будут устанавливаться в центральной (штабной) зоне, а остальные

АОСС (периферийные терминалы) будут устанавливаться каждый в своем строго выделенном секторе на удалении около двух километров от центральных терминалов.

В зонах с активными радиопомехами задача обнаружения периферийных терминалов и наведение на них центральных терминалов является сложной задачей.

Для решения этой задачи предлагается использовать автоматическую оптическую локационную систему. Система работает по принципу сканирующего лазерного дальномера, измеряющего расстояние по времени распространения светового импульса до цели и обратно [1]. В качестве цели выступают уголкового отражатели, закрепленные на терминалах периферийных АОСС. Излучатель и приемник жестко закреплены в корпусе локатора. Приемная часть системы состоит из приемного зеркала, фотодатчика ФД2 и оптического фильтра, отсекающего фоновое излучение. В верхней части корпуса на подвижной платформе находится стойка, на которой установлено сканирующее зеркало. При помощи двух электроприводов зеркало может вращаться по азимуту и углу места. Стойку со сканирующим зеркалом вращает шаговый двигатель ШДА (вращение по азимуту), на валу у которого установлен датчик угла поворота ДА. Шаговый двигатель ИПДУ вращает зеркало по углу места. Значения угла поворота зеркала по углу места отслеживаются датчиком ДУ, закрепленным на оси зеркала. Сигналы с датчиков угла поступают на микроконтроллер, который с помощью Н-мостов управляет работой электродвигателей.

Работает локатор следующим образом.

Лазер генерирует импульсы, которые подаются на качающееся (сканирующее) зеркало, осуществляющее развертку по вертикали. Смещение по горизонтали производится с помощью поворота стойки. В результате получаем сканирование заданной области по пилообразной траектории. Как только система получит отраженный сигнал от уголкового отражателя АОСС, микроконтроллер запомнит показания с датчиков угла поворота по азимуту и углу места ДА и ДУ, пересчитает их в относительные координаты и передаст в центр управления и наведения АОСС. Расстояние до цели определяется по временному интервалу между моментом прихода импульса от фотодатчика ФД1 и моментом прихода импульса от ФД2.

Разработанная оптическая локационная система позволит автоматизировать процесс установления связи между центральными и периферийными терминалами АОСС.

ЛИТЕРАТУРА

1. *Протопопов В.В.* Инфракрасные лазерные локационные системы. М.: Воениздат, 1987. 174 с.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА RSA

*М.М. Медведева, студентка 5 курса ФВС,
Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС
ТУСУР, кафедра КСУП, г. Томск, e-mail: poohy@ngs.ru*

Поскольку целью работы является оптимизация криптоалгоритма RSA на основе возможностей современных технологий, то первым шагом в работе стал выбор среды разработки программного обеспечения (ПО) и непосредственная программная реализация самого алгоритма.

В данный момент существует много средств разработки ПО. Для того чтобы сделать правильный выбор программной платформы остановимся на 3-х критериях, важных при реализации криптографического программного продукта. Это, во-первых, возможность работы программ, разработанных в данном средстве разработки, в семействе операционных систем Windows, во-вторых, возможность быстрой и удобной визуальной разработки программного обеспечения с удобным интерфейсом, и, в-третьих, наличие криптографических библиотек, ориентированных под данное средство разработки.

Этим условиям отвечают интегрированные среды разработки Visual C++, C++ Builder и Borland Delphi, из которых и будет сделан выбор среды разработки ПО.

Ориентация направлена на существующие программные криптографические библиотеки функций и процедур. На сегодняшний день распространены две общедоступные библиотеки, содержащие набор данных функций. Это Openssl, создаваемая в рамках проекта Openssl и реализованная на C+Assembler, а также библиотека Fgint, реализованная на языке Pascal. При сравнении этих библиотек предпочтение было отдано библиотеке FGInt, поскольку данная библиотека обладает большим набором функций, чем Openssl, что обусловило и выбор среды разработки. Можно также отметить, что библиотека FGInt реализована гораздо проще и не так громоздко, как Openssl, что позволяет легче модифицировать и оптимизировать функции и процедуры данной библиотеки под собственные нужды, создавать на их основе собственные функции и процедуры, и таким образом, позволяет уменьшить время и трудозатраты на разработку приложений.

В качестве языка программирования выбран Delphi 7.0 т.к он обладает мощными встроенными средствами визуального программирования на платформе Windows и позволяет создавать удобный пользовательский интерфейс. Так же Delphi 7.0 поддерживает Object Pascal, в котором реализована библиотека FGInt, что делает возможным под-

ключение данной библиотеки к проекту Delphi в качестве модуля. В Delphi много встроенных средств, интегрирующих приложения, созданные средствами данной среды разработки в сеть Интернет, а также разного рода компьютерные сети, что делает возможным создать защищенные коммуникации в сети Интернет, а также в локальных сетях, VPN-сетях и т.д.

При этом библиотека FGInt в Delphi 7.0 содержит набор функций для работы с большими числами, разрядность и размер которых превышает стандартный набор типов данных, реализованных в Delphi 7.0. Библиотека также содержит набор функций для работы с большими числами в конечных полях Галуа, такие, как сложение, умножение, деление по некоторому модулю, возведение в степень по модулю, тесты чисел на простоту и др., причем данные функции специально оптимизированы программистами-разработчиками для ускорения вычислений.

Программа реализации криптоалгоритма RSA состоит из следующего набора программных модулей:

1. FGInt – модуль с библиотекой функций для работы с большими числами в конечных полях.
2. FGIntPrimeGeneration – модуль, содержащий реализацию процедуры поиска простых чисел, используемую в программе.
3. FGIntRSA – модуль, содержащий реализацию процедур шифрования и дешифрования данных.
4. fInfo – модуль получения информации о системе, процессоре и памяти компьютера.
5. main – модуль с основной программой, с обработчиками событий главной формы.

Данные модули находятся в файлах
FGInt.pas, FGIntPrimeGeneration.pas, FGIntRSA.pas, fInfo.pas, main.pas соответственно вышеуказанному списку.

Разработанное ПО, позволяет зашифровывать и расшифровывать данные с использованием открытого (закрытого) ключей заданной пользователем длины, позволяет получать данные о системе, процессоре и памяти компьютера, а также реальное время шифрования и дешифрования с возможностью сохранения полученных данных в файлы для дальнейшего исследования.

Программа имеет удобный и интуитивно понятный интерфейс, удобна в обращении, занимает 1Мб памяти жесткого диска и требует минимальное количество ресурсов аппаратуры.

Для функционирования программы необходимо иметь на компьютере 64 МБ оперативной памяти, 1 МБ свободной памяти на жестком диске, процессор архитектуры Intel с тактовой частотой не менее 200 МГц, ОС Windows 95/98/Me/2000/NT/XP.

Программа включает в себя основной программный файл Pmain.exe, при запуске которого можно начинать работу, Pmain.ini, в котором хранится текущая конфигурация программы, Pmain.res – файл ресурсов программы. Также существуют специальные папки: Parameters (для хранения файлов с параметрами открытого ключа), Okey (для хранения открытых ключей), Secretkey (для хранения закрытых ключей отправителя) и System (для хранения информации о системе).

Для осуществления шифрования необходимо осуществить следующие шаги:

- выбрать размер ключа (от 64 бит до 4096 бит);
- сгенерировать или выбрать открытый и закрытый ключи шифрования;
- выбрать исходный файл, в котором хранится информация для шифрования, и файл результат (выходной файл), в который сохранится результат шифрования данных;
- зашифровать данные;
- пересылать получившийся выходной зашифрованный файл получателю.

Для расшифрования данных необходимо сделать следующее:

- выбрать полученный дешифруемый файл;
- выбрать файл результат (выходной файл);
- загрузить закрытый ключ;
- осуществить процесс дешифрования файла.

На рис. 1 приведена главная форма программной реализации криптоалгоритма RSA (вкладка «Генерация ключей»).

Рис. 1. Вкладка «генерация ключей».

Результаты испытаний алгоритма RSA

№ компьютера	Чистое время шифрования, мс	Чистое время дешифрования, мс	Открытый и закрытый ключи соответственно:		
			p=		
			e=		
			d=		
1	1108	2985	6020289604716651497464253063099684707741887148646800827280396519721042294323765537	12911971967575148915628963952413013755788509473121222860072938905875537894881	37967283677246504686641748906019847616720254123200644930584719888553804686123965537
2	1764	4515	3760868092466070450657505005540376379078911850332228590411515408966117164510093577771557324677938414857333935106926060509377311965293030160458296485680819965537	3491227896757514562362896395241301375578850965313332286007293890587553780065234352638139486140900889718250040898887443607567150339470950721649699791671471	9708713155310165277114902443310763830910131818310186998571042683372161949985
4	2532	6560	6012586770471756125310867357762633316848764615290026463196446309210851029830365537	277762297729226068403973053578316807756515634225206048692342046466170342261133869780586363430686941127745787421987729243483371417860764177254861572788441165537	36918992723646164324226155215085272014632720623696391281230844907463690721649387122864112932440826358254255544800331387950706786240969173448951082456839365537
7	1031	2530	363583724184494523440841056603044529880182551964471963994324010245499823413135055208284077474949274623956040026694157733170981779993704599095938438228351965537	21459778395611552338948885832581531448936889012887222891416130311990500242225693558623521472430877812074897799301944800849919144871010699951717052587054765537	119002498154329321582039148545441129666870596149205416708068127947287590612333809885520005831690440181182754595031496727733495538311059669891439888390257165537
10	2714	7050	2378874915912517182728880696087718132997850092348922505089163237334780473328		

Алгоритм шифрования данных RSA был реализован программно с той целью, чтобы в последствии оптимизировать его работу, используя возможности современных технологий, и сравнить быстродействие оптимизированного алгоритма с быстродействием реализованного в данной работе алгоритма RSA. Поэтому с целью сравнения были проведены испытания, результаты которых обобщены и сведены в таблицы

Испытания проводились следующим образом: производились операции шифрования и дешифрования с ключом фиксированной длины 128 бит на десяти компьютерах разной конфигурации, засекалось время выполнения операций, а также сохранялась в файл log.txt информация о системе компьютеров.

Для последующего сравнения быстродействия алгоритмов RSA (реализованного и оптимизированного) будет использована программа, в которой будет реализован криптографический оптимизированный алгоритм RSA, на той же самой программной платформе, с использованием тех же криптографических библиотек, что и в настоящей работе, поэтому и результаты экспериментов будут объективными.

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ IP-СЕТИ

Д.С. Момот, студент 5 ФВС

ТУСУР, каф.КСУП, г.Томск, dsmomot@yandex.ru

В настоящее время существует небольшое число различных программных продуктов, которые позволяют виртуально (на одном локальном компьютере) проектировать сеть. Происходит это чаще всего графически. В интерфейс программ входят модели различных типов сетевых устройств: маршрутизаторов, коммутаторов, сетевых карт, серверов и т.д. Также для организации связи между данными приборами в программах предусмотрены всевозможные виды соединительных кабелей: коаксиальный кабель, UTP-5, оптоволокно и т.д. Построив в окне программы из имеющихся элементов сеть, пользователь может проверить ее работоспособность. В программах для этого предусмотрены различные средства анализа качества работы сети. Такое моделирование позволяет минимизировать затраты на этапе проектирования и оценить стоимость реализации информационной системы.

На сегодняшний день практически любое образовательное учреждение не в состоянии позволить использование подобных программных продуктов в учебных целях. Так как стоимость таких комплексов составляет от нескольких тысяч до десятков тысяч долларов. Разработка программы имитационного моделирования IP-сетей направлена на использование ее в учебных учреждениях.

Программа предоставляет пользователю графический интуитивно-понятный интерфейс. Моделируемая сеть может состоять из следующих компонентов: маршрутизатор, коммутатор, компьютер (сетевая

карта), линия связи (UTP-5). После того как выстроена топология компьютерной сети, нужно произвести настройку. Необходимо задать IP-адрес для каждого хоста (компьютеры и порты маршрутизатора), определить тип маршрутизации (статический или адаптивный) и, если потребуется, вручную прописать таблицу маршрутизации. Для всех портов сетевых устройств есть возможность определить пропускную способность (по умолчанию задано значение 100 Мбит/с). Длина сетевого кабеля также является программно задаваемым параметром.

Имитация работы сети происходит, начиная с третьего (сетевого) уровня модели взаимодействия открытых систем (модели OSI). Единицей передаваемой информации является пакет. Моделирование произведено с использованием теории систем массового обслуживания. Заявками в данной системе являются сетевые пакеты, а обслуживающими приборами – маршрутизаторы, коммутаторы и компьютеры. Причем маршрутизаторы и коммутаторы имеют очередь заявок на каждом выходе порта, а компьютеры только одну очередь на выходе сетевой карты. Для каждой очереди заявок определена переменная, в которой записывается модельное время окончания обслуживания заявки, стоящей первой. Значение данной переменной зависит от времени момента поступления заявки в очередь, а также от характеристик выпускающего порта, порта приемника, длины соединяющего их кабеля и коэффициента вероятности передачи пакета.

Для проверки работоспособности сети реализованы сетевые команды. Например, команда `ping`. Ее можно вызывать с любого компьютера или консоли маршрутизатора. Также на каждом порту ведется статистика полученных и отправленных пакетов.

Результатом проведенных исследований стала программа, позволяющая графически создавать сети с различной топологией, наглядно демонстрировать работу IP-сети, изучать принципы маршрутизации. Программа будет полезна при проведении лабораторных работ в высших учебных заведениях по теме компьютерных сетей. В основу работы программы положено моделирование передачи сетевого пакета, что в будущем дает возможность расширения ее функциональных возможностей.

ПРОГРАММНЫЙ МОДУЛЬ «МЕНЕДЖЕР СМК» ДЛЯ ОРГАНИЗАЦИИ УПРАВЛЕНИЯ И ВЗАИМОДЕЙСТВИЯ ПРОЦЕССАМИ СМК В ИОА СО РАН

А.В. Николаев, студент 5 курса ФВС ТУСУР;

О.Е. Аркатова, зам. руковод. СлК в ИОА СО РАН

Институт оптики атмосферы, СО РАН

Создание систем эффективного управления организациями самого разного характера и сферы деятельности – одна из проблем, стоящих

перед современным динамичным менеджментом. Универсального алгоритма для создания таких систем управления не существует, однако возможна разработка общих принципов построения систем управления бизнесом. В число наиболее передовых методов построения систем эффективного управления входит так называемый процессный подход к управлению. Последний заключается в выделении в организации сети процессов и управления этими процессами для достижения максимальной эффективности деятельности организации.[1]

Цель системы управления процессами СМК заключается в способности организации устанавливать и понимать все виды ее деятельности и взаимосвязи между выполняемыми действиями. Это дает возможность организации определять и контролировать свою деятельность.

Для правильно применения процессного подхода необходимо их правильно описать (идентифицировать). Необходимо четко определиться, какие потребности организации реализуются настоящим процессом. Когда он начинается, когда он заканчивается, а также четко осознавать место процесса в сети процессов в организации.

Сеть процессов – это совокупность взаимосвязанных и взаимодействующих процессов предприятия, включающих в себя все виды деятельности, осуществляемой на предприятии [2].

Процесс – это устойчивая, целенаправленная совокупность взаимосвязанных видов деятельности, которая по определенной технологии преобразует входы в выходы, представляющие ценность для потребителя [2].

На вход процесса СМК поступают входящие ресурсы (материальные и нематериальные потоки), которые используются в ходе выполнения процесса при помощи ресурсов (персонал, инфраструктура, др.) для получения результатов. По ходу процесса определяются точки контроля (входы, внутри процесса, выходы), где осуществляется сбор данных с проведением необходимых измерений (т.е. проведение мониторинга продукции, процесса, удовлетворенности потребителя) с последующей передачей этих данных в подсистему анализа данных [3]. На рисунке приведен графический облик процесса.

В ИОА СО РАН идет процесс создания программы управления и взаимодействия процессами СМК.

Создаваемая программа поможет решить задачи, определенные стандартами ИСО.

- Определить и систематизировать перечень процессов организации.
- Классифицировать процессы, их аспекты и составляющие.
- Описать (задокументировать) процессы, используя методологию IDEF/0 (входы/ресурсы – поставщики, управление/операции – ответственные, выходы – потребители, требования).

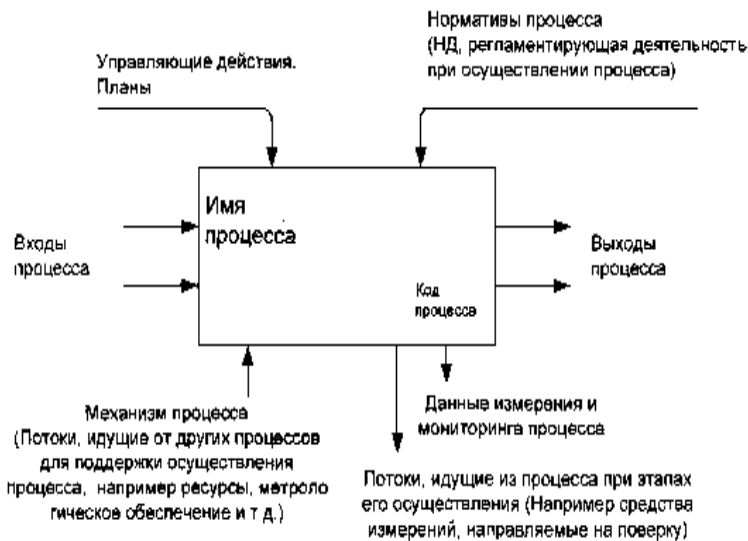


Рис. 1. Графическая модель процесса

- Определить и зафиксировать распределение ответственности и полномочий в рамках процесса.
- Проследить и описать взаимосвязи и взаимодействие процессов.
- Организовать мониторинг прохождения процесса, результат достижения запланированных результатов.
- Организовать анализ обеспеченности процессов ресурсами в соответствии с запланированными показателями.
- Быстро, понятно и убедительно довести всю вышеизложенную информацию до сведения сотрудников организации.

Так же реализуемая программа будет иметь встроенный графический редактор для создания диаграмм (блок-схем) процесса в котором можно будет выполнять следующие действия.

- Добавлять (удалять) операции.
- Добавлять (удалять) входы и выходы.
- Определять связи между различными операциями в пределах одного процесса по типу «выход» – «вход».
- Программа будет реализована в среде Borland Delphi 6 с использование СУБД PARADOX.

Основной особенностью данной программы является учет специфики научно-технических предприятий.

Новое инновационное решение создания процессно-ориентированной системы управления на основе применения программных средств облегчит задачу создания и внедрения СМК на соответствие ГОСТ Р ИСО 9001.

ЛИТЕРАТУРА

1. Елиферов В.Г., Репин В.В. Бизнес процессы. Регламентация и управление.
2. ISO 9000:2000 Системы менеджмента качества. Основные положения и словарь.
3. ГОСТ Р ИСО 9001:2001 Методика описания процесса СМК.

РАЗРАБОТКА ЛАБОРАТОРНЫХ МАКЕТОВ НА БАЗЕ ПИД-РЕГУЛЯТОРА ТРМ101

А.Н. Овчаренко, студент гр. 511-1, 5 курс ФВС;

Д.А. Рождественский, м.н.с. НИИ АЭМ

ТУСУР, кафедра КСУП, г.Томск

Для управления параметрами технологических процессов и установок в подавляющем большинстве применяются регуляторы, реализующие классический пропорционально-интегрально-дифференциальный (ПИД) закон управления. Способность ПИД-регуляторов управлять объектами, отличающимися по физической природе, свойствам и назначению, свидетельствует об их универсальности.

В проекте для студентов определен подход к решению следующей проблемы, состоящей в том, чтобы исследовать свойства оптимальных управлений динамическими объектами различного типа, выявить общие закономерности и, объединив их, синтезировать новый способ формирования управления для замкнутых систем, обладающий свойством универсальности. Таким образом, закон регулирования обеспечивает точность, стабильность и устойчивость системы. Первая задача, которая была поставлена, это проектирование и сборка лабораторного стенда, с использованием ПИД-регулятора ТРМ101 прибор компании ОВЕН. Для этого была взята за основу, наиболее широко используемую в технологических процессах и установках замкнутая система автоматического регулирования. В данной системе присутствуют три основных блока: это Регулятор, Исполнительное устройство и Объект управления, а также предусмотрено возмущающие воздействия.

Следующим этапом стала разработка лабораторных работ. Сформулированы теоретический и практический материал для освоения ручного способа ПИД-регулирования.

Целью данной лабораторной работы является – изучение лабораторного стенда и взаимодействие его устройств, изучение основ теоретического и практического ПИД-регулирования. Получение практических навыков работы в замкнутых системах автоматического регулирования с применением ПИД-регуляторов.

В этот блок лабораторного комплекса вошли следующие пункты.

В теоретический материал

- Место в АСУ ТП, достоинства и недостатки ПИД-регуляторов.
- Основные виды регулирования АСУ.
- Изучение устройств используемых в лабораторной установке и их взаимодействие.

– Общие принципы ПИД-регулирования.

В практический материал

- Настройка пропорциональной компоненты ПИД-регулятора.
- Настройка интегральной компоненты ПИД-регулятора.
- Настройка дифференциальной компоненты ПИД-регулятора.
- Описание основных методов программирования ПИД-регулятора TRM101.
- Индивидуальное задание и контрольные вопросы.

Еще одним важным и наиболее наглядным, с практической точки зрения, стала разработка АРМ, для прохождения студентами лабораторных работ с использованием SCADA – системы.

Целью данной лабораторной работы является освоение навыков ПИД регулирования в ПО MasterSCADA, умению свободно оперировать блоками управления и анализировать состояние системы с помощью блоков наблюдения.

Для разработки такого блока лабораторного комплекса было использовано Программное Обеспечение MasterSCADA, в которой разработана мнемосхема, с помощью, которой студентам предложено изучить следующее:

Теоретический материал

- Обзор, многофункциональность и характеристики SCADA систем.
- Введение в MasterSCADA.
- Взаимодействие с OPC-сервером.

Практический материал

- Запуск и описание рабочего режима мнемосхемы
- Индивидуальное задание
- Контрольные вопросы

После изучения студентами функциональных возможностей Мнемосхемы, в комплекс лабораторных работ включен следующий блок: Изучение внешних воздействий.

Целью данной лабораторной работы является изучение методов, с помощью которых можно повысить стабильность и устойчивость системы ПИД регулирования при внешних воздействиях.

Теоретический материал включает:

– *Методы стабилизации*

1. Увеличение скорости выхода на уставку (мнемосхема).
2. Гистерезис переключения компаратора (мнемосхема).

СИСТЕМА ОПТИЧЕСКОГО СКАНИРОВАНИЯ НА БАЗЕ ГИСТЕРЕЗИСНОГО ЭЛЕКТРОДВИГАТЕЛЯ С ПУСТОТЕЛЫМ ВАЛОМ

*О.Я. Погребских, студент 5 курса ФВС; И.Л. Столбов, аспирант
ТУСУР, кафедра КСУП, г. Томск*

Среди дистанционных методов исследования окружающей среды важнейшими являются лидарные методы, которые по соотношению с химическими, радиолокационными и акустическими методами обеспечивают ряд преимуществ. К ним в первую очередь относятся дистанционность, высокая дальность действия, высокое пространственно-временное разрешение (детальное исследование слоя атмосферы, гидросферы, облака либо дыма за короткое время) и возможность получения многопараметрической информации об объекте исследования [1].

Важнейшим элементом современных лидарных комплексов является оптико-механический сканер [2]. Наличие в схеме лидара сканера позволяет получать не только информацию о концентрации аэрозолей в атмосферном образовании и дальности до него, но и его изображение, формируемое на экране видеоконтрольного устройства или на бумаге с помощью графопостроителя.

Недостатком применяемых сканеров является наличие механической передачи вращения на оптический элемент, что снижает точность и надежность работы устройства сканирования и всей лидарной системы в целом.

Предлагается для вращения оптических элементов в лидарных сканерах использовать гистерезисные электродвигатели с пустотелым валом. Основным отличием данного типа двигателей является наличие сквозного канала вала, используемого для установки вращающихся оптических и радиоволноводных элементов приборов при осесимметричной структуре построения измерительных трактов. Прямой привод вращения на оптический элемент без механической передачи значительно увеличивает точность, надежность и бесшумность работы прибора [3].

Преимущество гистерезисных двигателей (ГД) перед другими типами двигателей заключается в возможности перемагничивания ферромагнитного ротора двигателя полем статора, что позволяет плавно, не выходя из синхронного режима работы, менять фазу вращения вала [4]. Управляя фазой вращения каждого из двигателей, мы тем самым управляем взаимным положением вершин оптических клиньев (оптических элементов сканера), а значит параметрами сканирования [5].

Для питания 3-фазных синхронных гистерезисных двигателей применяется 3-фазный мостовой инвертор напряжения со 180° управлением, который обеспечивает высокую стабильность выходного на-

пряжения и частоты. Автономный инвертор напряжения (АИН) питается от автономного источника постоянного напряжения. Схема управления привода управляя инвертором регулирует частоту и амплитуду напряжения, подаваемого на вход гистерезисного электродвигателя.

Обратная связь по положению ротора осуществляется с помощью фотоимпульсного датчика углового положения (энкодера), установленного на валу электродвигателя.

Обратная связь по положению вектора намагниченности ротора осуществляется при помощи датчика тока.

Для управления вектором намагниченности ротора (а значит и фазой вращения оптического клина) используется устройство импульсно-намагничивания. Моменты времени, в которые следует производить намагничивание ферромагнитного материала ротора ГД, рассчитываются по методу, представленному в [6].

Для получения высокого качества управления лидарным сканером в статических и динамических режимах предлагается использовать синергетический метод управления ГД [7].

ЛИТЕРАТУРА

1. *Межерис Р.* Лазерное дистанционное зондирование. Москва: Мир, 1987. 550 с.
2. *Протопопов В.В.* Инфракрасные лазерные локационные системы. М.: Военное издание, 1987. 176 с.
3. <http://www.utkit.com/gniicnp/catalog.nsf> – Электродвигатель переменного тока с пустотелым валом.
4. *Делекторский Б. А., Тарасов В. Н.* Управляемый гистерезисный привод. М.: Энергоатом издат, 1983. 128 с.
5. *Мирошников М.М.* Теоретические основы оптико-электронных приборов. Ленинград: Машиностроение. 1977. 600 с.
6. *Андреев М. И.* Влияние параметров обмотки статора на эффективность перевозбуждения СГД // Сб. статей «Электромеханические системы и устройства автоматического управления». Изд. Томского университета, 1986. с. 74–79.
7. *Столбов И.А.* Синергетический подход к управлению гистерезисным электродвигателем // Материалы докладов научно-технической конференции «Научная сессия ТУСУР-2003», Томск. 2003. Часть II.

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА «КОНТИНГЕНТ КАФЕДРЫ»

Е.А. Потапова, ассистент каф. КСУП
ТУСУР, каф. КСУП, г. Томск

С каждым годом всю большую ценность приобретает информация. Человечество входит в новый этап развития, в информационное обще-

ство. Встает вопрос о наиболее эффективном способе ведения данных. Требуется создавать такие системы управления данными, которые обеспечивают быстрый поиск необходимых данных, устраняют избыточность данных и обеспечивают сохранность и защищенность хранимой информации.

Следовательно, тема является актуальной в настоящее время. Данная разработка является локальной базой данных и служит для хранения и поиска информации, необходимой для секретаря кафедры КСУП:

1. Данные о студентах (Список группы, Общие сведения, ИУП, ПВЗ на обучение).

2. Данные о выпускниках.

3. Данные о сотрудниках (список сотрудников, общие сведения, домашний адрес и телефон, список ППС).

Для реализации проекта была выбрана реляционная модель данных, которая представляет связанную между собой совокупность таблиц БД. Это обосновано тем, что представление данных в виде таблиц наиболее близко к традиционным способам хранения информации. Связь между таблицами может находить свое отражение в структуре данных.

Пристальное внимание разработчиков приложений баз данных вызывают инструменты, при помощи которых можно было бы создавать приложения. Выдвигаемые к ним требования в общем виде можно сформулировать как: «быстрота, простота, эффективность, надежность».

В настоящее время популярна среда объектно-ориентированного программирования Delphi, основа которой – язык Object Pascal. Она позволяет быстро создавать приложения различной степени сложности – от простейших программ до профессиональных, предназначенных для работы с базами данных.

В основе такой общепризнанной популярности лежит тот факт, что Delphi, как никакая другая система программирования, удовлетворяет изложенным выше требованиям.

Delphi не имеет своего формата таблиц БД, однако несмотря на это, обеспечивает мощную поддержку многих СУБД, как локальных (например, dBase и Paradox), так и промышленных (например, InterBase и SyBase). Так как таблицы Paradox являются достаточно развитыми и удобными при создании БД, мы использовали именно этот формат таблиц.

Для системы Delphi документом является проект. Под документом понимается центральный объект, с которым работает приложение. При организации приложений мы использовали многодокументный интерфейс, т.к. в Windows различают два основных типа приложений: одно-

документные и многодокументные. Основным отличием является то, что многодокументное приложение может работать одновременно с несколькими различными документами.

Для ограничения доступа, после запуска системы (файл PUSK.EXE) появляется окно, в которое запрашивает пароль. Если пароль указан верно, то появляется заставка, а через 5 секунд – меню. С помощью опции Открыть мы можем выбрать документ, необходимый для работы. Помимо отображения записей набора данных в табличной форме, здесь имеются 3 панели: Поиск, Фильтрация и Правка. Панель Поиск осуществляет поиск по Ф.И.О. студента. Панель Фильтрация – фильтрует НД по группе. Панель Правка – служит для того, чтобы к полям записи в НД можно было осуществлять доступ из отдельных визуальных компонентов. Для редактирования записей служат кнопки Добавить, Изменить, Удалить, Запомнить, Отменить.

По аналогии с этим приложением выполнены приложения Общие сведения о студентах, ИУП, ПВЗ на обучение и Выпускники (выполняется фильтрация по группе и году выпуска).

Рассмотрим приложение Список сотрудников. Здесь есть только панель Правка. Аналогично выполнены приложения Общие сведения о сотрудниках, Домашний адрес и телефон, Список ППС.

В дальнейшем, при внедрении данной автоматизированной информационной системы на кафедре КСУП, это позволит пользователям, а конкретнее секретарю кафедры автоматизировать свое рабочее место, что в значительной степени сократит расходы времени, облегчит поиск нужной информации.

ИЗУЧЕНИЕ MASTER-SCADA

*Е.С. Румынская, студентка 5 курса ФВС;
Д.А. Рождественский, м.н.с. 18 отдел НИИ АЭМ
ТУСУР, кафедра КСУП, г.Томск*

Обоснование необходимости автоматизации систем управления технических процессов и применение для этого системы Master-Scada.

Сегодня наша жизнь протекает в условиях, когда время – это деньги. Чем быстрее мы достигнем поставленной цели, тем быстрее мы получим денежное вознаграждение за проделанную работу. Это и стало причиной возрастания потребности построения высокоэффективных и высоконадежных автоматизированных систем управления технологическим процессом (АСУТП).

Причины связаны со следующими основными факторами:

- Возросшими требованиями к повышению качества технологического процесса;
- Ростом дефицита природных ресурсов;
- Появлением мощных, компактных, недорогих измерительных и управляющих устройств, обусловленных прогрессом в областях вычислительной техники, программного обеспечения и телекоммуникаций;
- Повышение степени автоматизации и перераспределением функций между человеком и аппаратурой;

Какие же преимущества дает создание автоматизированных рабочих мест?

1. Позволяет заменить громоздкие, неудобные, дорогостоящие щиты управления на персональные компьютеры. Это уменьшает рабочую площадь, делает рабочее место более удобным, простым, наглядным и значительно снижает его стоимость.

2. Делает систему управления более гибкой, когда для того, чтобы добавить несколько сигнализационных ламп или управляющих рычагов не нужно полностью менять весь щит, а можно лишь сделать небольшие изменения в компьютерной программе.

3. Облегчает анализ и управление технологическим процессом, ведь программное обеспечение позволяет представлять данные в самом различном виде (графики, диаграммы, уровни, изменение положения, цвета и т.д.), позволяет сохранять данные продолжительное время, а управление производится нажатием клавиши или кликом мышки.

Достичь высокого уровня автоматизации в решении задач разработки систем управления, сбора, обработки, передачи, хранения и отображения информации позволяет применения SCADA-технологий. В настоящее время SCADA является основным и наиболее перспективным методом автоматизированного управления сложными динамическими системами (процессами). Итак, SCADA – процесс сбора информации реального времени с удаленных точек (объектов) для обработки, анализа и возможного управления удаленными объектами. Требование обработки реального времени обусловлено необходимостью доставки (выдачи) всех необходимых событий (сообщений) и данных на центральный интерфейс оператора (диспетчера).

Рассмотрим подробно одну из Scada-систем. Master-Scada – это первая в России объектно-ориентированная Scada фирмы InSat. При сравнении ее с другими традиционными Scada, было выделено множество преимуществ: это универсальное быстродействующее подключение к любому оборудованию, использование хранимых процедур, единый пользовательский интерфейс для всех функций, удобная и наглядная конфигурация объектов системы, интуитивно понятный интерфейс,

сравнительно не дорогой программный продукт, имеет полный набор всех необходимых документов (тренды, рапорты, мнемосхемы и др.)

Для наглядной демонстрации возможностей MasterScada опишем проект «Управление уровнем в баке».

Эта установка имеет три бака и исполнительные механизмы для регулирования уровня в каждом баке. При возникновении аварийных ситуаций, появляется сообщение об аварии. Ведется общий журнал и журнал аварий.

В этой ситуации система предпринимает действия по устранению возникшей аварии.

Установка имеет семь режимов, которые формируются тремя кнопками (тумблерами):

1. Отключение (закрытие) всех исполнительных механизмов;
2. Залив в емкость №1 из емкости №3;
3. Залив в емкость №2 из емкости №3;
4. Слив из емкости №1 в емкость №3;
5. Слив из емкости №2 в емкость №3;
6. Перелив из емкости №1 в емкость №2 через емкость №3;
7. Перелив из емкости №2 в емкость №1 через емкость №3.

Для того, чтоб разработанный продукт отвечал таким принципам как защищенность системы от посторонних лиц, ограничение полномочий по должностям, контроль операторов работающих в разные смены. Была разработана система защиты, которая предполагает создание должностей, присвоение каждой должности определенный перечень необходимых полномочий, чтоб обеспечить безопасную работу всей установки. Создание смен и перечень операторов, которые смогут иметь доступ к установке в определенное время. Каждый оператор имеет свой пароль для идентификации его системой.

В заключении можно сделать вывод, что Master-Scada – это полноценный объектный подход, разделение работы с системой и объектом, типизация и тиражирование решений, свыше 150 готовых объектов, визуальное выполнение всех действий, разработка сценариев без программирования, уникальный редактор мнемосхем, мощные средства обработки данных, открытая система (интеграция с внешними программами, интернет-публикации, поддержка стандартов обмена данными), наилучшее соотношение цена-качество на российском рынке.

ЛИТЕРАТУРА

1. *Встроенный помощник Master-Scada.*
2. *Учебник «Master-Scada быстрый старт», предоставляемый фирмой «InSat».*
3. Сайт фирмы «InSat» www.insat.ru

ПОДСИСТЕМА ВЕДЕНИЯ ДОГОВОРОВ ПАКЕТА ПРОГРАММ BASCOFFICE ОПЕРАЦИОННОГО ЦЕНТРА

А.С. Савельев, студент 5 курса ФВС;

А.Я. Клименко, д.т.н., профессор каф.КСУП

ТУСУР, кафедра КСУП, г. Томск, savgood@yahoo.com

Существующие системы по управлению договорами, как правило, очень дороги, разработка их занимает много времени, отсюда и берется высокая стоимость. Типизация этих подсистем – путь к индустриализации производства программного обеспечения [1]. Типовых решений в части подсистемы ведения договоров не существует или они не достаточно функциональны, или, наоборот, слишком функциональны, т.е. громоздки для приложения в операционном центре процессинговой компании. Поэтому создание такого рода подсистем актуально.

Система ведения договоров (СВД) – комплексное решение, предназначенное для управления договорами на всех стадиях их жизненного цикла. Данное решение позволяет обеспечить информационную поддержку и автоматизацию деятельности подразделений и служб предприятия, вовлеченных в процесс формирования, сопровождения и контроля исполнения договоров, заключенных предприятием.

СВД обладает развитыми возможностями по управлению договорами предприятия, включающий централизованный справочник договоров и деловых партнеров предприятия, ведение архива документов по каждому договору, функции планирования и контроля хода исполнения договоров, а также возможности подготовки и согласования проектов договоров, дополнительных соглашений.

Функциональная структура системы ведения договоров имеет вид:

- анализ атрибутов договоров;
- формирование договора;
- корректировка;
- импорт.

Функции модуля «Анализ атрибутов договоров»:

- регистрация атрибутов;
- генерация дерева договоров;
- составление таблиц договоров.

Функции модуля «Формирование договора»:

- формат документа;
- имя договора;
- номер договора;
- код покупателя, продавца, эмитента, эквайрера.

Выбор системы управления баз данных (СУБД) [2, 3] представляет собой сложную многопараметрическую задачу и является одним из

важных этапов при разработке приложений баз данных. Выбранный программный продукт должен удовлетворять как текущим, так и будущим потребностям предприятия, при этом следует учитывать финансовые затраты на приобретение необходимого оборудования, самой системы, разработку необходимого программного обеспечения на ее основе, а также обучение персонала. Кроме того, необходимо убедиться, что новая СУБД способна принести предприятию реальные выгоды. В качестве среды разработки использовалась среда Visual FoxPro 8.

ЛИТЕРАТУРА

1. Гильманов А.А., Клименко А.Я., Странгуль О.Н., Тарасенко В.П. Карточные технологии автоматизации маркетинга.
2. Буч Г., Рамбо Д., Джекобсон А.. Язык UML Руководство пользователя.
3. Фаулер М. и Скотт К.. UML основы, второе издание.

БАЗА ДАННЫХ «ВЫПУСКНИКИ КАФЕДРЫ КСУП»

И.В. Синянская, студент 5 курса ФВС;

М.В. Черкашин, ст. преподаватель кафедры КСУП

ТУСУР, кафедра КСУП, г.Томск

Основной целью разработки является автоматизация процесса сбора, обработки и хранения информации о выпускниках кафедры КСУП.

Современный мир информационных технологий трудно представить себе без использования баз данных. Практически все системы любого предприятия в той или иной степени связаны с функциями длительного хранения информации. Фактически информация становится фактором, определяющим эффективность любой сферы деятельности. Увеличились информационные потоки и повысились требования к скорости обработки данных, и теперь уже большинство операций не может быть выполнено вручную, они требуют применения наиболее перспективных компьютерных технологий. Любые административные решения требуют четкой и точной оценки текущей ситуации и возможных перспектив ее изменения. И если раньше в оценке ситуации участвовало несколько десятков факторов, которые могли быть вычислены вручную, то теперь таких факторов сотни и сотни тысяч, и ситуация изменяется не в течении года, а через несколько минут, а обоснованность принимаемых решений требуется большая, потому что и реакция на неправильные решения более серьезная, более быстрая и более мощная, чем раньше. И, конечно, обойтись без информационной модели производства, хранимой в базе данных (БД), в этом случае невозможно [1, 2].

Кафедра КСУП успешно работает по обучению студентов уже почти 20 лет. За это время было выпущено почти 1000 студентов. В последнее время в нашем университете появилась традиция проводить встречи выпускников каждый год. С этой целью проводится сбор информации о выпускниках кафедры. В настоящий момент, данный процесс не автоматизирован. Кроме того, студенты, заканчивающие кафедру, также оставляют информацию о себе и будущем месте работы в виде анкеты.

Таким образом, появилась проблема автоматизации процесса сбора, обработки и хранения информации о выпускниках кафедры КСУП. Поэтому целью данной работы является разработка базы данных и системы управления этой базой для автоматизации обработки данных по выпускникам кафедры КСУП.

В ходе работы была написана программа, реализующая регистрацию в базе данных выпускников кафедры КСУП, возможность просмотра и редактирования информации о выпускниках, добавление, изменение и удаление специальности и группы, поиск выпускников по фамилии, специальности, группе, году поступления, году выпуска и просмотра фотографий выпускников.

Для решения задачи в качестве средства разработки программы была использована среда программирования Borland Delphi 6.0 [3]. Сама база данных разработана при помощи технологии BDE (Borland Database Engine). Хранение данных организовано в виде таблиц, в которых содержится информация об личностных данных выпускников (Ф.И.О., дата рождения, адрес проживания, фото, место работы и др.) и служебная информация, предназначенная для сотрудников кафедры. Интерфейс программы прост и интуитивно понятен. Ввод, просмотр данных и редактирование осуществляется через диалоговые окна. Программа имеет краткую помощь по основным элементам интерфейса и порядку ввода (изменения) данных [4].

В ходе работы был реализован программный продукт база данных «Выпускники кафедры КСУП». Программа предназначена для автоматизации обработки и хранения данных по выпускникам кафедры КСУП. Применение данного программного продукта позволит сократить время на обработку и поиск информации по выпускникам, обеспечит ее хранение в электронной форме. Также возможен доступ к разработанной базе через всемирную сеть ИНТЕРНЕТ с использованием клиент-серверной технологии [5].

Разработанная система может быть также использована на других кафедрах ТУСУРа и других ВУЗов.

ЛИТЕРАТУРА

1. Карпова Т.С. Базы данных: модели, разработка, реализация. М.: Питер, 2002, 304 с.
2. Омельченко Л. Visual FoxPro 7.0: Самоучитель. М.: БХМ-Петербург, 2002. 600 с.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ ОБУЧАЮЩЕЙ СИСТЕМЫ НА БАЗЕ WEB-ТЕХНОЛОГИЙ

Н.В. Солодухина, студентка 5 курса ФВС;

Н.Ю. Хабибуллина, старший преп. каф. КСУП

ТУСУР, кафедра КСУП, г.Томск

В последние несколько лет наблюдаются развитие дистанционной формы образования и постепенное ее внедрение в образовательные инстанции. Разработка и автоматизация систем дистанционного обучения для среды Internet. Конечная цель данной системы: предоставить широкому кругу пользователей глобальной сети качественную систему обучения при минимальных затратах на поддержание и администрирование обучающей системы. Составляющей такой системы является автоматизированная обучающая система (АОС) на базе web-технологий.

АОС – система для разработки, модификации и использования обучающих программ, управления учебным процессом в диалоге с обучаемым, сбора и обработки информации о результатах обучения. Такая система предназначена для выполнения некоторых из функций преподавателя-человека [1]. Создавая АОС, нужно помнить о трех обстоятельствах:

- человеческий мозг способен перерабатывать в ограниченный промежуток времени ограниченный объем полезной информации;
- в большинстве отечественных вузов работа в компьютерном классе лимитирована по времени;
- «общение» студента-гуманитария с компьютером требует от первого повышенного психического напряжения.

Лучшие АОС никогда не бывают «насыщены» сложными формулами, схемами, др. Работа с ними не требует много времени, а текст нередко «разбавляется» шутками, забавными фразами и смешными рисунками [3]. Автоматизированные обучающие системы бывают нескольких типов. Одни АОС «способны» контролировать знания учащихся, другие содержат в себе элементы «учебного тренажа», третьи помогают овладению новым учебным материалом, четвертые предназначены для того, чтобы стимулировать интерес учащихся к изучаемому предмету [3].

В ходе работы создана АОС по дисциплине «Прикладные методы искусственного интеллекта (ПМИИ)». В состав разработанной АОС входят следующие модули:

- лекционный материал по дисциплине ПМИИ;
- лабораторные работы и задания к ним;
- методические указания к лабораторным работам;

- тестирование приобретенных знаний;
- редактор формирования тестирующих вопросов.

Ввод ответов при тестировании происходит тремя способами. Первый способ – это написание слова, второй – выбор одного ответа из предлагаемых вариантов, а третий способ – выбор более чем одного варианта ответа [2].

При выявлении требований для системы нужно учитывать требования, как со стороны преподавателя, так и со стороны учащегося. У учащегося требования заключаются в виде удобного использования учебника и правильности материала. Требования преподавателя – правильность работы теста и возможность без затруднительного ввода необходимых вопросов и ответов на них. А так же возможность удаления не подходящих вопросов.

Для разработки АОС были выбраны следующие программные средства:

1. Denver (или Denwer) – это универсальный пакет, в котором сразу есть настроенный и установленный PHP, MySQL, Apache, CGI, SSL, VirtualHosts. Это незаменимый пакет любого Web-программиста и дизайнера [5].

2. PHP – «PHP: Hypertext Preprocessor/Гипертекстовый Препроцессор», широко используемый Открытый Ресурс, язык скриптинга (сценариев) общего назначения, который особенно подходит для Web и может быть внедрен в HTML [5].

3. HTML – язык, который записывается в ASCII формате и поэтому может быть созданы и отредактированы в любом текстовом редакторе [6].

4. SQL – структурированный язык запросов, который является инструментом, предназначенным для выборки и обработки информации, содержащейся в компьютерной базе данных [4].

ЛИТЕРАТУРА

1. Манекин Р. Автоматизированные обучающие системы. М.: Наука, 2001. 245 с.
2. Кручинин В.В. Разработка компьютерных учебных программ. Томск: Изд-во ТГУ, 1998. 367 с.
3. <http://mw.com.ru>
4. <http://www.sbgro.com>
5. Коротеева Е.П. Учебник HTML. СПб.: Питер, 2000. 460 с.

ПРОГРАММА ЧИСЛЕННОЙ ИДЕНТИФИКАЦИИ ПАРАМЕТРОВ МОДЕЛИ СВЧ-ТРАНЗИСТОРА

Д.Е.Тимофеев, студент 5 курса ФВС

ТУСУР, кафедра КСУП, г.Томск

Цель работы – проектирование программы численной идентификации математической модели СВЧ транзистора по заданным параметрам рассеяния.

Автоматизация проектирования имеет огромное значение для развития науки, техники и производства в современном обществе. В настоящее время автоматизация проектирования – основной способ повышения производительности и эффективности труда инженерно-технических работников, занимающихся проектированием. Использование автоматизации проектирования позволяет создавать все более сложные технические объекты и гибко реагировать на появление новых решений в той или иной области техники.

Практическая реализация методов и идей автоматизированного проектирования происходит в рамках систем автоматизированного проектирования (САПР).

На кафедре КСУП разрабатывается комплекс программ автоматизированного проектирования СВЧ устройств. В данных программах используются модели транзисторов в виде S-параметров. Однако в некоторых случаях, например при проектировании согласующих цепей для СВЧ усилителей необходимо представление транзистора в виде ФЭС (физическая эквивалентная схема).

Для проведения расчетов СВЧ транзисторных малошумящих усилителей необходимо иметь информацию о поведении транзистора в широком диапазоне частот. Эта информация может быть получена из описания транзистора с помощью структурной модели – физической эквивалентной схемой (ФЭС) или бесструктурной – матрица параметров транзистора как четырехполюсника (ЧП). Знание полной ФЭС транзистора более предпочтительно, так как в этом случае имеется информация о характеристиках транзистора во всем частотном диапазоне. Поэтому при разработке программ для расчета СВЧ усилителей на ЭВМ необходимо стремиться к использованию ФЭС транзисторов.

Однако большая сложность ФЭС СВЧ транзистора по сравнению с его низкочастотной моделью из-за необходимости учета большего количества элементов и их режимных зависимостей практически исключает возможность ее использования при эскизных расчетах. Поэтому на первом этапе проектирования СВЧ усилитель более предпочтительно использовать описание транзистора внешними параметрами как четы-

рехполюсника. Необходимо отметить, что оба способа описания транзистора тесно связаны и дополняют друг друга. Так, например, измерение параметров элементов ФЭС может быть проведено с большей погрешностью, чем измерения некоторых параметров ЧП, описывающего транзистор. Поэтому одним из этапов машинного проектирования СВЧ транзисторов является «синтез» ФЭС транзистора, т.е. уточнение параметров некоторых ее элементов по измеренным внешним характеристикам транзистора.

Исследование характеристик линейных схем в частотной области может быть проведено с помощью метода узловых потенциалов, наиболее распространенного и простого в применении.

Данный метод основывается на записи первого закона Кирхгофа для всех узлов схемы. Для каждого узла составляют уравнение баланса токов. Система узловых уравнений может быть представлена в матричном виде и выражена через матрицу проводимостей, каждый элемент которой имеет размерность проводимости. Первой задачей возникающей при этом, является задача получения наиболее простым способом узловых уравнений с помощью матрицы проводимостей схемы [1].

Поэтому появилась необходимость создания программы численной идентификации параметров модели СВЧ-транзистора, заданной в виде ФЭС, по исходным S -параметрам. Указанная программа должна производить считывание параметров транзистора из файла S2P, производить идентификацию параметров модели по заданным S -параметрам, а также выполнять графическое отображение рассчитываемых S -параметров и ошибки идентификации.

Входными данными являются параметры рассеивания, заданные в файле на подмножестве языка Touchstone. При анализе цепь представляется в виде эквивалентного четырехполюсника. Алгоритм вычисления параметров эквивалентного четырехполюсника основан на методе узловых проводимостей. Этот алгоритм предлагает формирование матриц проводимости и спектральных плотностей шумовых токов для многополюсной цепи с последующим исключением внутренних узлов, переходом к системе S -параметров и расчетом рабочих характеристик.

В программе реализована оптимизация ФЭС, которая происходит до тех пор, пока не будет минимизировано среднеквадратическое отклонение заданных S -параметров, полученных в результате анализа ФЭС.

Предусмотрен вывод результатов в виде графиков. Предусмотрена реализация всех настроек, характерных для графиков.

Пользователю предоставляется возможность сохранения полученных характеристик ФЭС в файл (язык Touchstone) для последующего использования [2].

В качестве среды реализации будущей программы была выбрана система MATLAB 6.5. Система MATLAB (матричная лаборатория) была создана специалистами фирмы Math Works, Inc. как язык программирования высокого уровня для технических вычислений. Одним из самых важных достоинств системы MATLAB является возможность ее расширения с целью решения новых научно-технических задач. Это достигается, прежде всего, созданием целого ряда пакетов расширения системы, охватывающих многие новые и практически полезные направления компьютерной математики [3].

ЛИТЕРАТУРА

1. Петров Г.В. Линейные балансные СВЧ-усилители. М.: Радио и связь, 1983. 150 с.
2. Финдлер Дж.К., Найтингел К. Машинное проектирование электронных схем. М.: Высшая школа, 1985. 220 с.
3. Дьяконов В. MatLab 6: Учебный курс. Питер. 2001.

КОНФИГУРИРОВАНИЕ ПРОГРАММИРУЕМОГО ЛОГИЧЕСКОГО КОНТРОЛЛЕРА ЭЛСИ-ТМ

Ю.А. Томина, студентка гр. 581-2 ФВС КСУП;

*А.С. Удод, зав. лабораторией СУ ТП НИИ Электронных систем
ТУСУР, кафедра КСУП, г. Томск, т. 76-14-05, juliet@sibmail.com*

Рассмотрены вопросы, связанные с изучением принципов создания программных модулей для исполняющей системы ElsyTMS программируемого логического контроллера (ПЛК) ЭЛСИ-ТМ и методов конфигурирования модулей. Приведено описание средств конфигурирования ПЛК ЭЛСИ-ТМ и функций созданного программного модуля «Empty».

ПЛК ЭЛСИ-ТМ предназначен для автоматизации объекта «Резервуарный парк». Конфигурация ПЛК – это структурированный набор файлов, содержащий в себе информацию о составе контроллера, параметрах работы отдельных модулей и описания потоков данных между модулями. Конфигурирование ПЛК ЭЛСИ-ТМ направлено на решение следующих задач:

- а) сбор информации с датчиков уровня в емкостях, датчиков включения/выключения насосов и заслонок;
- б) выдача управляющих воздействий на рыле;
- в) логическое, программно-логическое управление установкой, автоматический пуск и останов оборудования;

- г) математическая обработка информации по различным алгоритмам;
- д) регистрация и архивация параметров работы установки;
- е) обмен данными с другими контроллерами в рамках контроллерной управляющей сети реального времени.

Технология программного модуля для исполняющей системы ElsyTMS ПЛК ЭЛСИ-ТМ состоит из следующих этапов:

- а) создание конфигурации модуля;
- б) создание правил сборки (правил компиляции и установки модуля);
- в) создание исходного кода модуля;
- г) компиляция и установка модуля в target-систему (установка модуля – это передача исполняемого кода в target-систему).

Конфигурирование модуля, а также ПЛК ЭЛСИ-ТМ выполняется с помощью специально предназначенной программы ElsyTMManager. Для установки исполняемого файла и работы с исполняющей системой используется программа ElsyTMPultPC. Работа над исходным кодом модуля ведется с использованием компилятора gcc версии 2.95.3. Разработанный модуль «Empty» – тестовый, поэтому основной цикл, где происходит обработка входных сигналов, довольно прост – имитация работы грузового лифта. Основная задача состоит в том, чтобы научиться правильно конфигурировать ПЛК ЭЛСИ-ТМ и создавать новые программные модули. Это необходимо для дальнейшей работы в области программирования и конфигурирования ПЛК.

ЛИТЕРАТУРА

1. *Программный комплекс «INFINITY».* Сервер ввода/вывода: методические указания. Томск, 2005. 98 с.
2. *Создание программного модуля:* методические указания. Томск, 2005. 25 с.
3. Контроллер программируемый ЭЛСИ-ТМ. Редактор конфигурации ElsyTMManager: методические указания. Томск, 2006. 23 с.
4. *Контроллер* программируемый ЭЛСИ-ТМ. Программное обеспечение: инструкция по установке и обновлению. Томск, 2006. 20 с.
5. *Контроллер* программируемый ЭЛСИ-ТМ. Программное обеспечение: руководство пользователя. Томск, 2006. 111 с.

ПРОЕКТИРОВАНИЕ УСТАНОВКИ ЛАЗЕРНОЙ РЕЗКИ

**С.А. Трунов, Е.А. Телицын, О.И. Каневский, студенты 5 курса ФВС
ТУСУР, кафедра КСУП, г.Томск**

Данный проект выполняет группа из трех человек. Техническое задание – спроектировать установку лазерной резки со следующими характеристиками:

- Лазер должен обеспечивать резку листовой стали толщиной не менее 4 мм;
- Лазер должен быть надежен в эксплуатации;
- Координатный стол должен обеспечивать точность позиционирования не хуже 0.1 мм;
- Рабочая зона стола – 2000×1500 мм;
- Конструкция стола должна быть эргономичной; нужно предусмотреть защиту рабочих элементов стола от повреждений, попытаться использовать внутреннее пространство для размещения каких-либо элементов конструкции (для компактности);
- Программное обеспечение установки должно поддерживать ввод данных с формата *.dwg

Лазерная обработка материалов является одной из технологий, определяющих современный уровень производства в развитых производственных предприятиях.

Лазерная резка – самый распространенный вид лазерной обработки. В процессе лазерной резки происходит плавление или испарение материала и удаление продуктов процесса из зоны резки продувкой кислородом, воздухом, азотом или другим технологическим газом. Основные достоинства: высокое качество технологического процесса, скорость, гибкость, минимальные затраты материала (диаметр «режущего инструмента» 0.1– 0.2 мм). При резке лазером отпадает необходимость механического закрепления заготовки ввиду отсутствия динамических или статических воздействий, резка осуществляется сфокусированным излучением.

Комплекс для лазерной резки материалов включает в себя следующие элементы:

- источник лазерного излучения с системой охлаждения и источником питания;
- технологический координатный стол с оптической системой;
- систему управления столом с пакетом программного обеспечения;
- систему подачи технологического газа;
- систему вентиляции и удаления продуктов резки.

Для резки применяются газовые CO₂-лазеры с мощностью более 500 Вт, маломощные CO₂, твердотельные YAG-лазеры и волоконные лазеры.

Координатный стол – промышленная установка, комплекс оборудования, предназначенный для перемещения по заданной траектории рабочего механизма станка или обрабатываемой детали.

Блок управления, в основном, располагают в специальном шкафу. В блоке управления используют промышленный контроллер, связанный с ЭВМ.

Система подачи технологического газа включает в себя компрессор (при работе с воздухом) или баллоны со сжатым технологическим газом, элементы масло– и влагоотделения и трубопроводы подачи газа в резак.

Система вентиляции и удаления продуктов резки состоит из мощного вентилятора, обеспечивающего удаление продуктов резки из рабочей зоны и системы фильтров для улавливания твердых частиц.

Результатом проделанной работы является проект установки резки лазером.

ПРИНЦИПЫ ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КОМПОНОВКИ ТЕХНИЧЕСКИХ ОБЪЕКТОВ В ЗАДАННОМ ОБЪЕМЕ

Р.С. Хрущев, аспирант

ИОА СО РАН, кафедра КСУП ТУСУР, г. Томск, am@nm.ru

Нахождение оптимального варианта компоновки технических объектов имеет существенное значение, так как влияет не только на стоимость проектируемого оборудования, но и на удобство работы и безопасность обслуживающего персонала. Решение данной задачи зависит от множества факторов, что существенно затрудняет автоматизацию поиска оптимального варианта компоновки объектов. Разработанные к настоящему времени методы автоматизированной компоновки ограничены конкретной областью применения [1, 2].

Компоновка технических объектов может производиться по различным критериям, например, таким, как: равномерность распределения массы по объему, минимум длины соединений между объектами, минимум взаимного электромагнитного, теплового взаимодействия и др.

Необходим механизм, позволяющий конструктору вносить изменения во время работы алгоритма компоновки. Разработка правил (эвристик), полученных в ходе диалога конструктора и машины, позволит создать обучаемую систему с обширной областью применения. Такой «человеко-машинный» подход позволит в кратчайшие сроки получить оптимальный результат, удовлетворяющий заданным критериям.

Разрабатываемая автоматизированная система позволит выполнять компоновку объектов в заданном объеме с равномерным распределением массы по объему. Система разбита на два модуля: модуль создания объектов, и модуль компоновки их в заданном объеме по заданным критериям.

Объект представляется в виде объединения нескольких примитивов. Для создания сложного объекта необходимо разбить требуемый объект на совокупность простых объектов, максимально приближенных к примитивам [3].

Каждый объект имеет определенные свойства: габариты, тип материала, плотность и др. По известным свойствам объекта рассчитывается масса объекта и определяется его центр тяжести. Центр тяжести всей сцены рассчитывается по известным центрам тяжести отдельных объектов, с учетом их расположения в заданном объеме [4].

Использование компьютерной графики для визуализации решения задачи позволяет наглядно показать конструктору компоновку в объеме и предоставляет средства для контроля и управления решением поставленной задачи.

ЛИТЕРАТУРА

1. Пащенко О.Б., Филиппов М.В., Волосатова Т.М. Метод построения эвристических алгоритмов в системе автоматизированного проектирования компоновки радиоэлектронного оборудования на борту маневренного самолета // Информационные технологии. 2005. №3. С. 6 – 8.
2. Бобков В.А., Роньшин Ю.И., Мельман С.Ю. Визуализация вексельных сцен // Информационные технологии. 2005. №6. С. 16 – 19.
3. Хрущев Р.С., Молчанов И.В., Андреев М.И. Автоматизированная система компоновки технических объектов // Материалы региональной НТК «Научная сессия ТУСУР-2003». Томск: ТУСУР, 2003. В 3 Ч. Ч 2. С. 142–145.
4. Хрущев Р.С. Система автоматизированного проектирования мобильных станций // Материалы Международной НПК «Электронные средства и системы управления». Томск: Издательство Института оптики атмосферы СО РАН, 2004. В 3 частях. Ч. 3. С. 126–127.

АВТОМАТИЗИРОВАННЫЙ ЛАБОРАТОРНЫЙ СТЕНД ПО ДИСЦИПЛИНЕ

«ТЕОРИЯ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ»

К.Ю. Царегородцев, студент 5 курса ФВС;

М.И. Андреев, к.т.н., с.н.с., доцент

ТУСУР, кафедра КСУП, г. Томск, heavy@ms.tusur.ru

С развитием вычислительной техники учебный процесс все больше склоняется к использованию вычислительных средств, в том числе и применению автоматизированных лабораторных стендов для выполнения работ по различным дисциплинам.

Разрабатываемый автоматизированный лабораторный стенд по дисциплине «Теория автоматического управления» использует в каче-

стве объекта исследований двигатель постоянного тока типа ДПМ -30 Н1-03Т, с номинальным напряжением питания 27В, номинальной скоростью вращения 4500 об/мин., номинальной мощностью 6Вт. В качестве изменяемой нагрузки используется такой же двигатель.

Автоматизированный лабораторный стенд с одной стороны дает возможность провести анализ процессов, например, рабочих характеристик или динамических процессов двигателя, с другой, является мощным инструментом научных исследований в области электрических машин и автоматизированного электропривода [1, 2, 3].

Автоматизированное измерение параметров на лабораторном стенде позволяет автоматически получать статические и динамические характеристики двигателя для последующего их исследования.

Лабораторный стенд состоит из пяти основных блоков: объект исследований; модуль управления; интерфейс управления; интерфейс сопряжения с ПК; программное обеспечение.

В предмете «Теория автоматического управления» основное внимание уделяется переходным процессам. При использовании автоматизированного лабораторного стенда существует возможность ускорить и визуализировать процесс построения переходных характеристик и автоматизировать анализ получаемой с датчиков скорости, тока и напряжения результатов.

Использование программного эмулятора двухлучевого осциллографа [4] снизит стоимость стенда на величину стоимости приборного двухлучевого осциллографа, сэкономит рабочее место. Программный эмулятор имеет наглядный интерфейс, прост в настройке программы для отображения измеряемого сигнала.

Одними из недостатков использования звуковой платы в качестве устройства сопряжения является ограничение измеряемого сигнала по частоте, т. е. можно измерить сигнал любой сложной формы с частотой до 20 кГц. Решением этого недостатка является использование более совершенных звуковых карт, либо разработкой специального устройства сопряжения с высокой разрешающей способности АЦП, чем у интегрированных звуковых плат.

ЛИТЕРАТУРА

1. Вегнер О.Г.. Теория и практика коммутации машин постоянного тока / М.: Энергоатомиздат, 1985. 164 с.
2. Кондратенко Р.Н. Микро-электродвигатели пульсирующего тока постоянного напряжения / М.: Энергия, 1974. 96 с.
3. Гольц М. Е., Гудзенко А.Б., Остеров В.М. Быстродействующие электроприводы постоянного тока с широтно-импульсными преобразователями / М.: Энергоатомиздат, 1986. 184 с.
4. Программный эмулятор двухлучевого осциллографа
<http://polly.phys.msu.su/~zeld/oscill.html>

РЕДАКТОР СХЕМ ДЛЯ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО СИНТЕЗА СВЧ-УСТРОЙСТВ

А.М. Черепанов, студент 5 курса ФВС

ТУСУР, кафедра КСУП, г.Томск

В настоящее время в связи с широким развитием таких областей применения радиоэлектроники, как космическая, персональная и сотовая связь, системы телекоммуникации и др., неуклонно увеличивается количество компаний занимающихся проектированием радиоэлектронных изделий ВЧ- и СВЧ-диапазона. При этом проблема проектирования СВЧ-устройств невозможна без применения средств автоматизированного проектирования.

На данный момент на рынке программного обеспечения существует большое количество программ моделирования линейных электрических цепей (в том числе и СВЧ), такие как Microwave Office (фирма Aplid Wave Research, Inc., США), Aplac, (фирмы Nokia), MicroCap (фирма Spectrum SoftWare), Touchstone (HP, США) и другие [1, 2]. В основном, это разработки крупных компаний, обладающие богатыми возможностями и практически универсальные. К сожалению, указанные программы являются дорогостоящими продуктами, что препятствует их использованию небольшими фирмами и исследовательскими лабораториями, а также университетами в учебных целях. Кроме того, программы имеют некоторые функциональные недостатки и недостаточно гибкий интерфейс пользователя. Отсюда следует вывод о целесообразности создания собственной программы, менее универсальной, но сравнительно дешевой и лишенной указанных недостатков. Оператор, работающий с программой, напрямую общается с интерфейсом пользователя и от его удобства и функциональности зависит эффективность работы.

Цель данной работы – написание программы-редактора схем для системы автоматизированного синтеза СВЧ-устройств.

В настоящее время на кафедре КСУП ведется разработка программы моделирования линейных СВЧ-цепей, предназначенная для вычисления различных характеристик цепи и отображения результатов моделирования. Организация ввода данных в этой программе реализована крайне неудобно. Для устранения данного недостатка возникла необходимость разработки и реализации редактора схем. Данный редактор должен выполнять все основные функции по созданию, редактированию, загрузке и сохранению схем, перенять все достоинства и исключить все недостатки аналогичных редакторов входящий в состав программ MicroCap 7.0, MWOOffice 2002.

Каждый элемент хранит информацию о своей топологии (местоположение на схеме, ориентация (вертикальное или горизонтальное положение), о своих соединениях), а также о своих физических характеристиках.

Основное внимание при разработке модуля уделяться удобству и функциональности пользовательского интерфейса.

Кроме того, программа должна удовлетворять следующим требованиям:

Обеспечить возможность создания схемы с произвольным количеством элементов и любой сложности топологии;

Программа должна обладать интуитивно-понятным интерфейсом, сочетающим в себе простоту и функциональную гибкость, вобравшим в себя основные достоинства аналогичных программ;

Обеспечить сохранение результатов в форме TOUCHSTONE, а также в графическом формате BMP;

Обеспечить гибкий механизм работы с деревом проекта, деревом компонентов и панелью инструментов;

Представление элементов должно иметь грамотное расположение надписей, несущих информационную нагрузку;

Предусмотреть возможность изменения масштаба схемы.

Вследствие того, что программа будет использоваться в программе анализа WinNoise, она должна поддерживать совместимость с этой программой посредством входных и выходных данных, а также иметь гибкую внутреннюю архитектуру для удобства интеграции.

В связи с тем, что программа WinNoise была реализована в среде программирования Microsoft Visual C++ 7.0, то для совместимости с ней реализация данной программы была выбрана эта же среда программирования. Еще одним аргументом в выборе среды программирования явился тот факт, что основным объектом разработок является интерфейс. Простоту его создания обеспечивают среды визуального программирования.

ЛИТЕРАТУРА

1. Фидлер Дж. К., Найтингел К.. Машинное проектирование электронных схем, М.: Высшая Школа, 1985.
2. Guild J., Rein S., Skogrand L.. *EEsof. Touchstone Reference*. Westlace Villige, USA, 1988. 240 p.

ЭЛЕКТРОННЫЙ ИЗМЕРИТЕЛЬ СКОРОСТИ ВЕТРА
Е.Г. Чижик, студент 5 курса ФВС; А.В. Ковинов, аспирант
ТУСУР, кафедра КСУП, г.Томск

В последние годы становится все более актуальной тема прогнозирования метеоусловий, проблема обеспечения безопасности полетов в метеорологическом отношении является наиболее важной.

Одним из наиболее многообещающих путей решения этой проблемы является создание новых методов и технических средств определения основных параметров атмосферы Земли на базе новейших разработок из области электроники и вычислительной техники.

Основная цель разработки и создания лидаров для дистанционного зондирования ветровых потоков – осуществление климатических наблюдений для метеопрогноза и повышение безопасности полетов самолетов в условиях возмущенной атмосферы. Значительную часть необходимых для решения этих задач исходных данных получают при измерении профиля скорости ветра и изучении динамики волновых процессов в нижних слоях атмосферы. Такие явления в атмосфере, как сдвиг ветра, струйные течения, турбулентность, «спутный след», могут быть определены различными методами. На данный момент особый интерес представляют дистанционные (оптические) методы, которые позволяют получать количественную информацию об этих явлениях с высоким пространственным и временным разрешением.

Непосредственное измерение скорости ветра на больших высотах сопряжено со значительными трудностями. В то же время информация об этом чрезвычайно важна для достоверного метеопрогноза. Работа предполагает использование для дистанционного измерения скорости ветров в атмосфере на различных высотах искажения спектра рассеянного излучения оптического диапазона вследствие эффекта Доплера. Для этого необходимо разработать модель взаимодействия лазерного излучения с неоднородностями атмосферы и произвести обработку данных лидарного зондирования.

Измеритель скорости ветра ВДЛ предназначен для:

- оперативной диагностики турбулентных неоднородностей пограничного слоя атмосферы;
- измерения скорости и направления ветра.

Полученные данные могут быть использованы для прогноза распространения в атмосфере газо-аэрозольных выбросов, для нужд авиационной метеорологии при обеспечении взлета/посадки летательных аппаратов, в других областях народного хозяйства, где требуются оперативные сведения и базы данных о состоянии нижнего слоя тропосферы.

Также эти приборы могут применяться в природоохранных структурах и исследовательских организациях.

Приборы данного типа применяются во многих условиях:

– географических: Европейская часть России, Сибирь, Средняя Азия, Атлантический океан;

климатических: 20–95% влажность, $-500^{\circ}\text{C} \dots +500^{\circ}\text{C}$;

производственных: аэропорты, промышленные площадки, борт судна, полигоны различных ведомств и назначений.

Прибор имеет следующие технические характеристики:

Диапазон измерений	от 0,1 до 30 м/с
Точность	не менее 0,1 м/с
Ошибка измерения	2 %
Температурный диапазон	$-50 \dots +50^{\circ}\text{C}$;
Размеры рабочей поверхности датчика	10 × 10 мм

Рассматривая проблему в целом можно прийти к выводу о том, что на сегодняшний день еще не существует технических возможностей для создания прибора с более высокими параметрами.

ЛИТЕРАТУРА

1. Козолупенко В.П., Кунцевич Б.Ф., Малюта Д.Д., Межесов В.С., Стрельцов А.П., Чураков В.В. Квантовая электроника. 1987 №14, 328 с.

ИНТЕГРИРОВАННЫЙ ИНСТРУМЕНТ ДЛЯ СИНТЕЗА СОГЛАСУЮЩИХ ЦЕПЕЙ В СРЕДЕ ПРОЕКТИРОВАНИЯ СВЧ-УСТРОЙСТВ MICROWAVE OFFICE

Ф.И. Шеерман, аспирант; А.С. Барышников, студент 4 курса;

М.В. Нехорошев, студент 4 курса; В.А. Вьюшков, инженер;

Л.И. Бабак, доц. каф. КСУП

ТУСУР, НПФ Микран, г. Томск, sfi1493@ms.tusur.ru

Описана интеграция программы синтеза согласующих цепей GENESYN и системы автоматизированного проектирования СВЧ устройств Microwave Office.

На сегодняшний момент в большинстве САПР СВЧ устройств нет встроенных средств синтеза (определения структуры и элементов) согласующих (СЦ) и корректирующих цепей. Поэтому для решения задачи синтеза СЦ разработчику приходится прибегать к специализированным программам (таким как MultiMatch, RF-Compiler, ZMatch и др.) При этом он вначале с помощью системы моделирования на ряде заданных частот вычисляет импеданс согласуемых генератора и нагрузки и затем вводит (обычно вручную) эти данные в программу синтеза.

Полученную в результате синтеза цепь (или несколько цепей) пользователь должен внести в систему моделирования для оценки характеристик всего устройства. Этот процесс в случае его частого повторения весьма неудобен, кроме того, вероятны ошибки на этапах ввода исходных данных в программу синтеза и полученной схемы СЦ – в систему моделирования.

В данной работе предложен и реализован способ интеграции программы синтеза СЦ GENESYN [1], разработанной на кафедре КСУП ТУСУР, и популярной системы автоматизированного проектирования СВЧ устройств – Microwave Office (MWO) фирмы AWR [2].

Интеграция выполнена на основе так называемого помощника (Wizard'a) среды MWO. Wizard представляет собой COM объект с реализованным стандартным интерфейсом IGenesynWizard (рис. 1), который поддерживается средой MWO. Wizard можно вызывать из MWO, он выполняет необходимые действия и по завершению возвращает управление в MWO. В нашем случае основной задачей Wizard'a является управление процессом проектирования СВЧ устройств с СЦ, включая организацию взаимодействия программ GENESYN и MWO и обмена данными.

После вызова Wizard'a он решает задачу по сбору исходных данных – значений импеданса генератора и нагрузки на выбранных частотах, которые рассчитываются при помощи среды MWO. По окончании расчета вызывается программа GENESYN посредством интерфейса

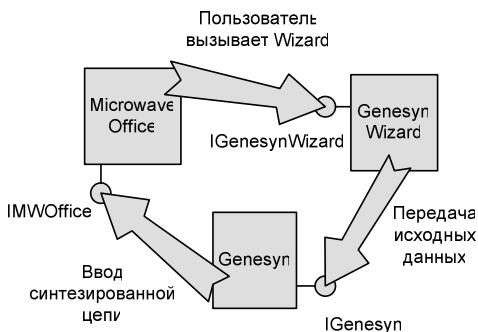


Рис. 1. Схема взаимодействия объектов

автоматизации IGenesyn, в нее автоматически передаются исходные данные. В программе GENESYN пользователь синтезирует СЦ и затем результат возвращается в среду MWO через вызовы соответствующих функций интерфейса IMWOffice (рис. 1).

Для реализации описанной схемы проектирования были написаны следующие программные блоки:

1. Wizard, реализующий механизмы сбора исходных данных и пользовательский интерфейс для управления процессом.
2. COM-Automation интерфейс для программы GENESYN, с помощью методов которого осуществляется вызов программы GENESYN и ввод исходных данных

3. Настройка для языка описания электрических схем SRL, используемого в программе GENESYN. Данная настройка по исходному тексту в формате SRL формирует схему цепи в среде MWO.

Внешний вид интерфейса Wizard'a представлен на рис. 2.

Рассмотрим процесс проектирования СВЧ-устройства с СЦ. После открытия проекта MWO и вызова Wizard'a пользователь последовательно указывает имя схемы СВЧ-устройства, в которую должна включаться СЦ, способ согласования (максимальный коэффициент передачи, минимальный шум) и значения частот в полосе согласования. После этого на выбранную схему автоматически помещается изображение четырехполусной подцепи – будущей СЦ (рис. 3). Затем пользователь соединяет подцепь с «левой» и «правой» частями схемы – эквивалентными генератором и нагрузкой, которые необходимо согласовать. При повторном вызове Wizard'a с помощью MWO на выбранных частотах рассчитываются импедансы генератора и нагрузки, формируется стандартный файл данных программы GENESYN (*.ma2), автоматически вызывается сама программа и в нее загружается созданный файл. Далее пользователь синтезирует СЦ с помощью программы GENESYN, результатом является описание СЦ в формате языка SRL.

После вызова специальной функции в меню программы GENESYN описание СЦ на языке SRL преобразуется в последовательность команд для ввода этой цепи в среду MWO, схема полученной СЦ заносится в MWO в виде подцепи. Теперь можно сразу моделировать СВЧ-устройство с подключенной синтезированной СЦ.

Описанный инструмент позволяет значительно ускорить, упростить и сделать более удобным процесс проектирования СВЧ-устройств с СЦ. В дальнейшем планируется реализовать по рассмотренной схеме интегрированные инструменты для автоматизированного синтеза корректирующих цепей и даже целых усилительных каскадов.

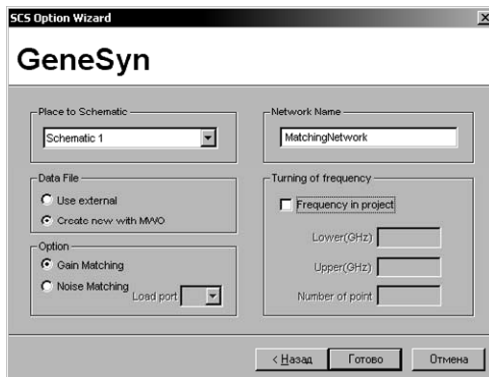


Рис. 2. Внешний вид Wizard'a

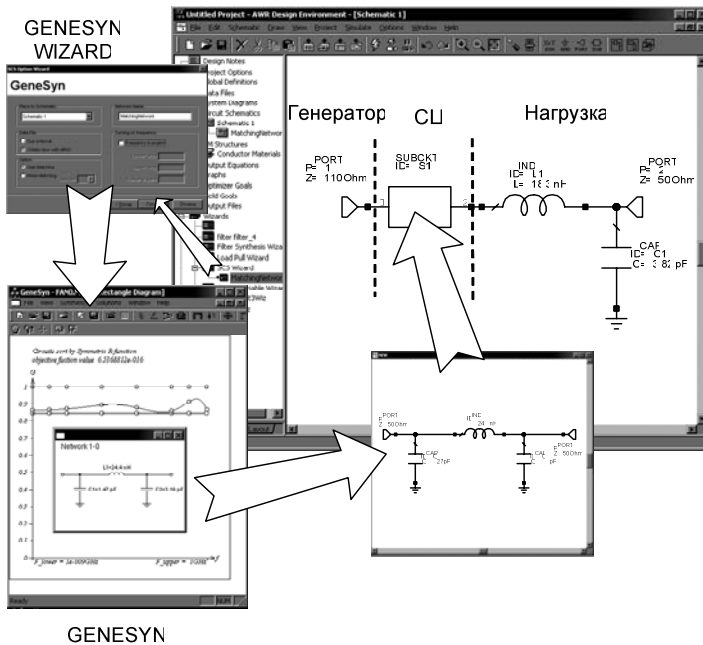


Рис. 3. Схема процесса проектирования СВЧ-устройства с СЦ

ЛИТЕРАТУРА

1. Бабак Л.И., Вьюшков В.А. Автоматизированный синтез согласующих цепей на основе генетического алгоритма // В сб. докладов научно-техн. конф. «Электронные средства и системы управления», Томск: изд-во Института оптики и атмосферы СО РАН. 2005. Ч. 2. с. 102–105.
2. Microwave Office, Applied Wave Research, Inc. [электронный ресурс], – режим доступа: <http://www.appwave.com>.

УПРАВЛЕНИЕ ПОСТАВКАМИ НЕСКОЛЬКИХ ВИДОВ ТОВАРОВ

Е.А. Штихлинг, студент 4 курса, ФПМиК;

Г.Н. Решетникова, к.т.н., доцент

Томский государственный университет, г. Томск,

FPMJon@mail2000.ru

При управлении поставками важную роль играют скорость и адекватность принятых решений относительно сложившейся ситуации.

В связи с этим разработка математических систем управления в совокупности с применением вычислительной техники приобретает все большую актуальность.

Пусть осуществляется поставка нескольких видов товаров. Процесс поставок будем описывать линейной непрерывной стохастической системой вида [1]:

$$\dot{x}(t) = \bar{A}(t)x(t) + \bar{B}(t)u(t) + \bar{F}(t)q(t), \quad x(t_0) = x_0, \quad (1)$$

где $x(t) = (Z(t), V(t), W(t))^T$ – вектор состояния, компоненты которого имеют следующий смысл: $Z(t)$ – объем товара на рынке; $V(t)$ – объем товара у покупателя; $W(t)$ – чистая прибыль; $u(t)$ – вектор управления, задающий темп поставок; $q(t)$ – вектор, характеризующий влияние случайных факторов в модели, который будем считать гауссовским шумом с заданными характеристиками. Матрицы $\bar{A}(t)$ и $\bar{B}(t)$ в (1) имеют следующий вид:

$$\bar{A}(t) = \begin{pmatrix} -N(C)Y(t) + N(C)\varphi_v(t) - K_1 & N(C)\varphi_z(t) & 0 \\ N(C)Y(t) - N(C)\varphi_v(t) & -N(C)\varphi_z(t) - K_2 & 0 \\ (CN(C)Y(t) - CN(C))\varphi_v(t) - K_3 & -CN(C)\varphi_z(t) & 0 \end{pmatrix}, \quad (2)$$

$$\bar{B}(t) = \begin{pmatrix} 1 & 0 & -\frac{1}{C} \end{pmatrix}^T. \quad (3)$$

В (2), (3) $Y(t)$, $\varphi_v(t)$, $\varphi_z(t)$ – функции, описывающие потенциальный спрос, поведение покупателя и ситуацию на рынке; $C, K_1, K_2, K_3, N(C)$ – коэффициенты, характеризующий торговую наценку, скорость потребление, плату за хранение, порчу товара и скорость продаж соответственно. $\bar{F}(t)$ – матрица, задающая влияния случайных факторов в модели (1).

Темп поставок в момент $t_k = t_0 + k\Delta t$, будем формировать на основе минимизации локального критерия вида:

$$J(k) = \frac{1}{2} M \{ (x(k+1) - x_z(t_k))^T C (x(k+1) - x_z(t_k)) + u^T(k) D u(k) \}, \quad (4)$$

где $x_z(\cdot)$ – состояние, соответствующее значению желаемой прибыли; $C \geq 0, D > 0$ – весовые матрицы, $A(k), B(k)$ – матрицы дискретной модели, эквивалентной (1). Тогда:

$$u(k) = -\left(B^T(k)CB(k) + D\right)^{-1} B^T(k)C[A(k)x(k) - x_z(k)]. \quad (5)$$

Выражение (5) отражает общий объем поставок всего товара. Объем каждого из видов товаров в отдельности можно определять, напри-

мер, решая, задачу оптимизации на каждом такте k в процессе формирования поставок.

Численное моделирование осуществлялось с шагом $\Delta t=1$ день по данным поставок двух видов товаров в течении 6 месяцев при слежении за состоянием, характеризующим увеличение прибыли на 5%. Результаты моделирования представлены на рис. 1, где сплошной линией изображена прибыль, полученная в результате моделирования, а точками прибыль, за которой осуществляется слежение.

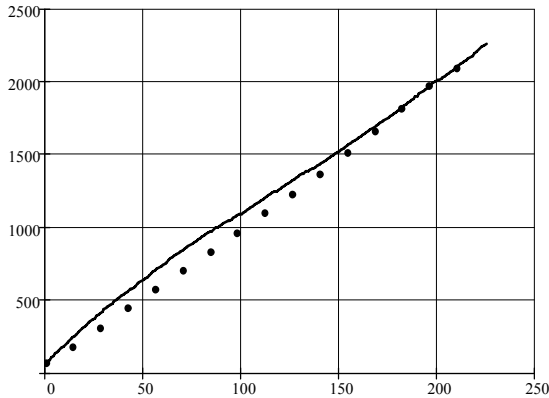


Рис. 1

Для определения объема поставок каждого вида товаров на k такте, решаем следующую задачу оптимизации:

$$\begin{aligned}
 & N(C)_1 \cdot u(k)_1 + N(C)_2 \cdot u(k)_2 \Rightarrow \frac{\min}{u(k)_1, u(k)_2} \\
 & N(C)_1 \cdot u(k)_1 + N(C)_2 \cdot u(k)_2 \leq \alpha \\
 & u(k)_1 > 0, \\
 & u(k)_2 > 0, \\
 & u(k)_1 \geq u(k)_1, \\
 & u(k)_1 + u(k)_2 \leq U(k) \\
 & w(k)_1 + w(k)_2 = W(k)
 \end{aligned}
 , \quad (6)$$

где $N(C)_i$, $u(k)_i$, $w(k)_i$, $i=1,2$ – коэффициенты характеризующие скорости продаж, объемы поставляемой продукции и чистую прибыль для каждого из товаров соответственно, α – точность решения задачи оптимизации, включающая ограничение на минимальный объем поставляемой продукции.

В отличие от подхода, предложенного в [2], когда модель процесса поставок записывалась с помощью блочных матриц, что существенно усложняет задачу, в настоящей работе формируются поставки всей продукции одновременно, а затем определяется объем поставок каждого из видов товаров, таким образом, чтобы в совокупности их реализация приносила желаемую прибыль. Заметим, что при этом можно ставить разные задачи оптимизации в зависимости от приоритетов в работе конкретного поставщика.

ЛИТЕРАТУРА

1. Решетникова Г.Н. Моделирование систем: учеб. пособие /Г.Н. Решетникова; Федеральное агентство по образованию, Томский Государственный университет систем управления и радиоэлектроники – Томск: Томский государственный университет систем управления и радиоэлектроники, 2005. 261 с.
2. Старых А.А., Решетникова Г.Н. Формирование следящей системы управления поставками при неполной информации.: Научная сессия ТУСУР-2005, 2005. 319 с.

ЭЛЕКТРОННЫЙ ПНЕВМОГРАФ **Ф.К. Щербаков, студент 5 курса ФВС** *ТУСУР, кафедра КСУП, г.Томск*

При изучении многих болезней выяснилось [1], что одни люди вдыхают слишком много кислорода и у них образуется в организме недостаточный процент CO_2 , другие дышат недостаточно интенсивно и у них из-за «тупых» альвеол наблюдаются болезни кислородного голодания, такие, как бронхиальная астма, гипертония. Проведенные эксперименты объясняют и случаи смерти актеров в момент произнесения страстных монологов. Причина их – не нервные и сердечные болезни, а непомерно длительное кислородное голодание организма, а также перенапряженность работы актера, оратора, нарушающая обмен веществ, нервную деятельность и мозговое кровообращение. Следовательно, изучение процессов дыхания в различных рабочих режимах является актуальной задачей. Для этого требуется прибор, способный измерять совокупности параметров дыхательного цикла (паттерна), исследовать динамику параметров последовательных дыхательных циклов за достаточно длительный период.

Существующие методы измерения совокупности параметров дыхательного цикла (паттерна) сопряжены с «инвазивным» наложением на верхние дыхательные пути загубников, лицевых масок, носовых зажимов, что приводит к искажению естественного дыхательного паттерна у обследуемого и вызывает у него чувство дискомфорта.

Разработан пневмограф, в основу работы которого положен индукционный принцип измерения расстояний и линейных перемещений, использующий зависимость ЭДС, наведенной в приемной катушке, от расстояния между приемной и передающей (возбуждающей) катушками [2].

В процессе дыхания грудь и живот вносят различный вклад в объем вдыхаемого-выдыхаемого воздуха (торакальный и абдоминальный вклад) [3]. Этот вклад зависит от состояния и положения испытуемого. Поэтому пневмограф был разработан 2-х канальным.

Прибор разработан для контроля и измерения параметров дыхания. Процесс дыхания осуществляется при помощи грудных мышц и мышц живота. Поэтому катушка возбуждения и приемная катушка первого канала крепятся на уровне груди (катушка возбуждения – со стороны спины, приемная катушка – спереди), а второго – на уровне живота. Выходы каналов подключаются через усилители к соответствующим входам микроконтроллера. Работа прибора основана на изменении ЭДС индукции магнитного поля, наводимой в приемной катушке за счет протекающего в катушке возбуждения переменного тока, с изменением расстояния.

Структурная схема пневмографа представлена на рис. 1.

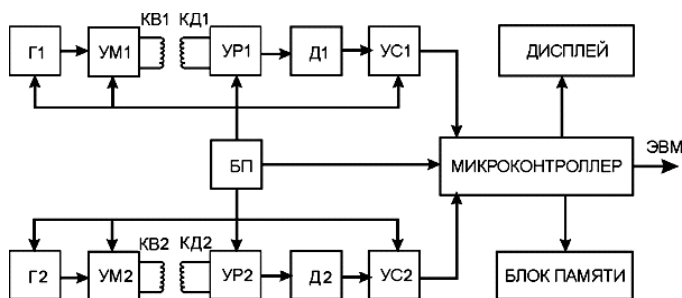


Рис. 1. Структурная схема электронного пневмографа

Прибор состоит из двух идентичных приемо-передающих каналов.

С помощью генератора синусоидальных колебаний Г1 вырабатывается переменное напряжение частотой 5000 Гц. С целью устранения взаимного влияния каналов частоты генераторов Г1 и Г2 должны отличаться примерно в 1,5 – 2 раза. Форма колебаний выбрана синусоидальной, чтобы не создавались взаимные помехи за счет высших гармоник.

Усилитель мощности УМ1 служит для создания в катушке возбуждения КВ1 переменного тока, достаточного для надежной работы прибора. Обычно этот ток выбирается максимально возможным для

данной катушки возбуждения, лишь бы катушка не перегревалась. За счет взаимной индукции в катушке датчика (приемной катушке) КД1 наводится ЭДС.

Напряжение с катушки подается на резонансный усилитель УР1, настроенный на частоту генератора Г1. С выхода усилителя переменное напряжение подается на детектор Д1. Через устройство сдвига нуля УС1 выпрямленное напряжение, зависящее от расстояния между катушками, подается на вход АЦП микроконтроллера, который оцифровывает значение напряжения в код и сохраняет его в блоке памяти.

Устройство сдвига нуля служит для установки нулевого напряжения на выходе прибора при переводе возбуждающей катушки и катушки датчика в исходное положение.

Генераторы, усилители мощности и катушки возбуждения составляют передающую часть прибора, остальные узлы – приемную часть. Блок питания БП вырабатывает все необходимые для работы прибора напряжения.

Результаты измерений напряжений, в сумме представляющие собой пневмограмму, сжимаются специальным алгоритмом и хранятся в памяти устройства.

Передача данных в ЭВМ осуществляется посредством интерфейса, встроенного в микроконтроллер. Пневмограмма так же может выводиться на дисплей прибора.

ЛИТЕРАТУРА

1. *Филатов В.Ф.* Последствия неправильного дыхания. Успехи физиологических наук, 1994, №7. с. 34–39.
2. *Фурно Г.* Микрокомпьютерные медицинские системы. Проектирование и применения. М.: Мир, 1983. 544 с.
3. *Миняев В.И.* Зависимость соотношений абдоминальных и торакальных вкладов в объемы и емкости легких от позы. Успехи физиологических наук, 1995, №2. с. 41–45.

СИСТЕМА МОНИТОРИНГА ПРОГРАММНОГО И АППАРАТНОГО ОБЕСПЕЧЕНИЯ СЕРВЕРНЫХ СТАНЦИЙ. СЕРВЕРНАЯ ЧАСТЬ

*Е.А. Юндин, студент 5 курса ФВС;
В.В. Одионов, к.т.н., доцент кафедры КСУП
ТУСУР, кафедра КСУП, г. Томск*

Серверная часть. В связи с тем, что отслеживать информацию необходимо с большого количества контролируемых серверных станций (контролируемых серверов), система мониторинга будет иметь клиент – серверную модель. Это подразумевает наличие в разрабаты-

ваемой системе клиентской и серверной части [1, 2, 3]. Контролируемый сервер в данном контексте подразумевает собой серверную станцию, подключенную к сети Интернет и выполняющую некую полезную работу.

Серверная часть разрабатываемой системы принимает, аккумулирует и выводит текущую информацию об аппаратной и программной части серверных станций. К аппаратной части серверных станций можно отнести загрузку ЦП, ОЗУ, ПЗУ, своп, а так же информацию о сетевом интерфейсе. К программной части серверных станций относятся такие сервисы как FTP, HTTP (веб-сервер Apache), СУБД MySQL [2].

Функции серверной части разрабатываемой системы:

- загрузка настроек из файлов конфигурации
- установление соединения с клиентской частью (по запросу) и создание для нее нового процесса
- обработка запроса, принятие данных от клиентской части
- разбор полученной информации и запись ее в БД
- предоставление пользовательского интерфейса для просмотра отслеживаемой информации локально и удаленно

Многопроцессный сервер. Существует два вида серверов – последовательный (итеративный) и параллельный (много процессный). Для простого сервера, как сервер времени и даты, допустимо использование первого варианта. Но когда обработка запроса клиента занимает больше времени, нельзя связывать один сервер с одним клиентом, поскольку необходимо обрабатывать множество клиентов одновременно. Решением является сервер, порождающий дочерний процесс для каждого клиента. Именно такое решение используется в разрабатываемой серверной части.

Модель интерфейса. Система имеет интерфейс для просмотра отслеживаемой информации [3]. Есть возможность просмотра этой информации локально (на машине, где установлена серверная часть приложения), так и удаленно (с любого сетевого узла снабженного Интернет браузером) т.е. используется веб-интерфейс. Для обеспечения такой функциональности будет использоваться СУБД MySQL, Web-сервер Apache и сценарии на языках PHP/Perl/HTML [1].

Проделана работа по изучению проблемной области. Разработана концепция создаваемой системы мониторинга. Определена структура и алгоритмы работы серверной части. К последующей работе можно отнести реализацию серверной части и веб-интерфейса.

ЛИТЕРАТУРА

1. *Стивенс У.Р.* UNIX разработка сетевых приложений. СПб. Питер, 2004 1086 с.
2. *Уолтон Шон* Создание сетевых приложений в среде Linux Москва: Вильямс 2001. 464 с.
3. *Одинокое В.В.* Операционные системы. Учебное пособие. Томск ТМЦДО, 2005. 246 с.

СЕКЦИЯ 11

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель – **Ильющенко В.Н.**, проректор по ИР ТУСУР,
зав. каф. РЗИ, д.т.н., профессор;
зам. председателя – **Загоскин В.В.**, к.ф.-м.н., доцент каф. РЗИ*

ЗАЩИТА ОПТИЧЕСКИХ ДИСКОВ КАК РЕШЕНИЕ ПРОБЛЕМЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

***А.Р. Аюпова, студент 4 курса; А.Р. Баширова, студент 4 курса;
Л.А. Кромина, преподаватель-стажер кафедры АСУ
Кумертауский филиал Уфимского Государственного
Авиационного Технического Университета,
республика Башкортостан, г. Кумертау,
тел. 8(34761) 4-23-10, Luyda_kr@mail.ru.***

Актуальность обеспечения защиты оптических (лазерных) дисков от несанкционированного применения в настоящее время постоянно возрастает, в связи с тем, что информационные ресурсы все больше подвергаются угрозам утраты носителей и нарушения целостности информации. Информация открыто стала товаром, и появилась реальная опасность ее расхищения за неимением способов защиты на носителях.

В данной работе рассматриваются вопросы, связанные с решением поставленной задачи для лазерных дисков (CD). Задача связана с предотвращением несанкционированного распространения объектов авторского права с неограниченной кратностью воспроизведения.

Для реализации поставленной задачи необходимо обеспечить выполнение следующих условий: а) незаконная копия CD должна отличаться от оригинала, причем необязательно записанными данными, достаточно обеспечить отличие свойств носителя; б) устройство воспроизведения (УВ) должно различать свойства носителя и отклонять запрос на воспроизведение диска, аутентифицированного как «чужой». Отличительная особенность диску должна придаваться в процессе выпуска информационного продукта. Взаимодействие диска с устройством воспроизведения должно быть бесконтактным и состоять во взаимной аутентификации.

Решением поставленной задачи можно рассмотреть два способа, взаимодействие которых обеспечить надежную защиту лазерных дисков от несанкционированного применения:

1. Устройство защиты электронного модуля. Высокий риск для устройств хранения и применения ключевой информации вызывает их потеря или хищение, поэтому носитель такой информации должен обладать следующими свойствами: а) устойчивостью к бесконтактным методам проникновения; б) устойчивостью к проникновению контактными методами, включая декомпозицию (разборку) изделия; в) возможностью самотестирования, включая контроль целостности содержащейся информации, а также возможность активной реакции на проникновение внутрь устройства; г) приемлемыми массогабаритными и ценовыми показателями.

Данное изделие позволит решить проблему, связанную с тем, что поставщик таких изделий не сможет повлиять на их защитные свойства, даже с учетом своих знаний о техническом цикле их производства. Основу замысла создания защищенного ключевого носителя составляют следующие принципы: 1. содержимое регистров внутренней памяти носителя сохраняется только в том случае, когда расположенная внутри схема защиты регулярно, с заданной периодичностью подтверждает целостность внешней оболочки и неизменность других критичных параметров носителя; 2. параметры схемы защиты случайным образом создаются в процессе изготовления и меняются от одного изделия к другому по схеме равновероятного выбора с возвращением, так что любая полнота знаний об устройстве изделия не обеспечит противнику возможность блокировки схемы защиты и проникновения внутрь носителя; 3. механическая защита интегрируется с контуром схемы электронной защиты так, что декомпозиция изделия становится невозможной.

2. Бесконтактная интегральная схема (БКИС). Бесконтактная интегральная схема для встраивания в оптический диск должна иметь интерфейс информационного и энергетического взаимодействия в оптическом диапазоне электронного излучения. Основные вычислительные функции микросхемы – криптографические преобразования, а в энергонезависимых регистрах БКИС должны храниться производные ключи для этих преобразований. Энергетическое взаимодействие осуществляется посредством фотовольтаической полупроводниковой структуры, которая преобразует падающее на не электромагнитное излучение оптического диапазона в электрическую энергию. Информационное взаимодействие – управляемых напряжением оптически активных структур. Демодуляция сигнала осуществляется на фотоприемнике устройства воспроизведения.

Результатом механизма взаимодействия диска и УВ. На диске могут храниться только производные ключи, так как уровень защищенности ключевой информации всегда будет ниже таковой у УВ. Исходны-

ми данными для запуска данного механизма является информация, связанная с автором, наименованием произведения, изготовителем, а также производные ключи. После изготовления диска для обнаружения сигнал «свой», в энергонезависимые регистры БКИС записываются необходимые исходные данные. Для восприятия БКИС этих данных используют группу фотовольтаических элементов. С целью предотвращения злоупотребления запись осуществляется однократно в контролируемых условиях. После переводят БКИС в режим «запрет записи». Такой режим может сопровождаться нарушением возможности приема информации фотовольтаическими элементами.

На первом этапе воспроизведения диска фотовольтаические элементы БКИС преобразуют падающее на них электромагнитное излучение оптического диапазона в электрическую энергию, эта энергия накапливается до нужного значения, обеспечивающего функционирование БКИС. После чего БКИС вырабатывает некоторый сигнал, который подтверждает легальность диска и формирует модулирующую структуру. Данная структура и изменяет форму отраженного сигнала. Сигнал воспринимается приемником устройства воспроизведения, демодулируется и поступает на электронный модуль УВ. В случае подтверждения легальности диска начинается воспроизведение, в противном случае – диск не воспроизводится. Таким образом, защита диска может обеспечиваться встраиванием в него описанной бесконтактной микросхемы и встраиванием в УВ электронного модуля в защищенном исполнении, который позволит осуществить анализ и обработку сигналов БКИС. Существует мнение, что уход от «пиратской» продукции приведет к резкому росту стоимости дисков. Увеличение продаж лицензионных дисков приведет к снижению цен на них за счет снижения «компенсационной» части цены, и при этом к росту доходов владельцев авторских прав.

На основе полученных результатов можно сделать вывод, что проблема защиты оптических дисков от несанкционированного применения до сих пор оставалась не решенной в связи с тем, что во всех предлагаемых процедурах диск оставался пассивным. Предложенная бесконтактная интегральная схема создает принципиальную возможность решения этой проблемы, причем без значительных переделок механической и оптической частей дисководов. Устройство защиты электронного модуля позволяет отказаться от асимметричной криптографии в пользу применения производных ключей, используя защитные коды аутентификации, низкая вычислительная сложность которых позволяет разработать аппаратуру с приемлемыми характеристиками. Использование этих устройств нацелено на решение таких вопросов, как защита

авторских прав, информационных ресурсов, обеспечение конфиденциальности информации.

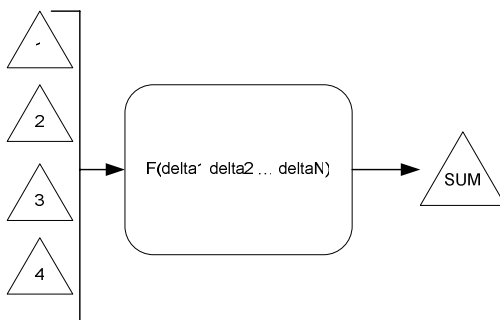
ЛИТЕРАТУРА

1. Лойко В.И. Информационные системы и технологии. М.: Финансы и статистика, 2003. 416 с.
2. Пятибратов А.П. Вычислительные системы, сети и телекоммуникации. М.: Финансы и статистика, 2003. 512 с.
3. Информационная безопасность: Информационные технологии/ под ред. И.С. Павлова, Ю.Н. Рыбакова// теоретический и прикладной научно-технический журнал № 10. 2005.

ИДЕНТИФИКАЦИЯ ОБЪЕКТОВ В АСИНХРОННЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Д.Ю. Копытков, аспирант каф. РЗИ
ТУСУР, г. Томск, E-mail: pisces@inbox.ru

В асинхронных распределенных системах каждый участник репликации локально работает со своей копией данных в заданный интервал времени $t_2 - t_1$, по истечению которого происходит синхронизация изменений сделанных каждым участником репликации, с разрешением конфликтных ситуаций. Как правило, центром синхронизации выступает отдельный сервер, одним из модулем которого является интеллектуальный сумматор, на «вход» которого поступает сделанные изменения (дельты, реплики) (рисунок), на выходе которого будет суммарная дельта.



Функция преобразования дельт

Каждая дельта содержит следующие данные:

- 1) идентификатор записи;
- 2) изменения сделанные в записи.

Проблема заключается в том, что функция вычисляется для записи, уже подвергнутой изменениям, а изменения сделанные для данной записи в каждом филиале могут быть различными. Таким образом, функцию создания идентификатора записи должна обладать следующими параметрами:

$$X(REC + \Delta_i) = X(REC + \Delta_j), \quad (1)$$

где $X(R)$ – функция создания идентификатора записи; REC – исходная запись; Δ_i – сделанные изменения i -м участником репликации; Δ_j – сделанные изменения j -м участником репликации.

В результате, использовать хеш-функции в роли функции создания идентификаторов записей является неприемлемый. Т.к. хеш-функции [1] – это преобразование, получающее из данных произвольной длины некое значение (свертку) фиксированной длины. Простейшими примерами являются контрольные суммы (например, `crc32`). Одним из основных правил хеш-функций является следующее правило: для любого фиксированного x вычислительно невозможно найти другой $x' \neq x$, такой что $H(x') = H(x)$, что противоречит утверждению (1).

Так же недопустимо использование порядковых номеров записей. Данный способ идентификации прост в техническом исполнении, но скрывает в себе ряд проблем:

а) в связи с тем, что каждый участник репликации работает локально со своей копией данных, то возможна ситуация, при которой в один интервал времени несколькими участниками репликации будет создана одна и та же запись, но основываясь на данном алгоритме идентификации записей, каждой записи будет присвоен свой порядковый номер

б) привязывание к порядковым номерам записей, например в СУБД CDS/ISIS, недопустимо, вследствие того, что после реорганизации файла документов, у записей будут совершенно другие номера, а учитывая тот факт, что каждый участник репликации будет проводить данную процедуру с локальными данными то возможно, что номера записей у различных участников репликации не будут совпадать.

Наиболее «привлекательной» функцией в роли функции создания идентификаторов записи является функция создания алгоритмических алкодов.

Под алгоритмическим алкодом [2–3] (АЛКОД) понимается идентификатор документа, который создается по определенным правилам (алгоритму) и однозначно идентифицирует источник.

В АЛКОД включаются символы из элементов записи в последовательности, определенной алгоритмом его формирования. При этом по-

строение АЛКОДа в автоматизированном режиме осуществляется на основе алгоритма и данных записи.

АЛКОД может включать: буквы кириллического и латинского алфавитов; цифры арабские.

При кодировании в АЛКОД не включаются следующие знаки и символы:

- знаки препинания – точка, точка с запятой, запятая, двоеточие, дефис, вопросительный и восклицательный знаки, кавычки, апостроф;
- математические знаки;
- все виды скобок;
- прочие знаки – параграф, наклонная черта, номер, амперсant;
- лигатуры;
- греческие символы;
- другие знаки – доллар, фунт стерлингов и т.д.

Результатом функции построения идентификаторов на основе алгоритмических кодов, будет строка, состоящая из данных, мало подверженных изменению в процессе жизни записи в распределенной среде

$$ID = G(A, R), \quad (2)$$

где ID – идентификатор записи; $G(A, R)$ – функция построения идентификатора записи на основе алгоритмических кодов; A – алгоритм построения алкода; R – запись, источник.

Задача создания АЛКОДа сводится к получению одинаковых значений ID для записей одного и того же документа, описанного (созданного, измененного) разными работниками в филиалах учатников репликации, но в то же время, к получению различных значений ID для разных документов.

Таким образом, в качестве функции получения идентификаторов записи целесообразно использовать функцию основанную на алгоритмических кодах. Данная функция позволяет получить одинаковые идентификаторы для записей подвергающихся изменению, что актуально для распределенных сред, основанных на асинхронных распределенных системах, но в то же время различные значения для разных документов.

ЛИТЕРАТУРА

1. ГОСТ Р 34.11-94. Вычисление хэш-функции
2. ГОСТ 7.14-98. Формат для обмена информацией. Структура записи.
3. ГОСТ 7.19-85. Коммуникативный формат для обмена библиографическими данными на магнитной ленте.

ПРОБЛЕМЫ ОБЪЕДИНЕНИЯ ОДНОВРЕМЕННО ИЗМЕНЕННЫХ ДАННЫХ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ С АСИНХРОННЫМ ТИРАЖИРОВАНИЕМ

*Д.Ю. Копытков, аспирант каф. РЗИ
ТУСУР, г. Томск, E-mail: pisces@inbox.ru*

В настоящее время существует два основных направления развития технологий репликации (тиражирования) данных – это синхронные и асинхронные модели репликации. Если к технологиям, основанным на синхронных моделях, требуется, как правило, постоянно активный канал связи между узлами-участниками репликации на время выполнения распределенной транзакции, тем самым каждый участник репликации после выполнения транзакции сразу же узнает о сделанных изменениях, то проблема одновременного изменения данных не возникает.

В асинхронных моделях напротив, каждый участник репликации работает со своей локальной копией данных, синхронизация которых происходит в заданный интервал времени на сервере репликации, в результате, сервер репликации в асинхронных моделях узнает о сделанных изменениях данных, только после получения соответствующих реплик (дельт) с узлов участников репликации.

Таким образом, перед сервером репликации, после получения всех дельт с узлов, стоит задача объединения реплик (дельт) с целью создания суммарной реплики (см. рисунок в предыдущей статье).

Если каждый филиал во время работы с локальными данными не изменял одни и те же данные, то проблемы создания суммарной реплики (дельты) не возникает и в качестве функции объединения реплик достаточно использовать формулу 1.1:

$$f(\Delta_1, \Delta_2, \dots, \Delta_n) = \Delta_1 + \Delta_2 + \dots + \Delta_n. \quad (1)$$

Но рассмотрим ситуацию, когда несколько участников распределенной системы изменили одни и те же данные (в частности, можно рассматривать изменения одной и той же записи БД). Ограничиться формулой (1) невозможно, т.к. несколько из дельт $(\Delta_1, \Delta_2, \dots, \Delta_n)$ затрагивают изменения одних и тех же данных (конфликтующие дельты). Следовательно, возможны следующие функции объединения реплик:

1) Выбор дельты с максимальным уровнем привелегий из конфликтующих дельт.

$$f(\Delta_1, \Delta_2, \dots, \Delta_n) = L(\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn}) + \sum_{i, i \neq k1, k2, \dots, kn}^n \Delta_i, \quad (2)$$

где $L(\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn})$ – функция выбора дельты с максимальным уровнем привилегий; $\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn}$ – конфликтующие дельты.

Данную функцию возможно использовать, если существует возможность установить каждому участнику репликации уровень привелегий (ранг). Как правило, это возможно в следующих случаях:

1) каждый участник репликации является внутренней структурой одной организации;

2) участниками репликации являются отдельные корпорации (организации) объединенные по определенной договоренности, в качестве договоренности может выступать координационный центр, выставяющий ранг участнику репликации как по уровню «грамотности» делаемых изменений, так и по другим соображениям.

2) Выбор дельты с максимальным объемом делаемых изменений или вносимых данных из конфликтующих дельт.

$$f(\Delta_1, \Delta_2, \dots, \Delta_n) = O(\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn}) + \sum_{i, i \neq k1, k2, \dots, kn}^n \Delta_i, \quad (3)$$

где $O(\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn})$ – функция выбора дельты с максимальным объемом делаемых изменений или вносимых данных; $\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn}$ – кон-

фликтующие дельты; $\sum_{i, i \neq k1, k2, \dots, kn}^n \Delta_i$ – сумма всех дельт, исключая кон- фликтующие.

3) Выбор дельты по времени создания дельты из конфликтующих дельт (формула 1.4).

$$f(\Delta_1, \Delta_2, \dots, \Delta_n) = T(\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn}) + \sum_{i, i \neq k1, k2, \dots, kn}^n \Delta_i, \quad (4)$$

где $T(\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn})$ – функция выбора дельты по времени создания дельты.

В качестве функции T может являться функция выбирающая как дельту, содержащую наиболее ранние изменения, так и с наиболее поздними. В случае использования данной функции необходимо выполнение двух условий:

1) синхронизация часов каждого участника репликации;

2) работа функции T осуществляется по глобальному времени, например Гринвичу. Данное требование возникает в случаях расположения участников проекта в различных часовых поясах.

4) Объединение данных из конфликтующих дельт используя специальную функцию (формула 1.5).

$$f(\Delta_1, \Delta_2, \dots, \Delta_n) = F(\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn}) + \sum_{i, i \neq k1, k2, \dots, kn}^n \Delta_i, \quad (5)$$

где $F(\Delta_{k1}, \Delta_{k2}, \dots, \Delta_{kn})$ – специальная функция объединения данных.

Данный вид функции, представляется наиболее сложным из приведенных выше и предполагает затрагивание внутренней структуры данных в используемой системе репликации.

В заключении необходимо отметить, что перед использованием асинхронной модели тиражирования данных, необходимо достаточно серьезно подойти к выбору функции объединения реплик, учитывать все требования участников репликации, для избежания потери данных, в силу отсутствия на данный момент универсальной функции.

СПАМ. МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

А.В. Космачев, студент 4 курса гр.1А2 РТФ

ТУСУР, г. Томск, т.89609766771, gla2@yandex.ru

Спам – это анонимная массовая непрошенная рассылка.

Анонимная – потому что пользователи страдают от автоматических рассылок со скрытым или сгенерированным случайным адресом.

Массовая – т.к. только массовые рассылки являются настоящим бизнесом для спамеров и большой проблемой для пользователей.

Непрошенная – очевидно, потому что никто на спам не подписывается, он сам находит в один счастливый день ваш почтовый ящик.

Спам – это бизнес. Т.е. от него можно получать доходы. Это и приводит к возникновению и росту спамовых рассылок. Почти 80 % всего публичного почтового трафика приходится на долю спама.

Спам является угрозой не только для крупных компаний, но и простых пользователей. Расходы на паразитный трафик, дополнительная загрузка персонала, опасность для стабильности инфраструктуры. Кроме того, спам содержит не только безобидные предложения, но и часто вирусы, трояны, и другие запрещенные программы.[1]

Т.е. спам – это не просто раздражающий фактор, а действительная опасность.

Спам-бизнес довольно быстро распространился в России. Дешевое, эффективное (базы данных спамеров содержит огромное количество адресов) средство рекламы для малого бизнеса.

Кстати, российские спамеры – одни из самых изобретательных в Интернете. Так, они ищут незащищенные компьютеры, через которые можно анонимно рассылать спам, – пользуются домашними компьютерами, например, американских пользователей, поскольку в США очень распространено постоянное домашнее подключение, когда компьютеры стоят включенными целый день и, как правило, ничем не защищены. Компьютер заражают специальными программами, которые позво-

ляют пересылать спам, причем, таким образом, используются сотни и тысячи компьютеров.

Закона о спаме в России нет, что дает большую свободу нашим спамерам. Данный законопроект вносился на рассмотрение, но не прошел. Например, в США в 2003 году был принят CAN-SPAM act, что позволило существенно снизить уровень спама. Впервые восемь месяцев 2005 г. спам составлял 67% писем – это на 9% ниже, чем в прошлом году.

Единственным успехом в борьбе с несанкционированными рассылками в IM-сетях стал арест и осуждение на 18 лет лишения свободы Энтони Греко Чиковага из Нью-Йорка, который разослал рекламные сообщения 1,5 млн. пользователей IM-сетей, нарушив три пункта из CAN-Spam Act.

Спамеры продвигают преимущественно сомнительную продукцию, в том числе порнографического характера, продажа которой компрометирует торговцев сама по себе, так что и бояться нечего. Впрочем, в последнее время стал наблюдаться крен в тематике спама в сторону более серьезных направлений бизнеса. В конце 2004 г. в Рунете появилось интервью с одним из ветеранов спама в нашей стране – Дмитрием Новгородским, владельцем компании DEMETRIUS Software (между прочим, совершенно легитимного юридического лица, как и многие другие фирмы, специализирующиеся на спаме). В ходе беседы было упомянуто одно интересное обстоятельство: спам практически не дискредитирует бренд, если в рекламе указан только номер контактного телефона. По мнению спамера, таким образом, поступают многие из его клиентов, имеющие положительный имидж на рынке. Этим объясняется, почему среди объявлений о продаже viagры время от времени проскальзывают проспекты безымянных турагентств, страховых брокеров, образовательных учреждений и прочих фирм, занимающихся вполне респектабельной деятельностью, 17% рекламы приходится на образовательные услуги, 4% – на финансовые сервисы, 4% – ИТ-предложения, 3% – туризм [1]. Способы борьбы со спамом можно разделить на три категории: 1) юридические; 2) процедурные; 3) технические. Юридическое законодательство о спаме работает только в США. Когда появится в России, и будет ли работать неясно, т.к. очень трудно или вернее практически невозможно найти спамеров. Для этого используется масса ухищрений (подделывание обратных адресов, подмена места отправления и т.д.) [2]. Процедурные – новые протоколы почты, которыми нужно переоснастить около 800 млн. пользователей.

Технические – фильтрация, которая является пожалуй на сегодняшний день самым эффективным средством.

Рассмотри технические методы фильтрации.

Наиболее распространено ПО, работающее по трем основным способам.

Во-первых, использующее черные и белые списки. При этом в белом находятся адреса, заслуживающие доверия, письма, поступающие с которых, доходят до пользователя без всяких ограничений. Сообщения же с адресов, занесенных в черные списки, напротив, автоматически помечаются, как спам и могут быть сразу же удалены с сервера. Обычно поддерживаются не только конкретные адреса, но и целые группы, выделяемые по маске (например, можно поставить в белый список всех корреспондентов с определенного домена). Существуют и публичные черные списки, которые можно скачать из Интернета и экспортировать в некоторые антиспам-приложения.

Достоинством метода является то, что программа не проводит анализа содержания письма, довольно часто приводящего к отсеиванию нужных писем.

Недостаток данного метода вполне банален – низкая эффективность, особенно в том случае, если спамеры используют для рассылки одноразовые адреса с бесплатных почтовых серверов.

Во втором методе применяется запрос на подтверждение. Суть этого метода заключается в задержке письма от адресата, отсутствующего в белом списке. Приложение генерирует и посылает ему письмо-ответ с запросом о намерении вступить в переписку. Если отправитель не ответил, через некоторое время письмо удаляется, а адрес заносится в черный список.

К достоинствам метода можно отнести рост эффективности работы со списками. Недостаток метода тоже очевиден: если отправитель не сможет вовремя ответить на запрос системы, то он автоматически будет занесен в ряды спамеров, а само письмо, возможно с ценным содержанием, будет удалено или, в лучшем случае, отложено без уведомления получателя в отдельную папку. Да и посылать вместо одного письма два при большой переписке не очень удобно. Спамеры же, использующие существующие адреса, часто автоматизируют отправку ответа на запрос.

Третий способ борьбы со спам-сообщениями заключается в анализе пути письма, соответствия служебных полей сообщения и, наконец, в наиболее интересном, эвристическом анализе темы и текста для выявления стандартных лингвистических конструкций, используемых спамерами. При этом применяется несколько алгоритмов, по которым выполняется сравнение текста с некоторыми шаблонами.

Достоинством метода является его независимость от спам-технологий рассылки.

Недостаток – слишком велика вероятность фильтрации как спам других сообщений.

На рынке существует множество бесплатных анти-спам программ. Однако некоторые программы рассчитаны на тех, кто постоянно борется со спамом.

На данный момент можно выделить семь основных технологических направления борьбы со спамом: 1. Простые рамки для правил (MIMESweeper). 2. Самообучающиеся (байесовы плагины) к почтовым клиентам Outlook, The Bat, Mozilla. 3. Карантинные системы.(E-style ISP). 4. Стандарты идентификации (Sender Policy Framework). 5. Встроенный решения(Outlook, The Bat). 6.Сетевые сервисы с подпиской.(Brightmail, Спамоборона). 7. Интегрированные коробочные анти-спам решения.(KAS, SpamAssassin).

Самым распространенным способом является Байесов метод самообучения ПО и встроенные решения. Т.к. они реализованы в почтовых клиентах и для пользователя удобнее и проще разобраться в настройках почтовой программы или установить дополнительный плагин, чем устанавливать отдельную программу. К тому же некоторые методы являются сетевыми и реализуются на серверах [3].

Наиболее популярными являются следующие почтовые клиенты: The Bat!; Mozilla Thunderbird; Foxmail; Outlook Express; Outlook Express.

Достоинства: есть практически везде, встроен в ОС Windows; понятный и удобный интерфейс; содержит встроенные антиспам-средства (фильтрация по размеру, отправителю, теме, вложениям и алгоритм действий).

Недостатки: необходимо выбирать из спама ключевые слова, анализировать, добавлять в правила; малоэффективен, т.к. невозможно создать общего шаблона для всех спам сообщений.

TheBat! Достоинства: возможность подключения байесовых плагинов, которые составляют статистику спам сообщений и фильтруют затем автоматически входящую почту; отличный алгоритм поиска в сообщениях ключевых слов, отправителя, заголовка сообщения, темы, исходный текст, прикрепленный файл.

Недостатки: если не использовать плагин, то надо анализировать все спам сообщения, чтобы заполнить ключевые слова и т.д.

Foxmail. Достоинства: есть Байесов фильтр; черный и белый список отправителей; может выполнять фильтрацию отдельно по Байесову фильтру или на основе созданных правил.

Недостатки: отсутствие алгоритма поиска ключевых слов, как в The Bat!.

Mozilla Thunderbird. Достоинства: байесов фильтр; фильтрация по черному/белому списку; поиск отправителя, работа с SpamPal, Spam Assassin. Недостатки: слабый алгоритм поиска в письме отправителя и т.д.

Наиболее функциональным из всех рассмотренных почтовых клиентов является **TheBat!** При работе байесова фильтра и созданного пользователем алгоритма поиска атрибутов, присущих спам письмам обеспечивает почти 100% фильтрацию. Эффективность фильтра созданного пользователем примерно 40%, т.е. из 10–15 сообщений, поступающих каждый день отсеивается 4–7. Эффективность Байесова фильтра чуть больше порядка 60–70%. Т.е. количество отсеиваемых сообщений 6–10.

В целом количество спам-сообщений снижается, многие почтовые службы и провайдеры устанавливают фильтры. Принятие в России законов о спаме приведет к признанию данной деятельности нелегальной. Спамеры в ответ на повсеместную установку спам фильтров совершенствуют собственные технологии, борьба будет идти за скорость: как быстрее разослать, пока тебя не успели распознать и поставить за-слон.

ЛИТЕРАТУРА

1. *Борьба со спамом* в 2005 году. Компьютер пресс. №7. 2005.
2. www.spamtest.ru
3. <http://www.pxy.ru/~gen/antispam/>

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

А.П. Курило, А.А. Малюк, С.Ф. Михайлов,

М.Ю. Сенаторов, А.И. Толстой

МИФИ, г. Москва, ait@mephi.edu

Развитие современных банковских информационных и автоматизированных систем связано с применением новейших достижений в области информационных технологий. Кроме этого, защита банковской информации является чрезвычайно актуальной проблемой, решение которой возможно только при использовании современных методов и средств. Все это требует привлечения высококвалифицированных кадров, дефицит которых явно наблюдается на рынке труда.

Учебная деятельность МИФИ в данном направлении была в 1995 г. сконцентрирована на факультете «Информационная безопасность», а с 1998 г. на кафедре «Информационная безопасность банковских систем»

этого факультета. Основными направлениями деятельности этой кафедры является подготовка специалистов с высшим образованием и повышение квалификации специалистов кредитно-финансовой сферы.

Подготовка специалистов с высшим образованием. Понимая важность и необходимость расширения подготовки специалистов для организаций кредитно-финансовой сферы, на кафедре был разработан в рамках учебного плана специальности 075500 «Комплексное обеспечение информационной безопасности автоматизированных систем» учебный план новой специализации «Технология обеспечения информационной безопасности банковских автоматизированных систем». Для этого был уточнен паспорт специалиста по защите информации и определен перечень и содержание учебных дисциплин специализации.

1. «Банковские информационные технологии»;
2. «Банковские корпоративные информационные системы»;
3. «Системы безналичного расчета клиент-банк»;
4. «Организационно-правовые методы защиты банковской информации»;
5. «Защита информации в банковских системах»;
6. «Защищенный электронный документооборот в кредитно-финансовой сфере»;
7. «Финансовая криптография»;

Кроме этого расширена тематика учебно-исследовательских работ, перечень тем и мест преддипломной практики и выполнения дипломных проектов.

Повышение квалификации специалистов как направление учебной деятельности относится к дополнительному образованию и по сравнению с подготовкой молодых специалистов с высшим образованием имеет ряд отличительных преимуществ. Именно поэтому дополнительное образование в форме кратковременного повышения квалификации является наиболее популярной образовательной услугой.

Факультет «Информационная безопасность» МИФИ занял на рынке образовательных услуг вполне определенную нишу, связанную с дополнительным образованием (повышением квалификации) специалистов банковской сферы.

Следует отметить позицию Банка России, который еще в 1994 г. первым принял решение о поддержке подготовки специалистов по защите информации на базе МИФИ, заключив с Государственным комитетом по высшему образованию РФ Генеральное соглашение, в силу которого МИФИ стал базовым высшим учебным заведением, ведущим подготовку специалистов по защите информации в интересах Банка России. В 1995 г. Банк России оказал МИФИ материально-техническую

поддержку, которая вылилась в размещении в МИФИ Учебно-методического стенда в составе пяти учебно-научных лабораторий, оснащенных оборудованием и программным обеспечением, которые планировалось использовать при построении защищенных информационных и телекоммуникационных систем Банка России. Это позволило с 2 февраля 1995 г. развернуть на постоянной основе учебную деятельность курсов повышения квалификации специалистов региональных учреждений Банка России по учебным программам, связанным с безопасностью банковских информационных технологий.

Взаимодействие факультета «Информационная безопасность» с банками России позже было расширено за счет установления отношений с Сбербанком России (с 1996 г.) и Внешэкономбанком (позже с Внешторгбанком) – с 2001 г..

За прошедшие время в МИФИ прошли повышение квалификации более 6000 специалистов различных банков. В данном случае накоплен большой опыт работы по повышению квалификации специалистов банковской сферы. Систематизации этого опыта посвящаются данная работа.

СЕРТИФИКАЦИЯ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

*А.А. Малюк, А.И. Толстой, З.В. Попова**

МИФИ, г. Москва, maluk@mephi.edu

**Учебный центр «Информзащита»*

Контроль уровня знаний и умений выпускников высших учебных заведений, ведущих подготовку специалистов по информационной безопасности, основан на сдаче студентами государственного междисциплинарного экзамена и защите дипломного проекта.

При дополнительном образовании форма контроля уровня знаний определяется учебным центром, проводившим обучение.

Недостатками таких подходов к подтверждению квалификационного уровня специалистов, прошедших обучение, является низкая их эффективность, связанная с фактором субъективности («кто учит, тот и проверяет знания»), отсутствием единых требований к уровню контроля знаний и высокой динамикой развития предметной области.

Анализ рынка труда показывает, что специалисты, устраивающиеся на работу или активно работающие в области информационной безопасности, вынуждены для подтверждения своего профессиональ-

ного уровня предъявлять не только диплом о высшем образовании, но и документы, дополнительно подтверждающие их профессиональный уровень. Существующая неудовлетворенная потребность в дополнительном образовании и сертификации знаний и недостаточное предложение соответствующих услуг со стороны отечественных программ и учебных центров привели к появлению на рынке образовательных услуг разработанных за рубежом программ обучения и сертификации специалистов в области информационной безопасности.

Среди таких программ можно выделить две группы программ обучения и сертификации:

- применение конкретных средств защиты информации и информационных технологий, которые предлагаются фирмами разработчиками и внедряются на различных предприятиях и организациях;
- создание комплексных систем, связанных с защитой информации, мониторингом и аудитом информационной безопасности различных систем.

Эффективность реализации первой группы программ обучения и сертификации контролируется определенным образом фирмами – разработчиками технологий, которые заинтересованы в поддержании ее высокого уровня.

Что касается второй группы программ, то, как правило, их содержание не учитывает специфику обеспечения информационной безопасности на российских объектах, связанную с существующей нормативной базой. Кроме этого, чаще всего, они реализуются на иностранном языке. Не смотря на это, а также на высокую стоимость обучения и сертификации, популярность таких программ растет из-за привлекательности сертификата зарубежного (в определенном смысле, конвертируемого) образца. Хотя высокая полезность такого обучения вызывает сомнение.

Изменение создавшейся ситуации возможно при создании отечественной системы сертификации специалистов в области информационной безопасности. Такая система может иметь следующие компоненты:

1. Совокупность разработанных и утвержденных на высоком уровне программ обучения (предполагает коррекцию существующих квалификационных характеристик и образовательных стандартов подготовки специалистов с высшим образованием).
2. Совокупность разработанных и утвержденных на высоком уровне программ обучения для дополнительного образования.
3. Сопряженные с первыми двумя комплекты программ сертификации.
4. Доверенные центры сертификации

5. Регламент проведения сертификации и выдачи соответствующих документов.

В создании такой системы могут принять самое активное участие ведущие высшие учебные заведения и центры дополнительного образования.

Доверенные центры сертификации могут быть созданы на базе Региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы.

Представляется целесообразным, чтобы контроль над созданием и функционированием системы сертификации осуществляло государство в лице, например, Министерства образования и науки РФ и Федеральной службы по техническому и экспертному контролю.

СОЗДАНИЕ БЛОКА ПЕРЕСТАНОВОК НА ОСНОВЕ ОБОБЩЕННОЙ РЕШЕТКИ КАРДАНО

А.А. Сапрыкин, студент 4 курса, В.Л. Спицын, к.ф.-м.н.

Самарский Государственный Технический Университет,

443100 г. Самара, ул. Молодогвардейская 244,

тел.: (846) 278-44-00, E-mail: Meridi@Nm.ru

В данной работе предлагается способ построения блока перестановок (**P-BOX**) как криптографического примитива, основанного на обобщенной решетке Кардано.

P-BOX порядка T представляет из себя полный не повторяющийся набор натуральных чисел от 1 до T .

Блок перестановок формируется при помощи обобщенной решетки Кардано, которая строится на основе классической решетки.

Классическое использование решетки Кардано:

Для ее изготовления берется лист из твердого материала (картон, пергамент, металл), представляющий собой квадрат (сторона квадрата четная, ≥ 2), в котором вырезаны «окна» (рис. 1). При шифровании решетка накладывалась на лист бумаги, и буквы открытого текста вписывались в «окна» слева на право, сверху вниз. При использовании всех «окон» решетка поворачивалась на 90° , и вновь буквы открытого текста вписывались в «окна» повернутой решетки. Затем вновь производился поворот на 90° и т.д. В один «заход» решетка работала 4 раза. *Это ничто иное, как шифр перестановки.*

Главное требование к решетке Кардано – при всех поворотах «окна» не должны попадать на одно и то же место в квадрате, в котором образуются шифртекст.

В работе подробно описана и проанализирована классическая решетка Кардано, выведена формула количества всех ключей при заданной стороне квадрата. Выявлены такие особенности как: эквивалентность ключевого пространства (оно сужается в 4 раза), «слабые» ключи, некоторые вложенные свойства распределения, полученные при помощи программы, демонстрирующей работу алгоритма. Для наглядности были использованы преобразования над графическими изображениями, которые позволили выявить недостатки классической решетки Кардано. На рис. 2 слева изображен прямоугольник, располагающийся вертикально, справа результат его перестановки. Из рис. 2 видно, что справа получилась не заполненное пространство – это следствие последовательного заполнения классической решетки Кардано (слева на право, сверху вниз).

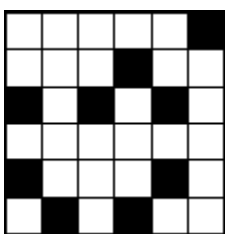


Рис. 1



Рис. 2

На основании полученных данных было предложено более универсальное использование классической решетки, которое позволило получить более равномерное распределение в блоке перестановок, расширив применение Р-BOX'a как криптографического примитива. На рис. 3 изображен результат перестановки картинки (254×254). Слева – фотография, по середине – перемешивание при помощи классической решетки Кардано, справа – при помощи обобщенной.



Рис. 3

Из рис. 3 видно, что получено более равномерное распределение в блоке перестановок – нет ярко выраженной вертикальной ориентации перемешанной картинки как по середине.

Была написана программа на языке программирования Borland Delphi 7.0, демонстрирующая работу алгоритма формирования блока перестановок.

Блок перестановок можно применять в различных шифрсистемах, как самостоятельный или вспомогательный элемент.

ЛИТЕРАТУРА

1. *Бабаш А.В., Шанкин Г.П.* Криптография.-М.: СОЛОН-Р, 2002. 512 с.
2. *Молдовян А.А.* Криптография: скоростные шифры. СПб.: БВХ-Петербург, 2002. 496 с.

МОДИФИКАЦИЯ ПРОТОКОЛА ТСП ДЛЯ ПРИМЕНЕНИЯ В SSL-VPN СЕТЯХ

В.В. Шейда, студент 5 курса каф. РЗИ

ТУСУР, г. Томск

Эффективность ведения бизнеса современного предприятия зависит от возможности его сотрудников получать доступ к информационным ресурсам компании и от способности сотрудников передавать данные в компанию в любой момент времени, находясь в любой точке планеты.

Однако, открытие ресурсов во вне приведет к тому, что они станут доступны не только сотрудникам компании, но и конкурентам. Поддержка модемного пула – достаточно дорогостоящее решение, так как помимо затрат на оборудование оно предполагает непосредственно оплату телефонных звонков, вместе с этим также возникают вопросы касающиеся безопасности.

Альтернативное решение – это использование VPN-технологии. Так как при обеспечении высокого уровня безопасности, эта технология является наименее дорогостоящей и не вызывает сложностей в применении у конечных пользователей.

VPN-технология, помимо защищенного удаленного доступа для сотрудников, позволяет предприятиям объединять сети территориально разнесенных филиалов и организовывать защищенные видео- и аудио-конференции через Интернет.

На данный момент существует множество VPN-решений, однако, в связи с тем, что часто для обеспечения дополнительной безопасности системные администраторы корпоративных сетей закрывают все порты кроме 80 и 443, использовать многие из них не представляется возможным. Вместо этого используют SSL-VPN, для работы которого, необходим только 443 порт.

Очень важно, обеспечить быструю и надежную работу VPN-сетей, так как от этого зависит оперативность информационного обмена между филиалами предприятия и его сотрудниками.

SSL-VPN обладает рядом недостатков, обусловленными используемыми протоколами, которые ограничивают применение SSL-VPN при передаче потокового вещания.

Целью работы является анализ технологии SSL-VPN и предложение оптимального решения для обеспечения наилучшей производительности.



Рис. 2. стандартный стек протоколов применяемый в SSL

Полный стек протоколов используемый в SSL-VPN выглядит следующим образом:

Существуют две основные проблемы реализации: «эффект таяния трафика» и транспортировка UDP поверх TCP.

Протокол TCP – протокол с гарантированной доставкой сообщений. Это значит, что если пакет, содержащий некоторое сообщение, не был доставлен, то он будет поставлен в очередь для повторной от-

правки и отослан по истечению определенного интервала времени (retransmission timeout – таймаут повторной передачи). Если по какой-то причине пакет снова не был доставлен, то TCP использует механизм увеличения таймаута повторной передачи, то есть времени перед следующей повторной отправкой пакета. Это было сделано, для того чтобы учесть возникшие в сети задержки или просто дать пакету, который по какой-то причине пошел по неоптимальному маршруту, больше времени, для того чтобы дойти до получателя.

Однако, при использовании протокола TCP поверх TCP увеличение таймаута повторной передачи внешнего TCP приводит к тому, что внутренний TCP не получает вовремя подтверждения о доставке пакета TCP посланного по корпоративной сети и начинает увеличивать свои таймауты. Это приводит к лавинообразному увеличению суммарных задержек, т.е. снижению скорости передачи – «эффект таяния трафика».

Еще одна проблема, связанная с наличием у TCP механизма повторной передачи возникает при транспортировке UDP-трафика, например видео или аудио информации.

В случае туннелирования UDP поверх TCP, внешний TCP, если пакет не был доставлен, возобновит передачу этого пакета. Следовательно, пакеты, следующие за ним, вынуждены ждать пока потерянный пакет будет доставлен, что приводит к большим задержкам потокового вещания. Если еще принять во внимание механизм увеличения таймаута повторной передачи, то задержки при передаче потоковой информации становятся абсолютно неприемлемыми.

Для решения вышеописанных проблем необходимо реализовать протокол, у которого будут отсутствовать стандартные встроенные механизмы гарантированной доставки TCP, однако, который будет полностью повторять структуру пакета TCP. В этом случае за все остальные механизмы, гарантирующие доставку, отвечает внутренних TCP либо протоколы прикладного уровня, если это необходимо. Также помимо решения проблемы таяния трафика, становится возможна эффективная передача потокового вещания по UDP.

Сложность такой реализации заключается в том, что в случае потери пакета возникают проблемы с SSL: обмен ключами и корректная расшифровка данных. Для правильного обмена ключами необходимо реализовать частичную гарантию доставки, а для обеспечения корректной расшифровки данных необходимо использовать отличный от CBC (Cipher Block Chaining) режим шифрования с небольшими изменениями.

ЛИТЕРАТУРА

1. Мэтью Н., Стоунс Р. Linux Programming – Wiley Publishing, Inc., 2004. 891 с.
2. Семенов Ю.А. Протоколы и ресурсы Internet М: Радиосвязь, 1996.
3. Сэтчел Стефен Т., Клиффорд Х. Б. Дж. Linux IP Stacks в комментариях / Пер. с англ. К: Издательство «ДиаСофт», 2001. 288 с.
4. Хетч Б., Колесников О. Linux: Создание виртуальных частных сетей (VPN) / Пер. с англ. М.: КУДИЦ-ОБРАЗ, 2004. 464 с.

ОБ ОПРЕДЕЛЕНИЯХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ОСНОВАННЫХ НА ЭНТРОПИИ ВЫРАБАТЫВАЕМОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

*А.В. Архангельская, аспирант
МИФИ, г. Москва, kaf42@mephi.ru*

В работе представлен анализ основных подходов к определению понятий генераторов случайных и псевдослучайных чисел и предложе-

на терминология, основанная на энтропии вырабатываемых генератором последовательностей.

Рассмотрим наиболее часто встречающиеся в литературе определения генераторов псевдослучайных и случайных чисел (ГПСЧ и ГСЧ).

Опр. 1. В математике *генератором* называется функция $g: \{0, 1\}^n \rightarrow \{0, 1\}^{q(n)}$, вычисляемая за время, полиномиально зависящее от n , где $q(n)$ – некоторый полином.

Интуитивно, генератор g является псевдослучайным, если порождаемые им последовательности неотличимы никаким полиномиальным вероятностным алгоритмом от истинно случайных последовательностей той же длины $q(n)$. Формально генератор описывается следующим образом.

Пусть T – полиномиальная вероятностная машина Тьюринга, вырабатывающая из двоичных строк длины $q(n)$ один бит. Положим

$$P_1(T, n) = P(T(r) = 1 \mid r \in_R \{0, 1\}^{q(n)}), \quad (1)$$

$$P_2(T, n) = P(T(g(s)) = 1 \mid s \in_R \{0, 1\}^n), \quad (2)$$

где вероятности определяются случайным выбором строк r и s соответственно и случайными величинами, которые машина T использует в своей работе. Заметим, что алгоритм вычисления функции g является детерминированным.

Опр. 2. Генератор g называется *криптографически стойким псевдослучайным генератором*, если для любой полиномиальной вероятностной машины Тьюринга T , для любого полинома p и всех достаточно больших n верно соотношение

$$|P_1(T, n) - P_2(T, n)| < \frac{1}{p(n)}. \quad (3)$$

Необходимым условием криптографической стойкости ГПСЧ является однонаправленность функции g [1], также доказано что существование криптографически стойких ГПСЧ равносильно существованию однонаправленные функций [2].

Опр. 3. ГПСЧ называется способ преобразования короткой случайной последовательности, называемой начальным заполнением, в длинную псевдослучайную последовательность с использованием детерминированного алгоритма [3].

Заметим, что результирующая последовательность называется псевдослучайной, а не случайной, так как количество возможных последовательностей, получаемых на выходе генератора, равно числу возможных начальных заполнений.

Опр. 4. ГПСЧ – это детерминированный криптографический алгоритм, вырабатывающий числа, которые должны успешно проходить

известные тесты на случайность, то есть должны быть неотличимы от случайных даже для эксперта, обладающего неограниченными вычислительными ресурсами [4].

Как правило, недетерминированность в работу ГСЧ вносится за счет источника случайности, то есть физического источника сигналов, выходы которого считаются случайными сами по себе. Возможно применение некоторой процедуры фильтрации или дополнительной обработки выходов источника случайности с целью улучшения их статистических характеристик.

Опр. 5. Если алгоритм получения случайных чисел является недетерминированным, то его реализация называется ГСЧ, а если – детерминированным, то ГПСЧ [5].

Рассмотренные определения учитывают лишь свойства выполняемых при генерации чисел преобразований, не принимая во внимание характеристики источника случайности. Заметим, что определения 1 и 2 рассматривают лишь бинарные входные и выходные последовательности, а определение 3 наиболее точно отражает сущность случайности, так как при внесении некоторой реальной случайности выходные числа также будут случайными, вопрос лишь в том, насколько случайными. Если следовать определению 5, то в определениях 2 и 3 речь идет о генераторе случайной последовательности, так как алгоритм генерации является недетерминированным в силу внесения некоторой случайности. Однако в рассмотренных определениях не участвуют какие-либо количественные оценки и они мало пригодны для практического использования, быть может, за исключением определения 4. Но и в этом случае остается открытым вопрос об определении той конечной совокупности статистических тестов, при помощи которой требуется оценить свойства генератора, что также не является тривиальной задачей.

Предлагается придерживаться определения 5, так как при внесении реальной случайности выходные значения остаются случайными. В любом случае (ГСЧ или ГПСЧ) необходимо проводить оценку энтропии генератора. Так же выходы ГСЧ должны успешно проходить статистические тесты и, в случае применения их в криптографии, необходимо оценивать стойкость генератора к различным криптоаналитическим атакам.

Рассмотренные определения можно обобщить на случай небинарной последовательности, не имеющей равномерного распределения. Используя энтропийный подход (по Шеннону), синтезируем на основе приведенных определение, не обладающее отмеченными недостатками и учитывающее случай небинарной случайной последовательности.

Пусть последовательность $a_1, \dots, a_n$ подается на вход ГСЧ, а $b_1, \dots, b_m$ – результирующая последовательность. В предположении, что обе последовательности являются реализациями случайных величин ξ и η , оценим их энтропию $H(\xi)$ и $H(\eta)$.

Опр. 6. Если $H(\eta) \leq H(\xi)$ и ξ и η независимы, назовем генератор ГСЧ, в противном случае – ГПСЧ.

Таким образом, в ГПСЧ часть энтропии выходной последовательности добавляется за счет детерминированного псевдослучайного преобразования, которое выглядит случайным и неотличимым от случайного в смысле определения 2.

ЛИТЕРАТУРА

1. *Введение в криптографию* / Под общей ред. Яценко В.В. СПб.: Питер, 2001.
2. *Levin L.A.* One-way functions and pseudorandom generators // *Proceedings of 17th ACM Symposium on Theory of Computing*, May 1985. PP. 363–365.
3. *Shafi Goldwasser, Mihir Bellare.* *Lecture Notes on Cryptography*, 2001. <http://www.cse.ucsd.edu/users/mihir/papers/gb.html>.
4. *John Kelsey, Bruce Schneier and others.* *Cryptanalytic Attacks on Pseudorandom Number Generators*. *Fast Software Encryption, Fifth International Workshop Proceedings*, Springer-Verlag, 1998.
5. Сайт исследовательской группы pLab Университета Зальцбурга (Австрия). <http://random.mat.sbg.ac.at>.

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ С РАСПРЕДЕЛЕННЫМ СЕКРЕТНЫМ КЛЮЧОМ

*А.В. Архангельская; С.В. Запечников, к.т.н., доц.
МИФИ, г. Москва, kaf42@mephi.ru, oka@mephi.edu*

В системах криптографической защиты информации (СКЗИ), использующих схемы разделения секрета (СРС), одним из важных примитивов является распределенный механизм вычисления псевдослучайных функций (ПСФ). Предлагаемый авторами способ реализации этого примитива является развитием классических СРС.

Опр. Пусть $F_m = \{f_\alpha\}$ – семейство ПСФ с параметром m и ключом α . (t, n) -пороговое вычисление F_m – тройка $\langle S, F, G \rangle$ функций (функция разделения ключа, вычисления с разделенными данными и функция реконструкции соответственно), вычисляемых за полиномиальное время, таких что:

$$1) \forall f_\alpha \in F_m: S(\alpha) = \langle \alpha_1, \dots, \alpha_n \rangle;$$

$$2) \forall 1 \leq i_1 < \dots < i_t \leq n : G(\langle i_1, F(\alpha_{i_1}, x) \rangle, \dots, \langle i_t, F(\alpha_{i_t}, x) \rangle) = f_\alpha(x);$$

3) $\forall 1 \leq i_1 < \dots < i_{t-1} \leq n$: по заданным $\{\alpha_{ij}\}_{j=1}^{t-1}$ и множеству Y величин (количество которых полиномиально ограничено, а элементы множества выбираются адаптивно, возможно, в зависимости от $\{\alpha_{ij}\}_{j=1}^{t-1}$) и по данным $\langle f_\alpha(y), \{F(\alpha_i, y)\}_{i=1}^n \rangle$ для $\forall y \in Y$, функция f_α является псевдослучайной на множестве аргументов, не принадлежащих множеству Y [1].

Механизм распределенной генерации ПСФ по передаваемым на вход числам h выполняет (t, n) -пороговое вычисление ПСФ, т.е. возвращает данные, по которым запросивший определяет значения $f(h)$, причем их последовательность вычислительно неразличима с последовательностью случайных чисел [1]. Известны различные подходы к вычислению таких функций. Для использования в СКЗИ предлагается адаптировать способ, основанный на обобщении СРС Шамира [2] для многочленов от двух переменных, который дает высокопроизводительные алгоритмы, а последовательность генерируемых значений функции является истинно случайной. Особенностью способа является ограничение количества значений $f(h)$, после которого последовательность перестает быть случайной.

Пусть $G = \{S_1, \dots, S_n\}$ – множество узлов распределенной компьютерной системы, U – пользователь, имеющий защищенные каналы связи с узлами $S_i \in G$, $i = \overline{1, n}$. F – множество всех многочленов от двух переменных $P(x, y)$ над конечным полем H , в которых максимальная степень вхождения переменной x в одночлены равна $t-1$, переменной y – $l-1$. α – ключ, выбираемый случайным образом, состоящий из lt коэффициентов многочлена, при помощи которого выбирается функция $f_\alpha \in F$. Значением функции является элемент поля H , размер которого должен быть порядка требуемой длины значения ПСФ. Параметр l определяет предельное количество ключей, которые могут быть выработаны при сохранении свойства псевдослучайности. Механизм вычисления ПСФ включает три протокола, все операции выполняются в поле H .

Протокол инициализации:

1. Узел $S_i \in G$, $i = \overline{1, n}$, выбирает многочлен $P_i^{(0)}(x, y)$ со случайными коэффициентами и рассылает его всем остальным узлам S_j , $j \neq i$. Общий многочлен определяется как $P(x, y) = \sum_{S_i \in G} P_i^{(0)}(x, y)$.

2. Каждый узел $S_i \in G$ вычисляет свой ключ $\alpha_i = P(i, y) = Q_i(y)$, $\deg Q_i(y) = l-1$.

Протокол вычисления значения ПСФ:

1. Пользователь U рассылает узлам $S_i \in G$, $i = \overline{1, n}$, значение h , для которого необходимо получить $f(h) = P(0, h)$.

2. Узел $S_i \in G$, $i = \overline{1, n}$, вычисляет $\beta_{i, h} = F(\alpha_i, h) = Q_i(h) = P(i, h)$ и пересылает его пользователю.

3. Пользователь U выполняет интерполяцию по формуле Лагранжа, по точкам $\left\{ (i_j, \beta_{i_j, h}) \right\}_{j=1}^t$, $S_j \in G$ находит $P(0, h) = Q_0(h) = f(h)$.

Протокол обновления ПСФ:

1. Узел $S_i \in G$, $i = \overline{1, n}$, выбирает многочлен $P_i^{(t)}(x, y)$ со случайными коэффициентами, такой что $P_i^{(t)}(0, y) = 0$ и рассылает всем остальным узлам S_j , $j \neq i$ значения $P_i^{(t)}(j, y)$.

2. Все узлы выполняют протокол совместной генерации случайного числа r .

3. Узел $S_i \in G$, $i = \overline{1, n}$, вычисляет $P_i^{(t)}(x, r)$ и рассылает этот многочлен всем остальным узлам $S_j \in G$, $j \neq i$.

4. Узел $S_j \in G$, $j = \overline{1, n}$, проверяет для каждого i , что $P_i^{(t)}(0, r) = 0$ и проверяет соответствие этого многочлена присланному ему на шаге (1). В случае положительного результата для всех i он полагает, что новый многочлен $P_j^{(t)}(x, y) = P_j^{(t-1)}(x, y) + \sum_{S_i \in G} P_i^{(t)}(j, y)$.

Необходимо отметить следующую особенность данного механизма вычисления ПСФ. Существует простая процедура подтверждения того, что пользователь получает корректные данные от узлов системы. Для этого необходимо, чтобы пользователь производил вычисления с узлами системы, количество которых больше, чем n , а затем использовал свойства исправления ошибок кодов Риды–Соломона (Reed–Solomon) [3] для вычисления корректного результата.

Приведенный механизм может быть усовершенствован внесением следующих изменений. Можно добиться упреждающей безопасности схемы, которая позволяет множеству узлов системы автоматически продолжать работу после сбоя или взлома какого-либо узла без нарушения безопасности [4]. Для этого узлы должны осуществлять согласованное периодическое обновление разделяемых секретов, причем безопасность обеспечивается до тех пор, пока количество узлов, вышедших из строя за время между соседними обновлениями, не превысило некоторое пороговое значение.

Для снижения сложности интерполяции можно использовать несколько полиномов меньшей степени и случайным образом устанавливать соответствие между ключами и полиномами.

ЛИТЕРАТУРА

1. Naor M., Pinkas B., Reingold O. Distributed pseudo-random functions and KDCs. – Advances in Cryptology: EUROCRYPT'99, LNCS, V. 1592. Springer-Verlag, 1999. PP. 327–346.
2. Shamir A. How to share a secret // Comm. of the ACM, Vol. 22, No. 11, 1979. PP. 612–613.
3. McEliece R.J., Sarwate D.V. On sharing secrets and Reed-Solomon Codes // Comm. of the ACM, Vol. 24, No. 9, 1981. PP. 583–584.
4. Canetti R., Gennaro R., Herzberg D., Naor D. Proactive security: Long-term protection against break-ins, 1997. <http://citeseer.ist.psu.edu/canetti97proactive.html>

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КЛЮЧЕВОЙ СИСТЕМЫ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОЙ СРЕДЕ

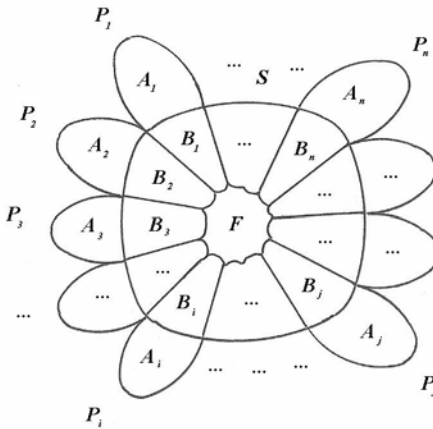
*С.В. Запечников, к.т.н., доцент
МИФИ, г. Москва, oka@merphi.edu*

Решение задачи обеспечения живучести средств защиты информации (СЗИ) в распределенных компьютерных системах, использующих криптографические ключи, должно опираться на обобщенную модель их ключевой системы (КС). В докладе представлены основные положения предлагаемой автором обобщенной модели типовой КС, позволяющей удобно специфицировать требования по безопасности, предъявляемые к КС.

Ключевой системой СЗИ будем называть совокупность всех используемых в нем криптографических ключей и правил их использования. Таким образом, для описания КС необходимо задать структуру множества K составляющих ее ключей и специфицировать политику безопасности КС $Pol(K)$.

В соответствии с системным подходом к описанию функциональности, принятым в современной концепции открытой распределенной обработки данных, распределенную компьютерную систему DS можно представить как систему функциональных блоков (ФБ), или сервисов, предоставляющих услуги множеству пользователей $U = \{U_1, U_2, \dots, U_n\}$, что позволяет каждому из них реализовать свою технологию обработки информации. Пусть F – множество системных

ключей ФБ, не известных пользователям, $P_k = A_k \cup B_k$ – множество ключей пользователя $U_k, k = \overline{1, n}$, состоящее из двух подмножеств: A_k – ключи, известные только пользователю U_k и не известные ФБ, B_k – ключи, общие для U_k и какого-либо ФБ распределенной системы. Таким образом, множество системных ключей $S = F \cup B_1 \cup B_2 \cup \dots \cup B_n$, а



множество всех ключей, составляющих КС, может быть записано в виде $K = S \cup P_1 \cup P_2 \cup \dots \cup P_n$ (рис. 1).

В подавляющем большинстве случаев КС современных СЗИ распределенных компьютерных систем являются иерархическими.

Рис. 1. Типовая структура ключевой системы СЗИ в распределенной среде

Будем называть *чисто симметричной КС уровня вложенности t* такую ключевую систему, которая состоит из множества общих секретных ключей $SK = \left\{ k_0, k_{1,1}, \dots, k_{1,j(1)}, k_{2,1}, \dots, k_{2,j(2)}, \dots, k_{m,1}, \dots, k_{m,j(m)} \right\}$, где

$$k_{i,j} = G \left(f^{(i)}(k_{i,1}, \dots, k_{i,q}), f^{(i-1)}(k_{i-1,1}, \dots, k_{i-1,j(i-1)}), \dots, f^{(1)}(k_{1,1}, \dots, k_{1,j(1)}), f^{(0)}(k_0) \right), \\ q < j^{(i)}, i \leq m.$$

Будем называть *чисто асимметричной КС уровня вложенности t* такую ключевую систему, которая состоит из множества пар частных секретных и соответствующих им открытых ключей

$$AK = \left\{ (s_0, p_0), (s_{1,1}, p_{1,1}), \dots, (s_{1,j(1)}, p_{1,j(1)}), \dots, (s_{m,1}, p_{m,1}), \dots, (s_{m,j(m)}, p_{m,j(m)}) \right\},$$

где $p_0 = g(s_0)$, $p_{i,j} = g(s_{i,j})$ и

$$s_{i,j} = G \left(f^{(i)}(s_{i,1}, \dots, s_{i,q}), f^{(i-1)}(s_{i-1,1}, \dots, s_{i-1,j(i-1)}), \dots, f^{(1)}(s_{1,1}, \dots, s_{1,j(1)}), f^{(0)}(s_0) \right), \\ q < j^{(i)}, i \leq m.$$

Комбинированной КС будем называть КС, состоящую из множества ключей $СК$, подмножествами которого являются чисто симметричные и чисто асимметричные КС.

Под безопасностью ключевого материала понимается одновременное достижение свойств доступности, аутентичности и конфиденциальности (если требуется). Свойство аутентичности ключевого материала нами понимается как обобщение свойств целостности при хранении и (или) подлинности доставки. *Политикой безопасности КС* будем называть множество правил, отображающих множество ключей КС на множество пользователей, имеющих в каждый момент времени полномочия для санкционированного использования ключей. Под *политикой управления ключами КС* будем понимать множество правил, отображающих функциональные зависимости между ключами, обеспечивающие в каждый момент времени реализацию политики безопасности КС.

Опираясь на введенные определения, можно сформулировать критерии безопасности КС, важные для обеспечения живучести СЗИ.

1. «Прямой» критерий безопасности КС – условие, при котором в соответствии с политикой безопасности КС при утрате ключевого материала верхних уровней иерархии, действительного для санкционированного использования в текущий момент времени, сохраняется безопасность функционально зависимого от него ключевого материала нижних уровней иерархии. «Прямой» критерий рационально применять для подмножеств $P_k, k = \overline{1, n}$.

Простыми примерами политик управления ключами, обеспечивающих реализацию «прямого» критерия за счет «временного» распределения ключа, могут служить схемы цифровой подписи с эволюцией ключа. В них секретный ключ подписи s_{ij} замещается серией зависящих от времени производных ключей $s_{i+1,j}(t), t = \overline{1, q}$, для каждого из которых $s_{i+1,j}(t) = f(s_{ij}, s_{i+1,j}(1), \dots, s_{i+1,j}(t-1))$, и обеспечивается свойство совершенной опережающей безопасности схемы.

2. «Обратный» критерий безопасности КС – условие, при котором в соответствии с политикой безопасности при утрате части ключевого материала нижних уровней иерархии, действительного для санкционированного использования в текущий момент времени, сохраняется безопасность ключевого материала верхних уровней иерархии, от которых функционально зависим ключевой материал нижних уровней. «Обратный» критерий рационально применять для подмножества S , и в особенности для F .

Примерами политик управления ключами, обеспечивающих реализацию «обратного» критерия за счет «пространственного» распределения ключа, являются пороговые схемы разделения секрета. В них секретный ключ k_{ij} замещается серией функционально зависящих от него ключей $k_{i+1,j}(u), u = \overline{1, q}$, для каждого из которых $k_{i+1,j}(u) = f\left(k_{ij}, k_{i+1,j}(1), \dots, k_{i+1,j}(u-1)\right)$, и обеспечивается свойство восстановления k_{ij} методом интерполяции.

ТЕХНОЛОГИЯ СОЗДАНИЯ ЭЛЕКТРОННЫХ АРХИВОВ, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

П.К. Алексеев

МИФИ, г. Москва, pashaalex@mtu.net.ru

Рассматриваются вопросы создания электронных архивов, содержащих конфиденциальную информацию.

В настоящее время в РФ накопилось достаточное кол-во конфиденциальной информации, находящейся на бумажных носителях. Хранить информацию в таком виде неудобно по ряду причин: высокая стоимость аренды помещений под хранение, невозможность быстрого поиска и доступа к документу. В связи с этим, многие организации-владельцы таких архивов готовы к их переводу в электронный вид [1].

Для того, чтобы создать электронный архив – необходимо выполнить ряд операций. Сначала необходимо отсканировать все документы, потом, создать поисковую БД для быстрого поиска документов. Во время создания БД происходит привязка поисковых реквизитов документа к набору графических образов документа. Для этого необходимо перевести поисковую информацию с отсканированных образов в текстовый формат. Для этого могут быть использованы технологии OCR [2] или ручной ввод. К сожалению, на сегодняшний момент не существует промышленных алгоритмов для распознавания рукописного текста с приемлемой точностью. Единственным приемлемым вариантом остается ручной ввод.

Сканирование документов не является трудоемкой операцией. Производительность современных сканеров позволяет обрабатывать документы со скоростью до 300 стр./мин [3], что позволяет выполнять эту операцию силами владельца архива.

Создание поисковой БД – более трудоемкий процесс, особенно при использовании технологии ручного ввода. На этом этапе целесообразно привлечение сторонних организаций для создания поисковых БД[4]. Такой подход зачастую оправдан качеством результата и стоимостью работ. И имеет неоспоримое преимущество перед развитием собственной технологии с точки зрения скорости выполнения работы.

Однако, при формировании поисковой БД для архива, встает вопрос о том, что человек, принимающий участие в формировании БД неизбежно знакомится с содержимым документов. В случае передачи отсканированных образов в стороннюю организацию это недопустимо.

Заметим, что если взять документ, «вырезать» из него поисковые реквизиты, перемешать их в случайном порядке с реквизитами других документов – то восстановить содержимое документа будет невозможно.

В данном случае предлагается подобная схема. Если у нас есть набор отсканированных образов и нам необходимо составить поисковую БД, то алгоритм выглядит так:

1. При помощи алгоритмов машинного зрения [5, 6] из документов выделяются поисковые реквизиты.

2. Реквизиты одних документов перемешиваются с реквизитами других в случайном порядке. Матрица перемешивания сохраняется у владельца архива.

3. Исполнителю отдаются перемешанные реквизиты документов в графическом формате.

4. Задача исполнителя – поставить в соответствие каждому графическому файлу текстовое представление реквизита.

5. Матрица соответствия передается заказчику.

6. Имея матрицу соответствия и матрицу перемешивания, заказчик без труда формирует поисковую БД.

Актуальным остается вопрос о конфиденциальности самих реквизитов и риском их передачи сторонней организации. Данный вопрос, так же, как и вопрос о целесообразности создания электронного архива, должен решаться экспертной комиссией.

По мнению автора, применение описанной технологии позволит ускорить процесс формирования электронных архивов, содержащих конфиденциальную информацию.

ЛИТЕРАТУРА

1. В. Сленко. Электронные архивы бухгалтерской документации «Финансовая газета. Экспо». № 5. 2005. с. 6–7.
2. <http://www.abbyy.ru>
3. <http://www.scamax.ru>
4. <http://www.elar.ru>

5. *Форсайт Д., Понс Ж.* Компьютерное зрение. Современный подход. / Пер. с англ. М.: Издательство «Вильямс», 2004.
6. Методы компьютерной обработки изображений / Под ред. В.А. Сойфера. 2-е изд., испр. М.: ФИЗМАТЛИТ, 2003.

МЕТОД СОЗДАНИЯ МНОГОАГЕНТНЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ЭВМ

***А.А. Берестов, В.А. Петров, к.т.н., доцент**
МИФИ, г. Москва, pva@mephi.edu*

В докладе предлагается метод создания многоагентной системы для защиты информации в сетях ЭВМ от вирусных атак с использованием продукционно-фреймовой модели базы знаний.

В настоящее время для работы в сетях ЭВМ используется технология многоагентных систем для различных приложений. Многоагентные системы (МАС) – это программно-вычислительные комплексы, где взаимодействуют различные агенты для решения задач, которые трудны или недоступны в силу своей сложности для одного агента [1]. Точное определение агента на сегодняшний день отсутствует. В основном используется определение, принятое на конференции международной ассоциации по лингвистике FIRA (Federation of Intelligent Physical Agents) в октябре 1996 г. в Токио: Агент – это сущность, которая находится в некоторой среде, интерпретирует и исполняет команды, воздействующие на среду [2]. Каждый агент имеет определенные обязанности и обладает собственными ресурсами для выполнения этих обязанностей.

Разработка МАС основывается на методах и средствах систем искусственного интеллекта, сетевых технологиях и включает три основные модели: модель агентов, модель услуг и модель отношений. Модель агентов задает классы агентов, составляющих МАС, и соответствующие экземпляры агентов. Модель услуг определяет основной набор услуг, связанный с каждым типом агентов. Модель отношений характеризует возможные контакты для каждого типа агентов[3].

Целью данной работы является исследование возможности применения технологии МАС для защиты информации в сетях ЭВМ от вирусных атак.

Для реализации поставленной цели необходимо выполнить следующие задачи:

- провести сравнительный анализ и выбор технологий МАС и исследовать модели агентов;

- исследовать возможность применения технологии МАС для защиты информации в сетях ЭВМ от вирусных атак;
- осуществить выбор модели базы знаний по определению вирусных атак;
- создать базу знаний (правил) в соответствии с выбранной моделью;
- разработать и протестировать МАС приложения по защите от вирусных атак в сети ЭВМ.

Одной из главных задач является выбор модели базы знаний.

База знаний может представлять экспертные правила, полученные эвристическим методом на основе накопленного опыта работы с анти-вирусными средствами защиты информации. На сегодняшний день существуют эвристические модели баз знаний: семантические сети, фреймы, сценарии, продукции[4]. Модель базы знаний может быть представлена в виде фреймов. Фрейм используется для описания типовой вирусной атаки. Слоты фрейма описывают признаки вирусной атаки и ссылки на процедуры и библиотеки по устранению вирусных атак.

Фреймы-экземпляры описывают вирусную атаку определенного типа. Процедурный слот описывает действие или ссылку на программу-агент, выполняющую действие по отражению вирусной атаки. Таким образом, предлагаемый подход использует продукционно-фреймовую модель для создания многоагентных приложений по отражению вирусных атак.

Эвристические правила базы знаний по определению типа атаки можно описать с помощью правил-продукций. В результате выводов полученных с помощью базы знаний локализуется источник вирусной атаки и выбирается средство защиты.

Разрабатываемая многоагентная система может быть использована администраторами сетей для отражения вирусных атак серверов баз данных, а также программ и файлов рабочих станций в сети ЭВМ. Также данное приложение может быть использовано как обучающая система по диагностике вирусных атак.

ЛИТЕРАТУРА

1. Гаврилова Т.А., Хорошевский В.Ф. «Базы знаний интеллектуальных систем»: СПб: Питер, 2000.
2. Чекинов Г.П., Чекинов С.Г. «Применение технологии многоагентных систем для интеллектуальной поддержки принятия решения». Сетевой электронный научный журнал «Системотехника» № 1. 2003.
3. Тарасов В.Б. «От многоагентных систем к интеллектуальным организациям: философия, психология, информатика». М.: Эдиториал УРСС, 2002 г.
4. Искусственный интеллект. Кн. 2. Модели и методы: Справочник / Под ред. Д.А. Поспелова-М: Радио и связь, 1990.

ПРОБЛЕМЫ СОЗДАНИЯ СИСТЕМЫ ИСКУССТВЕННОЙ ДЕВЕРСИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.А. Борискин

МИФИ, г. Москва, miltur@mephi.edu

Рассматриваются различные подходы к решению проблемы деверсификации программ для повышения их устойчивости к преднамеренной компрометации. Особое внимание уделяется задаче создания системы управления деверсификационными механизмами и оценке ее эффективности.

На сегодняшний день проблема так называемых «монокультур» в информационных технологиях (операционных системах, бизнес-приложениях) представляет собой одну из ключевых задач обеспечения информационной безопасности автоматизированных систем [1]. Широкая распространенность коммерческого программного обеспечения (ПО) с закрытым исходным кодом делает большинство компьютеров с доступом в Интернет уязвимыми перед угрозами компрометации с использованием недостатков в системном и прикладном ПО. Относительно недавние «эпидемии», связанные с появлением сетевых червей Sasser и NetSky [2] и их модификаций, являются доказательствами того, что всего лишь одна вредоносная программа способна вывести из строя технологическую инфраструктуру сразу нескольких компаний на довольно длительное (по экономическим меркам) время.

Проблема «монокультур» не является относительно новой. История по созданию подходов к разработке устойчивого к сбоям ПО насчитывает не одно десятилетие. Одним из самых обсуждаемых (в том числе, и до сих пор) подходов является так называемое N -версионное программирование [3]. В своем классическом варианте, данный подход подразумевает разработку одной и той же программной системы несколькими командами разработчиков в рамках одного проекта. В результате выпускается несколько реализаций одного и того же продукта, с различной структурой и характеристиками исполняемого кода. В теории N -версионного подхода доказывается, что вероятность синхронного сбоя всех N систем при возникновении угрозы одного типа, как правило, сводится к нулю.

Очевидно, что N -версионный подход является экономическим неэффективным (по крайней мере, в том виде, в каком он существует сейчас). В условиях жесткой конкуренции для любой организации не выгодно оплачивать работу нескольких проектных команд, создающих один и тот же программный продукт. Поэтому на практике N -версионное программирование применяется только в исследовательских

проектах, а для коммерческих компаний представляет только теоретический интерес.

Другой тип методик по деверсификации программных систем основан на преобразовании уже существующего (как исходного, так и исполняемого) кода с целью искусственного внесения в систему стохастических характеристик, затрудняющих применение к ней одних и тех же средств компрометации.

Все подобные методики можно условно разбить на две категории [4]: изменяющие исполняемый код и изменяющие исходный код программы.

К первой категории относятся:

- шифрование и перемешивание программных блоков (obfuscation);
- преобразование относительных и абсолютных адресов условного перехода и вызовов подпрограмм;
- преобразование набора инструкций процессора;
- шифрование сетевых и интерфейсных протоколов.

Вторая категория включает в себя следующие методики:

- изменение поведения кода;
- преобразование внутренних потоков данных;
- преобразование внутренних потоков управления;
- искусственное расширение пространства состояний протоколов;
- размещение уязвимых данных за пределами буферов памяти.

Очевидно, что каждый из подходов, не зависимо от категории, представляет собой дополнительный источник накладных расходов, причиной которому может стать неудовлетворительная в рамках заданных требований производительность программной системы. Кроме того, остаются открытыми вопросы о том, как получить приемлемый уровень деверсификации в рамках конкретной технологической инфраструктуры и как управлять деверсификацией при возникновении новых угроз. Второй вопрос представляет интерес еще и тем, что деверсификационный подход является «проактивным», то есть предугадывающим те или иные угрозы. Поэтому для управления деверсификационными механизмами, возможно, также понадобится некоторая прогнозирующая модель, способная определять временные периоды их функционирования.

ЛИТЕРАТУРА

1. D. Geer. Monopoly considered harmful. IEEE Security & Privacy Magazine, 1(6):14–16, December 2003.
2. <http://www.virusbtn.com/resources/viruses/>.

3. A. Avizienis, «*N-Version Approach to fault tolerant Software*», *IEEE-Software* eg., vol- SE11, No12, Dec 1985, PP. 1491–1501.
4. J. E. Just and M. Cornwell. Review and analysis of synthetic diversity for breaking monocultures. In Proc. Of the 2nd Workshop on RapidMalcode, Washington, D.C., October 2004.

МЕТОДЫ КОНТЕНТ-АНАЛИЗА СОЦИАЛЬНО-ДИНАМИЧЕСКИХ ПРОЦЕССОВ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.С. Лекишин

МИФИИ, г. Москва, pva@mephi.edu

Цель данного доклада состоит в том, чтобы определить возможность применения математических методов исследования социально-динамических процессов, происходящих в современной культуре, к изучению проблем информационной безопасности.

Вопросы безопасности информации включают в себя исследование состояния защищенности информации от различных воздействий, направленных на нарушение конфиденциальности информации, целостности, доступности и других ее характеристик. В теории информационной безопасности постулируется также существование возможности воздействия информации на воспринимающую ее систему, в том числе человека и человеческое общество, и ставится задача изучения этого воздействия.

Задача данного доклада состоит в том, чтобы определить возможность применения математических моделей, в рамках которых поддаются формальному описанию элементы современной культуры (в частности, сообщения естественного языка), рассматриваемые как носители информационного воздействия.

Информационное воздействие осуществляется с применением таких средств, которые позволяют осуществлять с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия [1].

Ключевой точкой при описании взаимодействия «информация – человек» (или «информация – общество») является элемент, преобразующий информационное воздействие – культура (индивидуальная и групповая в случаях человека и общества соответственно).

Изучение культуры основывается на обобщенной технике контент-анализа [2]. Индивидуальная культура – это особая выборка культуры социальной группы, к которой относится данный индивидуум, однако

ее изучение строится на тех же приемах. Каждый из представленных элементов культуры должен быть расположен в соответствии с некоторым числом измерений, определяющих структуру их совокупности. Среди этих элементов, помимо специфических измеримых параметров, называемых классификационными, имеются параметры общего характера: степень абстрактности, которая характеризует уровень доступности сообщения для различных членов социальной группы. На восприятие сообщения также влияет параметр, определяющий степень вовлеченности индивидуума в описываемое событие (т.н. «близость» события).

С точки зрения информационной безопасности, необходимо иметь возможность оценивать степень воздействия сообщения на индивидуальную культуру человека. Очевидно, данная мера находится в определенной зависимости с уровнем доступности сообщения и степенью вовлеченности.

Вопросы социодинамики и информационной безопасности человека и общества сильно пересекаются, так как в обоих случаях изучается изменение объекта под действием воспринимаемых им информационных потоков. Используя математический аппарат методов контент-анализа, возможно выделение набора параметров, характеризующих элементы культуры человека и человеческого общества, позволяющих кластеризовать эти элементы и, как следствие, типизовать их, а так же определять уровень воздействия информации на систему (человека, общество).

ЛИТЕРАТУРА

1. *Расторгуев С. П.* Информационная война. «Радио и связь». Москва, 1999.
2. *Моль А.* Социодинамика культуры. «Прогресс». Москва, 1973.

ВЫЯВЛЕНИЕ ИСТОЧНИКОВ РАССЫЛКИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ ПРОТОКОЛА SMTP

К.П. Рудик

МИФИ, г. Москва, pva@mephi. edu

В данном докладе рассматриваются вопросы разработки и применения автоматизированной системы выявления сетевых узлов, участвующих в распространении вредоносного программного обеспечения посредством протокола SMTP.

Одной из важных задач, которые приходится решать при реализации эффективной системы защиты, является выявление источников несанкционированных действий, в данном случае сетевых узлов, участ-

вующих в распространении упомянутых программ посредством протокола SMTP [1, 2].

Протокол SMTP в настоящее время является одной из главных сред распространения вредоносных программ (вирусов, троянских программ и т.п.). По данным компании «Лаборатория Касперского» [3] за 2004 г. 17 из 25-ти самых распространенных вирусов, что составляет 68%, способны рассылать свои копии, используя SMTP.

Для выявления нарушителя необходимы детальный анализ и проверка информации, находящейся в заголовках сообщений электронной почты. Ручной анализ такой информации оказывается крайне неэффективным из-за весьма больших объемов почтового трафика, а также из-за временных ограничений накладываемых механизмами проверки. В связи с этим не вызывает сомнений потребность в автоматизированных системах, которые позволили бы локализовать нарушителя (скомпрометированный сетевой узел).

Основными методами нарушителя направленными на сокрытие информации о себе являются использование [4]:

- подложной информации об отправителе;
- компьютеров «зомби» (предварительно «взломанных» сетевых узлов);

- различных прокси-серверов (HTTP-проху, SOCKS-проху, и т.п.).

Применяемые в настоящее время системы, которые обеспечивают фильтрацию почтового трафика на предмет наличия в нем вредоносных программ, предоставляют ограниченную информацию для аудита информационной безопасности. Используемый в них в качестве информации о нарушителе электронный адрес отправителя в подавляющем большинстве случаев является поддельным.

В общем случае задача определения сетевого узла, являющегося начальным в формировании вредоносных почтовых сообщений, является неразрешимой, так как нарушителем могут быть соблюдены все формальные условия по правильности составления дополнительных ложных заголовков, источник может скрываться за различными проху-серверами или узлами-зомби, а также из-за некоторого различия форматов заголовков для различных почтовых систем.

Однако при работе в реальных условиях можно задать набор правил (условий), проверка которых в большинстве случаев позволит выявить сетевой узел, который будет являться либо непосредственно источником несанкционированных действий (распространение вредоносных программ), либо сетевым узлом, через который действовал нарушитель (проху, ЗОМБИ). Возможно также проведение дополнительной проверки, которая в определенных случаях поможет установить, к какому типу принадлежит найденный узел.

Разрабатываемая система получения информации предназначена для выявления нарушителей и имеет в своей основе замечания предыдущего абзаца.

Информация о сетевых узлах, участвующих в распространении вредоносных программ посредством протокола SMTP, несомненно, будет важна при решении как задачи нейтрализации вирусных эпидемий, так и других задач, связанных с распространением вирусов. А системы, предоставляющие такую информацию, могут с успехом применяться как в глобальных, так и в локальных сетях для обеспечения более эффективной работы системы информационной безопасности.

ЛИТЕРАТУРА

- 1 RFC 821 (<ftp://ftp.rfc-editor.org/in-notes/rfc821.txt>)
2. RFC 2821 (<ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt>)
3. «Развитие вредоносных программ в 2004 году» (<http://www.viruslist.com/ru/analysis?pubid=157007259>)
4. «Почтовые вирусы становятся все умнее» (<http://www.ivnet.ru/modules/news/article.php?storyid=412>)

ПРЕДЛОЖЕНИЕ ТЕХНОЛОГИИ ПОСТРОЕНИЯ АИС, ПОВЫШАЮЩЕЙ УРОВЕНЬ ДОСТУПНОСТИ ДАННЫХ И СОХРАНЯЮЩЕЙ ЗАДАННЫЙ УРОВЕНЬ СЛОЖНОСТИ АДМИНИСТРИРОВАНИЯ

С.И. Ткаченко

МИФИ, г. Москва, pva@merphi.edu

В работе рассматриваются тенденции развития существующих технологий построения автоматизированных информационных систем (АИС), показываются недостатки, возникшие в ходе развития технологии. Предлагается на рассмотрение подход автора к построению АИС.

Уровень развития вычислительной техники сегодня достиг такого значения, когда средняя клиентская станция по вычислительной мощности сопоставима с серверными станциями двух-трех летней давности. Технология построения АИС напротив движется в направлении консолидирования вычислительной нагрузки на серверную часть системы. По мнению автора, это объясняется, прежде всего, стремлением облегчить процесс администрирования.

Автор предлагает архитектуру АИС, в которой компоненты системы находятся на сервере приложений, и выполняются не сервером приложений, как это принято, а на стороне клиента [1]. На стороне клиента находится лишь небольшое приложение-интерпретатор, не

требующее администрирования, что позволяет сохранить уровень сложности администрирования, как в варианте с тонким клиентом. Данный подход позволяет снять с сервера ряд функций системы, а именно снять выполнение процедур, функций и триггеров, перенести функции ведения аудита и шифрования данных на сторону клиента. На стороне сервера остаются его первоочередные задачи: управление сессиями пользователей, хранение и выборка данных.

Перенос функционала АИС на сторону клиента позволит, как предполагается, снизить среднее время обработки запроса пользователя сервером на 25%. Используя аппарат теории очередей, легко показать, как это отразится на работе АИС в целом.

Представим модель клиент сервер как очередь с одним проборм обслуживания.

Будем считать, что мы имеем пуассоновский поток. Пусть t_s – время обслуживания запроса, а σ_{ts} – стандартное отклонение времени обслуживания, q – число запросов в системе, ожидающих обслуживания и обслуживаемых в данный момент времени. Пусть t_q – время пребывания запроса в системе, т.е. время, затраченное им и на ожидание, и на обслуживание.

Средние значения величин q и t_q обозначим соответственно через $E(q)$ и $E(t_q)$. Пусть ρ – коэффициент использования оборудования. Тогда благодаря устойчивости состояния

$$\rho = E(n) E(t_s)$$

Основываясь на основной формуле теории очередей с одним проборм обслуживания, которая была получена Хинчиным и Поллачеком, была выведена формула [2], позволяющая рассчитать среднее время пребывания запроса в системе

$$E(t_q) = E(t_s) + \frac{\rho E(t_s)}{2(1-\rho)} \left\{ 1 + \left[\frac{\sigma_{t_s}}{E(t_s)} \right]^2 \right\}.$$

Рассмотрим пример, иллюстрирующий возможную выгоду от использования предлагаемой выше автором корректировки архитектуры АИС. Предположим, что в системе формируется в среднем $E(n) = 2$ запроса в секунду, сервер тратит на обработку запроса $E(t_s) = 400$ мс, стандартное отклонение равно также $\sigma_{ts} = 400$ мс, т.е. время обслуживания имеет экспоненциальное распределение, это связано с тем, что запросы имеют различную сложность. Тогда пользователь тратит на ожидание выполнения запроса в среднем $E(t_q) = 2$ с.

Если время на обработку запроса снизить на 25%, т.е. $E(t_s) = 300$ мс, то это позволит снизить время ожидания пользователя в среднем до $E(t_q) = 0,75$ с. или на 62,5%.

При характеристиках сервера $E(n) = 2$ запроса в секунду и $E(t_s) = 400$ мс коэффициент использования будет равен $\rho = E(n) E(t_s) = 0,8$ и увеличение нагрузки на 25% (2,5 запроса в секунду) данный сервер просто не выдержит ($\rho = 1$). В случае снижения времени обработки запроса на 25% коэффициент использования будет равен $\rho = 0,75$, а время обработки будет в среднем $E(t_q) = 1,2$ с, что меньше времени ожидания пользователем выполнения запроса до повышения нагрузки исходной системы на 40%.

ЛИТЕРАТУРА

1. Подход в технологии построения защищенных информационных систем на основе СУБД Oracle. Материалы Всероссийской конференции «Методы и технические средства обеспечения безопасности информации», С.-Петербург, 2004.
2. Дж. Мартин Системный анализ передачи данных. М.: 1975.

РАССМОТРЕНИЕ ПРОБЛЕМ, ВОЗНИКАЮЩИХ ПРИ ШИФРОВАНИИ ДАННЫХ В БАЗЕ ДАННЫХ

С.И. Ткаченко

МИФИ, г. Москва, rva@mephi.edu

В работе рассмотрены проблемы, возникающие при использовании средств шифрования данных в базе данных, предоставляемых системой управления базами данных (СУБД) Oracle. Также в данной работе автор делает постановку задачи, решение которой позволит устранить ряд проблем.

Сегодня хорошо просматривается тенденция к увеличению круга пользователей в различных автоматизированных информационных системах (АИС), все больше персональной и конфиденциальной информации передается на хранение в базы данных (БД), соответственно, все острее встает вопрос о защите этих данных от несанкционированного доступа. Параллельно растет количество лиц, имеющих в том или ином виде административный доступ к БД, позволяющий прочитать любые данные. Это приводит к тому, что на «серых» рынках можно приобрести за небольшие деньги копию практически любой интересующей БД.

Решение, которое позволит существенно ограничить доступ к данным, заключается в ведении шифрования данных, хранящихся в БД, при этом ключ хранится только у тех пользователей, которые действительно имеют право на доступ к данным, данное решение предполагает реализацию процессов шифрования и дешифрования на стороне клиента. Следует отметить, что администратор, в общем случае, не является

таковым, ему лишь необходимо производить операции резервного копирования и восстановления. Действительно, при шифровании данные по-прежнему хранятся в БД, и управление с точки зрения администрирования может производиться в прежнем объеме.

Тем не менее, существует ряд проблем, ограничивающих использование шифрования, а именно, используется шифрование или нет, все равно необходимо иметь возможность выполнять ряд операций над данными. Определим множество операций M необходимых для работы с данными, где элементами множества будут следующие операции:

- m_1 – операция проверки на равенство значений ($=$),
- m_2 – операция проверки на не равенство значений ($<>$),
- m_3 – операция конкатенации,
- m_4 – операция поиска подстроки в строке,
- m_5 – операции сравнения ($>$, $>=$, $<$, $<=$),
- m_6 – операция индексирования.

После введения шифрования доступными сегодня в Oracle Advanced Server security [1] алгоритмами шифрования становится возможным подмножество операций $M_1\{m_1, m_2\} \subset M$. Т.е. проведя операцию проверки на равенство между шифрованными значениями, можно говорить о равенстве открытых значений. Использование остальных операций требует значительных затрат ресурсов сервера, что снижает доступность данных в АИС в целом. Действительно, предположим, существует таблица, в которой значения одного из столбцов хранятся в шифрованном виде. Количество строк равно 10000. Чтобы произвести сортировку открытого текста по данному столбцу серверу необходимо динамически произвести дешифрование значений всего столбца и произвести их сортировку, но при этом, не используя индексов. Среднее время выполнения операции, по предварительным оценкам, увеличится на 200%, соответственно снизится доступность системы в целом, а если записей не 10000, а несколько миллионов, некоторые сервера просто не справятся с нагрузкой.

Выход из сложившейся ситуации может быть следующим, необходимо разработать такой алгоритм шифрования, который позволил бы расширить множество M_1 до M , т.е. сделать $M_1 = M$. Таким образом снять необходимость дешифрования информации перед выполнением операций, что повысит защищенность и доступность системы в целом [2], а также снизит стоимость системы.

ЛИТЕРАТУРА

1. Oracle. Руководство по безопасности. Марлен Терьо, Аарон Ньюмен. М.: Лори, 2004.
2. Предложение технологии построения АИС, повышающей уровень доступности данных и сохраняющей заданный уровень сложности администрирования. Материалы XIII Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы». М.: МИФИ, 2006.

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ ПЕРЕДАВАЕМЫХ ПО СЕТИ ДАННЫХ СУБД ORACLE

С.Г. Филатов

МИФИ, г. Москва, pva@merphi.edu

В работе рассматривается безопасность сетевой передачи данных между базами данных СУБД Oracle.

В настоящее время большие объемы информации хранятся в различных СУБД с использованием разнообразных механизмов репликации и связей между базами данных. В качестве механизмов репликации обычно используются стандартные решения производителей баз данных (в рассматриваемом нами случае используется СУБД Oracle). Однако использование таких решений может быть потенциально небезопасным из-за того, что основной упор в данных решениях делается на производительности СУБД и целостности данных. Для устранения таких потенциально небезопасных решений существуют несколько программных пакетов, как выпущенных Oracle Corporation, так и распространяющихся по лицензии GNU.

В своей работе я использовал созданный мной тестовый стенд, на котором выявлялись и проверялись:

- способы несанкционированного доступа к данным;
- способы получения системной информации СУБД Oracle: имена пользователей, пароли пользователей, структура базы данных и так далее;
- способы нарушения целостности (замена некоторого незначительного количества байт в передаваемых данных с целью нарушения целостности сетевого пакета СУБД);
- способы нарушения достоверности передаваемой информации (замены данных в сетевом пакете СУБД с целью изменить содержание пакета СУБД не нарушая при этом целостности пакета).

Цель данной работы – определить возможность несанкционированного доступа к передающимся по сети данным СУБД Oracle и найти методы противодействия несанкционированного доступа к данным. Так же определялась возможность нарушения целостности и достоверности передающихся по сети данных СУБД Oracle.

Были рассмотрены следующие варианты передачи данных:

- передача в открытом виде по протоколу Net8;
- передача данных, зашифрованных с помощью программного пакета Oracle Advanced Security;
- передача данных, зашифрованных с помощью программного пакета OpenSSH;
- передача зашифрованных данных по протоколу ipsec.

Перечисленные выше варианты охватывают все основные способы защиты сетевого трафика СУБД Oracle:

- отсутствие шифрования;
- шифрование с помощью продукта Oracle corporation;
- шифрование с помощью открытого продукта, являющегося частью ядра операционной системы (ipsec);
- шифрование с помощью открытого продукта, являющегося прикладной программой.

Было выяснено, что при передаче данных в открытом виде вполне возможно получить несанкционированный доступ к данным, а так же нарушить целостность и достоверность передаваемых данных. При передаче данных, зашифрованных с помощью программного пакета Oracle Advanced Security возможно нарушение целостности передаваемых данных и обнаружение некоторых системных параметров СУБД Oracle, таких как имя пользователя, имя базы данных, сетевые настройки СУБД Oracle. При передаче зашифрованных данных по протоколу ipsec либо помощью программного пакета OpenSSH несанкционированный доступ, а так же нарушения целостности и достоверности данных не возможны.

Выполненная работа позволяет сформулировать обоснованные рекомендации по защите передаваемых по сети данных СУБД Oracle .

ЛИТЕРАТУРА

1. Oracle9i Application Developer's Guide – Large Objects (LOBs) Release 2 (9.2).
2. Oracle для профессионалов. Книга 1 Архитектура и основные особенности. Второе издание. Том Кайт. DiaSoft, Москва, Санкт-Петербург, Киев, 2004 г.
3. Oracle9i Security Handbook (Oracle 9.2 documentation A96582-01).

ВЫБОР ТЕОРЕТИКО-ИГРОВОЙ МОДЕЛИ ОПИСАНИЯ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ

М.О. Чибиров

МИФИ, г. Москва, pva@merphi.edu

Использование теории игр в области защиты информации

Теория игр давно и успешно применяется для моделирования процессов защиты информации. Однако, в большинстве источников, в качестве примера, используется антагонистическая игра с нулевой суммой. В этом случае, для генерации хода применяется мини – максный поиск по дереву вариантов. Исследования по мини – максному поиску в литературе основываются на предположении, что в конце игры один

из игроков побеждает, а другой проигрывает[1]. В области информационной защиты, эта симметрия нарушена, так как злоумышленник может иметь цель полностью противоположную цели системы защиты информации, а может добиваться того, что нарушит требования политики безопасности, но не скомпрометирует первоочередные цели системы[2].

Различие конечных целей дискредитирует предположение, применяемое в текущих исследованиях о том, что цели злоумышленника и системы защиты варьируются во вполне определенных рамках. Это также уменьшает вероятность того, что набор эвристик включаемых в платежную функцию злоумышленника является подмножеством эвристик систем защиты. Для решения данной проблемы, процессы защиты информации могут быть смоделированы некооперативной игрой с двумя участниками и ненулевой суммой выигрыша. Эта игра отличается тем, что выигрыш одного игрока не равен проигрышу другого. Кооперация игроков либо невозможна, либо запрещена. В этом случае требуется создание базы данных, в которой бы хранились цели и эвристики, соответствующие достижению этих целей. Тогда при моделировании поведения игрока можно исходить от эвристики, включенной базу данных. Таким образом, можно смоделировать не только платежную функцию противника, но и идентифицировать его возможные цели.

ЛИТЕРАТУРА

1. Оуэн Г. Теория игр./Пер. с англ.-М.:Мир,1971.
2. Домарев В. В Безопасность информационных технологий. Методология создания систем защиты. М.: ООО «ТИД «ДС», 2002

РАЗРАБОТКА АРМ ДЛЯ ПРОВЕДЕНИЯ ПЕРВИЧНЫХ ИССЛЕДОВАНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ПРЕДМЕТ ВЫЯВЛЕНИЯ СВОЙСТВ, ПОДПАДАЮЩИХ ПОД ДЕЙСТВИЕ 28 ГЛАВЫ УК РФ: МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЙ ПРОГРАММНЫХ СРЕДСТВ СКРЫТОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ (ПССИВ)

Е.И. Чугунов

МИФИ, г. Москва, pva@mephi. edu

Целью работы является создание методического аппарата и специального программного обеспечения (ПО) для решения задач защиты объектов СВТ органов безопасности от компьютерных вирусов и ПССИВ, а также оперативно-технических задач в ходе расследования компьютерных преступлений.

Объектом исследования являются ПССИВ в среде ОС Windows NT4/2000/XP/2003, способы их внедрения, методы обнаружения признаков наличия программных закладок (ПЗ) в ПО [5]. Методика проведения испытаний основана на динамическом и статическом анализе поведения исследуемой прикладной программы (ПП) с целью выявления скрытого информационного воздействия [1, 6]. Ключевым является распознавание в ПП шаблонов поведения вредоносного кода (ШПВК) и отклонений от штатного функционирования программы.

Предложен метод построения и распознавания ШПВК и шаблонов поведения прикладной программы (ШППП) в графе передачи управления между системными вызовами (СВ) ПП, полученного в динамике [7]. Рассмотрены методы генерации ШПВК и ШППП, основанные на алгоритме кластеризации вокруг ядер [2]. Для определения подобия ШПВК, ШППП и графа передачи управления между СВ в ПП, рассмотрено понятие энтропийного расстояния [3].

Сформулированы основные классы программных закладок, выявляемых средствами динамического анализа, их признаки, способы их выявления [5]. Показано, что большую часть признаков, выявляемых динамическим анализом, составляют: функции, реализующие разрушающее воздействие; функции внедрения ПЗ; функции маскировки ПЗ; используемые объекты программно-аппаратной среды (ПАС), в том числе интерфейсы.

Показано, что следует следить не только за СВ и обращениями к ресурсам системы, но и за всеми объектами исполнительной системы. Например, учет наличия объектов, времени их создания и количества. Фактически, эти цели следуют из задач обеспечения целостности ПАС, представляя механизм обнаружения несанкционированного воздействия со стороны ПП на ПАС [4].

Для статического анализа в силу сложности его формализации, решено ограничиться анализом строк и РЕ заголовка исполняемого файла. В качестве строк хранятся имена импортируемых и экспортируемых функций, основные пути реестра и жесткого диска, с которыми работает образец, названия ресурсов, команды текстовых сетевых протоколов (SMTP, POP3, IRC, HTTP и т.д.), команды интерпретатора. Выделяются названия сетевых интерфейсов (pipes, mailslots, winsockets и т.д.), определяется, имеет ли ПП доступ к адресному пространству других процессов. Показано, что по выделенным именам функций и путям можно восстановить часть функционала образца. Анализируется весь файл и все его секции, в том числе и ресурсы внутри которых могут быть исполняемые файлы, которые определяются по наличию РЕ заголовка.

Любому вредоносному воздействию характерен определенный набор функций, путей реестра и файловой системы. Важным является

взаимное расположение строк относительно в файле. Поэтому составляются шаблоны, которые это учитывают.

Основной задачей на данный момент является построение ШПВК и набора ШППП, отработка алгоритмов распознавания ШПВК. Опробование подсистем динамического анализа и подсистемы статического анализа, связывание этих подсистем.

ЛИТЕРАТУРА

1. ГОСТЕХКОМИССИЯ России. Руководящий документ. Защита от несанкционированного доступа к информации.
2. *Сапегин Л.Н.* (<http://beda.stup.ac.ru/RV-conf/v05/006/>) «Метод кластеризации многомерных статистических данных»
3. *Вадим Дунаев.* «О ранговых распределениях в классификации».
4. *Касперски К.* «Секреты поваров компьютерной кухни или ПК: решение проблем» Издано: 2003, ВНУ
5. *Чугунов Е. И.* Труды всероссийской конференции студентов, аспирантов и молодых ученых. «Поэтапная методика и схема стенда по анализу программных средств на наличие закладных элементов»
6. *Казарин О.В.* «Теория и практика защиты программ». 2004.
7. «API Spying Techniques for Windows 9x, NT and 2000» (<http://www.internals.com/articles/apispy/apispy.htm>)

АУТЕНТИФИКАЦИИ В КОРПОРАТИВНЫХ ПОРТАЛАХ

С.С. Велигодский , Н.Г. Милославская
МИФИ, г. Москва, milmur@mephi.edu

Современные задачи ведения бизнеса требуют решения проблемы управления и поддержки данной среды путем создания единого интерфейса доступа сотрудников, клиентов и партнеров к различным сервисам и приложениям , называемого информационным порталом. Как правило, порталы обладают открытой архитектурой, позволяющей расширять их функциональность за счет добавления сторонних приложений или дополнительных компонентов. На сегодняшний день в рамках комитета JSR-168 разработаны и утверждены спецификации программных интерфейсов, предназначенных для создания специализированных порталных приложений – портлетов. Основными функциональными возможностями корпоративных порталов являются поддержка принципа единой регистрации пользователей в корпоративной инфраструктуре (Single Sign-On) и поддержка средств интеграции приложений (Enterprise Application Integration). Указанные механизмы создают определенные риски информационной безопасности – в случае компрометации учетной записи пользователя злоумышленник получит

полный доступ ко всем его порталным ресурсам. Вследствие этого при построении корпоративных порталов с точки зрения информационной безопасности необходимо уделить особое внимание вопросам надежной аутентификации пользователей. Анализ механизмов аутентификации, предлагаемых крупнейшими разработчиками порталных технологий (IBM, BEA, Oracle и т.д.) показывает, что их реализация подсистемы аутентификации в целом основывается на стандартном наборе Web-технологий (идентификаторы сессий, аутентификация по имени и паролю, протокол SSL и пр.), обладающих известными слабостями. Сегодня использование данных технологий в ряде случаев не отвечает требованиям безопасности и зачастую создает иллюзию защищенности разработка новых технологий аутентификации пользователей в сложных Web-приложениях особенно актуальна.

Одним из возможных способов решения данной проблемы предлагается механизм аутентификации по схеме «запрос-ответ», аналогичный протоколу, реализованному компанией Microsoft в ОС семейства Windows NT, но в отличие от него полностью реализованный на базе Web-технологий. При первоначальном запросе пользователем страницы аутентификации, сервером портала создается случайное значение, которое записывается в скрытое поле страницы, возвращаемой сервером в ответ на запрос пользователя. На стороне пользователя с помощью специализированного скрипта осуществляется вычисление значения хеш-функции от введенного пароля пользователя и случайного значения, полученного от сервера портала. Далее это значение передается на сервер портала одновременно с остальной регистрационной информацией. Сервер портала, зная пароль пользователя, осуществляет аналогичные операции и сравнивает свое значение и полученное от пользователя. В случае их соответствия сервер портала считает, что он успешно аутентифицировал пользователя. В настоящее время разработаны скрипты, реализующие вычисление значений хеш-функций по протоколу MD5. Благодаря тому, что скрипт создан на языке сценариев JavaScript, поддержка которого встроена во все современные Интернет-браузеры, пользователю не требуется установка дополнительного программного обеспечения.

Предложенный метод обеспечивает защиту от активного и пассивного перехвата сетевого трафика, однако не обеспечивает защиту от клавиатурных шпионов и атак путем прямого подбора паролей. Данный метод может быть усилен путем хранения парольной информации на специализированных аппаратных носителях (например, устройствах Touch Memory).

После проведения процедуры аутентификации пользователя сервер портала должен создать идентификатор сессии пользователя и все последующие запросы от него обрабатывать в рамках данной сессии. В случае перехвата и кражи данного идентификатора злоумышленник получает возможность выполнять запросы к portalу от имени законного пользователя. При этом хочется отметить, что на сегодняшний день вопросы надежной защиты идентификаторов сессий не решены.

ЛИТЕРАТУРА

1. JSR 168 Reference Implementation Pluto <http://jakarta.apache.org/pluto/>.
2. Information about the user profile attributes in P3P: <http://www.w3c.org/TR/P3P>.
3. US Army Goes To War with P2P, Graeme Wearden, ZDNet, August 31, 2001, <http://www.zdnet.com/>
4. Collaborative Tools, Command and Control Battlelab, www.c2b.hurlburt.af.mil/collaborativetools.htm
5. Application Platform Suites, An Architectural Cost Analysis, BEA, 2003, <http://www.bea.com>
6. Websphere Portal – Express for Multiplatforms, IBM, <http://www.ibm.com/redbooks/>

ПОСТРОЕНИЕ РКІ НА ОСНОВЕ ЦИФРОВОЙ ПОДПИСИ С ОПЕРЕЖАЮЩЕЙ БЕЗОПАСНОСТЬЮ

Г.В. Зубенко

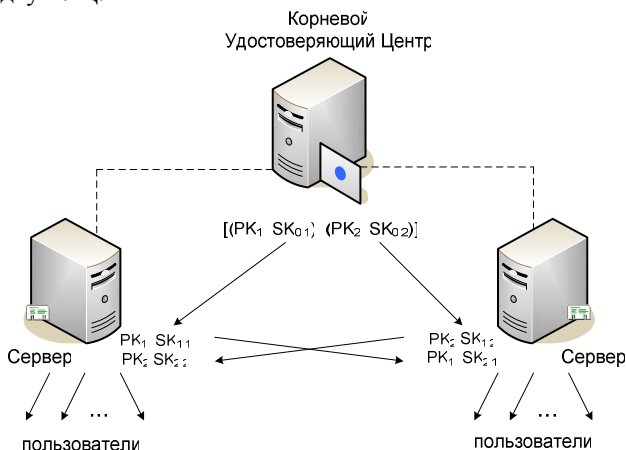
МИФИ, г. Москва,) oka@mephi.edu

Недавно в криптографической теории получили большое распространение схемы цифровой подписи и асимметричного шифрования с опережающей безопасностью. Они отличаются от классических схем тем, что, основываясь на сложности решения задачи распознавания Диффи-Хеллмана, позволяют защитить уже подписанные или зашифрованные документы, даже если секретный ключ системы скомпрометирован. Достигается это сменой секретного ключа через определенные промежутки времени без соответствующей замены открытого ключа. Более подробно с ними можно познакомиться в работах М. Bellare и S.K. Miner [1, 2, 3].

В работе представлена инфраструктура открытых ключей электронного документооборота на основе схемы подписи с опережающей безопасностью.

Суть заключается в том, что множество ключевых пар (открытый ключ и секретный ключ) генерируется на основе схемы подписи с опережающей безопасностью и распределяется между удостоверяющими

центрами (УЦ). В работе предложена математическая модель их распределения, которая позволяет при компрометации одного из УЦ, не допустить компрометации остальных. При этом сертификаты содержат столько подписей, сколько секретных ключей. При их проверке используется соответствующее множество открытых ключей, которое является открытыми ключами корневого УЦ. На рисунке показан пример для двух УЦ.



Только в случае, когда все подписи корректны, проверяющий может считать полученный сертификат корректным. Более того, с помощью набора открытых ключей центра сертификации можно проверить любой список отозванных сертификатов.

При использовании данного метода рекомендуется совмещать его с методами криптографии с изоляцией ключа. Схема подписи с изоляцией ключа (*KIS – key-insulated signature scheme*) предложена Y. Dodis [6]. *KIS* – один из способов смягчить последствия компрометации, в случае, когда она уже произошла. Это достигается за счет того, что секретный ключ, хранимый на плохо защищенном устройстве, обновляется в определенные периоды времени с помощью взаимодействия с физически безопасным устройством, которое хранит «корневой ключ». Так же как и в схеме подписи с опережающей безопасностью, открытый ключ остается постоянным, и подписи в любых периодах времени могут быть проверены одним открытым ключом.

Таким образом, представленная схема имеет следующие преимущества:

- 1) один ключ для проверки списка отозванных сертификатов;
- 2) длина цепочки сертификации равна числу секретных ключей в наборе;

3) нет зависимости между распределенными УЦ, что позволяет сохранить в секрете ключи УЦ, при компрометации одного из них.

ЛИТЕРАТУРА.

1. *Mihir Bellare and Sara Miner*. A forward-secure digital signature scheme. In *Advances in Cryptology – CRYPTO '99*, Springer-Verlag, 1999. Revised version is available from <http://www.cs.ucsd.edu/~mhir/>.
2. *Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest*. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2): pp. 281–308, April 1988.
3. *Itkis G., Reyzin L*. Forward Secure Signatures with Optimal Signing and Verifying // *CryptoBytes*, Vol. 5, No. 2, Summer 2002, pp. 14–25
4. *Adi Shamir*. On the generation of cryptographically strong pseudorandom sequences. *ACM Transactions on Computer Systems*, 1(1): pp. 38–44, February 1983.
5. *Louis Claude Guillou and Jean-Jacques Quisquater*. A «paradoxical» identity-based signature scheme resulting from zero knowledge. In Goldwasser, pp. 216–231.
6. *Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu and Moti Yung*. Strong Key-Insulated Signature Schemes, International Workshop on Practice and Theory in Public Key Cryptography (PKC 2003), Lecture Notes in Computer Science, Vol. 2567, pp. 130–144, Springer-Verlag, 2003.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ И РЕАЛИЗАЦИИ СХЕМ РАСПРЕДЕЛЕННОГО БЛОЧНОГО ШИФРОВАНИЯ

М.М. Мясумов

МИФИ, г. Москва, oka@merphi.edu

Большинство известных работ, посвященных пороговой криптографии, касаются вопросов распределения криптографических примитивов с открытым ключом, в частности, схем пороговой подписи и механизмов пороговых операций расшифрования. Но в последнее время предприняты попытки применения пороговой криптографии для схем симметричного шифрования, и в частности, для операций блочного зашифрования и расшифрования. В докладе рассматриваются некоторые прикладные вопросы построения и реализации таких схем.

В пороговой криптографии основной целью распределения операций вычисления базовых криптографических примитивов между определенным числом узлов являются:

- ослабление требований доверия к безопасности отдельных узлов;
- повышение устойчивости к выходам из строя отдельных узлов.

Существует несколько причин для распределенного выполнения криптографических операций:

1) повышение эффективности (отдельные узлы выполняют различные задачи);

2) обеспечение отказоустойчивости (если некоторые узлы выйдут из строя, другие могут выполнять их задачи);

3) повышение защищенности к утрате части ключей (секретные данные, необходимые для выполнения задачи, распределены между узлами).

Впервые техника распределенного выполнения операций блочного шифрования была в работе [1]. Метод, представленный авторами этой работы, назван *последовательным распределением (sequence sharing)*.

При разделении алгоритма блочного шифрования подразумевается, что операции блочного зашифрования и расшифрования являются процессами, распределенными между группой объектов. При распределенном зашифровании группа отправителей совместно генерирует шифртекст, который они потом отправляют одному получателю. При распределенном расшифровании один отправитель зашифровывает сообщение и отправляет его группе получателей, которые должны совместно расшифровывать сообщение.

Рассмотрим пример возможного применения техники распределенного выполнения алгоритма блочного шифрования. Директора филиалов компании установили систему, использующую алгоритмы блочного шифрования для связи с генеральным директором, который находится в главном офисе. Задача распределенного шифрования в данном случае состоит в следующем: любые, например, три директора могут совместно сгенерировать зашифрованное сообщение для генерального директора и отправить ему, который, в свою очередь, корректно расшифровав сообщение, может быть уверен, что некоторая группа, по меньшей мере, из трех директоров совместно сгенерировала шифртекст. Задача распределенного расшифрования заключается в следующем: генеральный директор компании будет обладать возможностью отправлять зашифрованные сообщения директорам филиалов, и для того чтобы они смогли его расшифровать, необходимо взаимодействие минимум трех директоров филиалов.

Автором доклада представлены следующие варианты реализации схем распределенного блочного шифрования [2]:

- распределенное блочное шифрование с использованием схемы пороговой криптографии;
- разделение алгоритма блочного шифрования, основанное на каскадах;

- разделение алгоритмов блочного шифрования, используя последовательное деление;
- с использованием кумулятивного отображения;
- каскадное разделение алгоритма блочного шифрования с использованием кумулятивных отображений;
- разделение блочного шифрования с использованием XOR-сумм;
- разделение алгоритма блочного шифрования, основанное на разбиении открытого сообщения.

Представленные методы распределения операций блочного шифрования в одинаковой степени применимы, но каждый имеет свои особенности и области эффективного применения. Решающими критериями их выбора являются увеличение сообщения при зашифровании и объем ключевой информации, необходимой для зашифрования и расшифрования участниками схемы.

ЛИТЕРАТУРА

1. Brickell E., Crescenzo G., Frankel Y. Sharing Block Ciphers. *Information Security and Privacy, Lecture Notes in Computer Science*, 2000.
2. Martin K. M., Safavi-Naini R., Wang H., Wild P. R. Distributing the Encryption and Decryption of a Block Cipher, 2004.

СОВРЕМЕННЫЕ БИЗНЕС-МОДЕЛИ И РЕШЕНИЯ РАЗВЕРТЫВАНИЯ PKI

О.Ю. Полянская

МИФИ, г. Москва, olga@mephi.edu

В докладе рассматриваются преимущества технологии PKI (Public Key Infrastructure – инфраструктура открытых ключей), обеспечивающей высокий уровень безопасности корпоративной среды и способствующей более тесному взаимодействию с партнерами, поставщиками и потребителями, а также анализируются возможности PKI для реализации типовых моделей ведения бизнеса.

PKI предлагает единую инфраструктуру безопасности, которая может использоваться для множества приложений в большинстве гетерогенных сред. Технология PKI считается единственной позволяющей применять методы подтверждения цифровой идентичности при работе в открытых сетях [1]. С каждым годом возрастает важность технологии PKI для корпоративной среды, для реализации компаниями однократной регистрации, защищенного обмена сообщениями, электронной коммерции, виртуальных частных сетей. Сегодняшний бизнес все в

большей степени начинает использовать эту технологию, обеспечивающую высокий уровень безопасности и способствующую более тесному взаимодействию с партнерами, поставщиками и потребителями. Помимо этого, к дополнительным преимуществам от внедрения технологии PKI можно отнести:

- повышение эффективности делопроизводства;
- оптимизацию рабочего процесса;
- выбор экономически эффективного решения безопасности;
- сокращение бумажного документооборота;
- сокращение расходов на администрирование;
- снижение ущерба от компьютерных хищений и мошенничества;
- сокращение расходов на телекоммуникации;
- предоставление платных услуг.

Как свидетельствуют многие примеры развертывания PKI, доминирующими сегодня бизнес-моделями являются модель внутренних коммуникаций, модель внешних коммуникаций и гибридные модели [2].

Бизнес-модель внутренних коммуникаций затрагивает взаимодействия внутри организации, а бизнес-модели внешних коммуникаций – взаимодействия типа «бизнес-бизнес» и «бизнес-заказчик». Для установления деловых коммуникаций и связывания своих корпоративных PKI-доменов организации должны иметь серьезную мотивацию и определенные цели бизнеса, например, потребность в безопасности транзакций электронной коммерции.

Взаимодействие «бизнес-заказчик» осуществляется, как правило, посредством Интернета. Отношения, возникающие в сфере электронной коммерции между продавцами или поставщиками услуг и клиентами, описываются двумя бизнес-моделями внешних коммуникаций. Первая модель – это модель доверия, сконцентрированного вокруг пользователя. В этом случае индивидуумы получают свои сертификаты от поставщика услуг третьей стороны или генерируют свои собственные сертификаты (например, при помощи Open PGP). Чаще всего для ведения бизнеса индивидуумы используют стандарт Web-технологии. В этой модели практически невозможно осуществлять контроль и управлять жизненным циклом сертификатов и ключей, конфиденциальность связи между браузером и сервером и соответственно безопасность транзакций электронной коммерции обеспечивается при помощи протокола SSL/TLS.

Вторая модель внешних коммуникаций считается более управляемой и более безопасной, чем первая. В ней сама организация (например, банк) действует как УЦ и выпускает сертификаты для тех индивидуумов, с которыми взаимодействует в рамках ведения бизнеса, а также может предложить им пользоваться специальным программным

обеспечением, позволяющим более полно управлять жизненным циклом сертификатов и ключей и лучше защищать коммуникации. Эта модель дает возможность организации контролировать назначение и сферу применения выпускаемых сертификатов.

Модели внутренних и внешних коммуникаций не должны рассматриваться как взаимно исключающие друг друга, безусловно, для многих организаций естественно одновременно предлагать сервисы внутренней и внешней безопасности, основанные на технологии PKI. На практике многие из сегодняшних реализаций PKI начинаются с небольшого пилотного проекта, ориентированного на ограниченное сообщество пользователей (несколько десятков или сотен), а затем следуют крупномасштабные инициативы, предполагающие включение дополнительных приложений, увеличение числа пользователей и разветвление коммуникаций «бизнес-бизнес» и «бизнес-заказчик».

ЛИТЕРАТУРА

1. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. Москва «Горячая линия – Телеком», 2004
2. C. Adams, S. Lloyd. Understanding PKI. Concepts, Standards and Deployment. Second Edition, Addison-Wesley, 2002

ОБОБЩЕНИЕ СХЕМЫ ПРОЕКТИРОВАНИЯ ПОРТАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

С.В. Зыков

МИФИ, г. Москва, szykov@ngk.itera.ru

Манипулирование накопленными современным обществом объемами данных представляет существенную проблему для ИС. Представлена комплексная модель для обработки корпоративного контента, включающая средства поддержки всего жизненного цикла (ЖЦ) программного обеспечения (ПО), а также объединяющая представления для предметной области (ПрО) и среды вычислений.

Цель статьи – представление комплекса моделей, основанного на творческом синтезе основных положений теорий конечных последовательностей [1], вычислений (по Д.С. Скотту) [3], категорий [4], семантических сетей [5] и абстрактных машин (АМ) [6], а также использующего принцип свертывания [7] и фреймы для визуализации [5].

Важным результатом для Интернет-систем оказывается достаточность двукратного применения принципа свертывания.

Среди объектов данных (ОД) будем различать классы, (элементы) шаблонов страниц ИС управления контентом (ИСУК) и (значения) контента, которые являются компонентами для построения модели ОД, а их конкретизации – функциями соотнесений.

Обобщенно, элементы модели представимы тройками <класс, объект, значение>, что развивает концептуальный метод проектирования В.Э. Вольфенгагена [7] в направлении современных объектных ИС, прежде всего, ориентированных на Интернет-среду вычислений.

В случае Интернет-ИС подход выявляет следующие виды сущностей:

- 1) класс объектов интегрированной БД программного комплекса;
- 2) объект шаблона информационной страницы ИСУК;
- 3) информационная страница ИСУК (как означивание ОД шаблона).

Переходы (1-2) и (2-3) являются шагами *концептуализации* – снижения уровня абстракции от классов к ОД и значениям.

Адекватность модели обусловлена наличием операций абстракции (т.е. изменения уровня концептуальности сущностей) и аппликации (приложения функции к аргументу). Последняя позволяет формализовать вычисление значений с поэтапной конкретизацией при проектировании.

Интеграция ИС вовлекает CASE-средство ConceptModeller и алгоритм объединения компонент в корпоративные программные комплексы [2].

При конкретизации класса в соотнесении с шаблоном ИСУК означивание семейства шаблонов устанавливает в значение «истинно» его элемент, совпадающий по номеру с номером шаблона. Второе соотнесение приводит к конкретизации шаблона ИСУК значениями контента. Исследование взаимодействия классов, объектов и значений позволяет сформулировать основной принцип моделирования:

[класс объектов] : соотнесение → объект.

Созданная модель ОД ПрО адекватно формализует данные и метаданные гетерогенных ИС «унаследованных», промежуточных и современных архитектур, в т.ч. с использованием промежуточного ПО, унифицируя и упорядочивая управление сложными ОД в Интернет-среде.

В соотнесении с передовым коммерческим ПО (IBM WebSphere, BEA WebLogic, Oracle Portal, Microsoft CMS и др.) открываются возможности строго математического тестирования и верификации ИС и программных комплексов, улучшается манипулирование гетерогенными ОД высокой сложности, ускоряется построение запросов и отчетов гетерогенной структуры, интеллектуализируется обработка мультимедийного контента.

Созданная методология, модели, алгоритмы, методы и программные средства были практически апробированы при реализации Интернет-сайта (www.itera.ru) и Интранет-портала Международной группы компаний «ИТЕРА» (около 150 компаний более чем в 20 странах).

В итоге по важнейшим показателям совокупной стоимости владения (ТСО) и возврата инвестиций (ROI) реализованный программный комплекс превосходит названные аналоги в среднем более чем на 30% [8–11].

ЛИТЕРАТУРА

1. *Барендрегт Х.* Лямбда-исчисление. Его синтаксис и семантика.– М.:Мир, 1985. 606 с.
2. *Зыков С.В.* Проектирование Интернет-порталов. М.:МФТИ, 2005. 258 с.
3. *Scott D.S.* Lectures on a mathematical theory of computations. Oxford University Computing Laboratory Technical Monograph. PRG-19, 1981. 148 p.
4. *Curry H.B., Feys R.* Combinatory logic, vol.I, North Holland, Amsterdam, 1958.
5. *Roussopoulos N.D.* A semantic network model of data bases, Toronto Univ., 1976.
6. *Cousineau G., Curien P.-L., Mauny M.* The categorical abstract machine. // Science of Computer Programming 8(2), p.p.173-202, 1987.
7. *Wolfengagen V.E.* Object-oriented solutions. // ADBIS96, Springer, 1996. PP. 407–431.
8. *Zykov S.V.* *ConceptModeller*: a Problem-Oriented Visual SDK for Globally Distributed Enterprise Systems. // CSIT'2005, Ufa:USATU, 2005
9. *Zykov S.V.* Abstract Machine as a Model of Content Management. // CSIT2004. Budapest. 2004. Vol. 1. PP. 251–252
10. *Zykov S.V.* Integrated Methodology for Internet-Based Enterprise Information Systems Development. // WEBIST2005, Miami:INTICC, 2005, PP. 168–175
11. *Zykov S.V.* The Integrated Approach to ERP:Embracing the Web.//CSIT'2002. Patras. 2002.

УПРАВЛЕНИЕ ИНТЕРНЕТ-КОНТЕНТОМ: СЕМАНТИЧЕСКИЙ ПОДХОД

С.В. Зыков

МИФИ, г. Москва, szykov@ngk.itera.ru

Быстрый рост числа и объемов разнородных Интернет-ресурсов (ИР) требует концептуальной ясности процедур управления ими в динамичной, распределенной среде вычислений. Предлагается моделировать управление данными ИР на основе абстрактных машин (АМ) с состояниями. Представлены семантика модели, разработанные на ее базе инструментальные средства, результаты внедрения корпоративного portalного программного комплекса.

В современных условиях динамичного развития рынка актуален вопрос унификации корпоративной информационной инфраструктуры. В работе предлагается модель программного обеспечения (ПО) для управления корпоративным контентом на основе понятия состояния.

Моделирование ИС управления контентом (ИСУК) основано на синтезе типизированного λ -исчисления [1], комбинаторной логики и

теории категорий [4], АМ [5] и теории вычислений Д.Скотта в ее развитии [3], [6]. При этом адекватна модель в виде АМ управления контентом (АМУК), оперирующей в пространстве декартово замкнутых категорий и характеризующейся *состоянием* в произвольный момент времени.

АМУК моделирует отображение объектов шаблонов веб-страниц ИР в значения элементов веб-страниц (с точки зрения модели – означивание).

Семантика АМУК моделируется семантическими доменами Д.Скотта [3] по следующей схеме [2]: перечисление *стандартных* (наиболее частых), *конечных* (с явно перечислимыми элементами) доменов, их *конструкторов* (способов комбинирования) доменов и агрегирование доменов на основе конструкторов.

Язык АМУК содержит множество выражений, идентификаторов и команд (присваивание, ветвление, каскадирование инструкций и др.).

Вычислительная модель АМУК строится по следующей схеме:

1) определение *синтаксических доменов* (характеризующих основные синтаксические категории) для идентификаторов, выражений и команд;

2) определение *семантических функций*, отображающих синтаксические конструкции АМУК в семантические представления;

3) построение *семантических предложений* в форме состояний АМУК.

В процессе выполнения программы АМУК происходит смена состояния, состоящего из «памяти», которая в простейшем случае характеризует соответствие идентификаторов и значений. Состояние АМУК определяется состоянием «памяти». Управление «памятью» означает отображение из домена идентификаторов в домен значений.

Вычисление значения *денотата* (правильно построенной конструкции, в т.ч. команды) АМУК приводит к изменению состояния с ошибкой либо к связыванию переменной со значением. Денотатами констант являются значения этих констант в форме упорядоченных пар вида «(значение, состояние)» без смены состояния.

Заполнение шаблона ИСУК контентом может приводить к изменению состояния либо к генерации ошибки. Обновленное состояние ОД АМУК отличается от прежнего тем, что в памяти АМ происходит подстановка значения контента ИР вместо идентификатора ОД шаблона ИСУК.

Для перехода от модели к реализации создан комплекс программных средств, включающий ИСУК для предметно-ориентированного эргономичного динамического формирования корпоративного контента и его публикации на Интернет-портале; динамика состояний реализована на базе скриптов [2]. При коррекции дизайна портала миграция

ОД в новую метаинформационную структуру существенно упрощается и ускоряется.

Разработанные модель и ИСУК практически апробированы в ходе реализации Интернет-сайта (www.itera.ru) и Интранет-портала крупной (около 10 тыс. человек) международной группы компаний «ИТЕРА».

По важнейшим показателям совокупной стоимости владения (ТСО) и возврата инвестиций (ROI) реализованный программный комплекс превосходит передовые коммерческие аналоги (IBM WebSphere, Microsoft CMS и др.) в среднем более чем на 30%. Преимущества интеграции гетерогенных ИР получены за счет устранения дублирования и противоречий ОД, упорядочения схемы проектирования ПО и экономии трудозатрат корпоративных менеджеров.

ЛИТЕРАТУРА

1. *Барендрезт Х.* Лямбда-исчисление. Его синтаксис и семантика. М.: Мир, 1985. 606 с.
2. *Зыков С.В.* Проектирование Интернет-порталов. М.: МФТИ, 2005. 258 с.
3. *Scott D.S.* Lectures on a mathematical theory of computations. Oxford University Computing Laboratory Technical Monograph. PRG-19, 1981. 148 p.
4. *Curry H.B., Feys R.* Combinatory logic, vol.I, North Holland, Amsterdam, 1958.
5. *Roussopoulos N.D.* A semantic network model of data bases, Toronto Univ., 1976.
6. *Cousineau G., Curien P.-L., Mauny M.* The categorical abstract machine. Science of Computer Programming 8 (2), 1987. PP. 173–202.
7. *Wolfengagen V.E.* Object-oriented solutions. //ADBS96, Springer, 1996. PP. 407–431.

ИНТЕГРАЦИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОРПОРАЦИИ НА ОСНОВЕ ПОРТАЛЬНОЙ ТЕХНОЛОГИИ

С.В. Зыков

МИФИ, г. Москва, szykov@ngk.itera.ru

В условиях быстрого роста крупномасштабных программных комплексов для унификации управления распределенными гетерогенными информационными системами (ИС) требуется новая концептуально-методологическая основа. Представлены важнейшие компоненты подхода: математические модели, инструментальные средства и программное решение в форме корпоративного портала крупной международной группы компаний.

Манипулирование быстро растущими объемами данных ИС различной степени структурированности, зачастую созданными на основе разнородных программных технологий, вычислительных моделей и методов, алгоритмов и инструментальных средств, представляет собой

существенную проблему. Разработан и апробирован комплексный концептуально-методологический подход к проектированию Интернет-ориентированных ИС корпоративного масштаба, включающий семейство математических моделей для интегрированной предметной области (ПрО) и среды вычислений корпоративных ИС, а также алгоритмы и инструментальные средства проектирования и реализации.

Модели синтезируют основы теорий конечных последовательностей [1], вычислений [2], категорий [3], семантических сетей [4] и абстрактных машин (АМ) [5] с применением свертывания (концептуализации) [6] по схеме «класс – объект – значение». *Класс* – семейство ОД объединенной ПрО, *объект* – конкретизация класса шаблоном ИС управления контентом (ИСУК), *значение* формируется ИСУК как страница портала.

Семантика ИСУК полностью формализуется оригинальной АМ с состояниями на основе теории переменных доменов [2].

Разработанные формализации включают алгоритмы интеграции компонент в состав существующих ИС, трансляции семантической модели ПрО в схемы БД и UML-диаграммы, методы визуализации веб-страниц портала. Для перехода от моделей к программной реализации создан комплекс средств проектирования ПО (ConceptModeller) [7] и управления контентом (ИСУК) [8]. Средство ConceptModeller разработано для визуального предметно-ориентированного проектирования ПО с автоматизированной трансляцией из фреймовой модели в семейство UML-диаграмм для интеграции с CASE-ПО. Реинжиниринг до уровня фреймов позволяет верифицировать ПО на чисто математической основе. ИСУК осуществляет предметно-ориентированное формирование корпоративного контента и его публикацию на основе динамических ролевых профилей доступа с гибким редакторским циклом.

Интерфейс портала динамически формируется в зависимости от аппаратных предпочтений пользователя, конфигурации клиентского ПО и прав доступа с явным разделением на front-end и back-end.

Межмодульные интерфейсы используют стандартные веб-браузеры и средства промежуточного ПО (для «унаследованных» ИС – CORBA). Разработанные методология, модели, алгоритмы, методы и программные средства были апробированы при реализации Интернет-сайта (www.itera.ru) и Интранет-портала Международной группы компаний «ИТЕРА» (около 150 компаний более чем в 20 странах).

По важнейшим показателям совокупной стоимости владения (TCO) и возврата инвестиций (ROI) программный комплекс превосходит передовые коммерческие аналоги (IBM WebSphere, BEA WebLogic, Oracle Portal, Microsoft CMS и др.) в среднем более чем на 30% [7–12].

В результате внедрения концепции и методологии, преимущества интеграции ПрО получены за счет устранения дублирования и противоречий данных, упорядочения схемы проектирования и экономии трудозатрат менеджеров. Подход открывает возможности интеграции ИС, интеллектуального управления сложными ОД, а также позволяет верифицировать и тестировать ПО чисто математическими методами.

ЛИТЕРАТУРА

1. *Барендрегт Х.* Лямбда-исчисление, его синтаксис и семантика.–М.: Мир, 1985. 606 с.
2. *Scott D.S.* Lectures on a mathematical theory of computations. Oxford University Computing Laboratory Technical Monograph. PRG-19, 1981. 148 p.
3. *Curry H.B.*, Feys R. Combinatory logic, vol.I, North Holland, Amsterdam, 1958.
4. *Roussopoulos N.D.* A semantic network model of data bases, Toronto Univ., 1976.
5. *Cousineau G.*, *Curien P.-L.*, Mauny M. The categorical abstract machine. Science of Computer Programming 8 (2), 1987. PP. 173–202.
6. *Wolfengagen V.E.* Object-oriented solutions. // ADBIS96.–Springer, 1996, PP. 407–431.
7. *Zykov S.V.* ConceptModeller: a Problem-Oriented Visual SDK for Globally Distributed Enterprise Systems. // CSIT2005, Ufa:UGATU, 2005
8. *Zykov S.V.* Abstract Machine as a Model of Content Management // CSIT'2004, Budapest, Vol. 1. PP. 251–252.
9. *Zykov S.V.* Integrated Methodology for Internet-Based Enterprise Information Systems Development // WEBIST2005, Miami:INTICC, 2005.– PP. 168–175
10. *Zykov S.V.* Enterprise Portal: from Model to Implementation// CSIT'2004, Budapest, Vol. 2. PP. 188–193.
11. *Zykov S.V.* The Integrated Approach to ERP: Embracing the Web. // CSIT2002, Patras. 2002.
12. *Zykov S.V.* Human Resources Information Systems Improvement: Involving Financial Systems and Other Sources Data // ADBIS98, New York: Springer, 1998. PP. 351–356.

РАЗРАБОТКА ПЕРСОНАЛЬНОГО МЕЖСЕТЕВОГО ЭКРАНА С ВОЗМОЖНОСТЬЮ ШИФРОВАНИЯ СЕТЕВОГО ТРАФИКА

А.А. Станкевичус

МИФИ, г. Москва, kaf42@tephi.ru

В операционных системах Windows XP/2003 существует недостаток функций контроля сетевого доступа и обнаружения вторжений, что открывает их для различного рода атак. На данный момент существует ряд программно-аппаратных межсетевых экранов [1-2], позволяющих относительно надежно защитить сеть, но эти решения достаточно доро-

ги. Многие существующие на данный момент персональные межсетевые экраны для операционной системы Windows XP/2003 не позволяют выполнять фильтрацию на основе полей заголовка протокола IPX [1–3], что делает применение клиента для сетей Novell NetWare в операционной системе Windows небезопасным. Существует потребность в персональном межсетевом экране для операционной системы Windows, позволяющем выполнять фильтрацию трафика на основе полей заголовка протокола IPX.

Широкое распространение получили беспроводные сетевые технологии. Во многих сетях уже имеются беспроводные мосты и точки доступа для мобильных клиентов. При этом многие встроенные в сетевое оборудование средства обеспечения безопасности беспроводных сетей поддерживают иностранные криптографические стандарты (такие как WEP и WPA использующие алгоритм шифрования RC4), стойкость которых спорна [4–5]. На рынке ощущается нехватка в средствах беспроводной связи, реализующих защиту передаваемых данных при помощи отечественных криптографических алгоритмов.

Реализация систем фильтрации трафика и обнаружения вторжений возможна в виде персональной системы, обрабатывающей только трафик, предназначенный или исходящий только от ЭВМ, на которой она установлена, либо в виде «сетевой» системы, обрабатывающей весь трафик, проходящий по сегменту сети [6]. «Сетевые» системы способны обнаруживать больший процент атак, однако персональные системы требуют в несколько раз меньшего количества системных ресурсов и не требуют установки выделенного сервера, что резко снижает стоимость и тем самым повышает доступность решения.

Реализация систем защиты от сетевых атак возможна в виде «пассивной» системы обнаружения вторжений либо в виде «активной» системы предотвращения вторжений [7]. «Активная» система обеспечивает более высокий уровень защиты, но требует существенно большего количества системных ресурсов чем «пассивная». «Гибридные» системы, активно предотвращающие только часть сетевых атак, представляются в сложившихся условиях оптимальным выбором.

Автором данной статьи разработана система фильтрации и защиты сетевого трафика для ЭВМ под управлением операционной системы Windows XP и Windows 2003 Server. Разработанная система является персональным межсетевым экраном с «гибридной» системой обнаружения и предотвращения вторжений и возможностью шифрования сетевого трафика. Система позволяет обеспечить для каждой защищаемой ЭВМ безопасность входящего и исходящего трафика на всех закреплённых за ней сетевых интерфейсах, а так же обеспечить хорошо

масштабируемую архитектуру сети. Применение разработанной системы может привести к удешевлению и упрощению реализации и управления решением безопасности в корпоративной сети.

Ядро безопасности разработанной системы реализовано в виде NDIS-драйвера промежуточного уровня [8] и располагается между драйвером сетевой карты и стеком протоколов – ниже, чем защищаемые приложения. Это позволяет разработанной системе закрыть все неиспользуемые порты, ограничивая таким образом доступ к NT-приложениям и сервисам операционной системы. Разработанная система позволяет осуществлять фильтрацию по полям заголовков различных сетевых протоколов, в том числе IP и IPX, а так же шифрование трафика по алгоритму ГОСТ 28147-89.

Разработанный драйвер и компонент, выполняющий отображение журнала операций, включены в состав Персонального Центра Защиты, разрабатываемого в НТИЦ «Атлас».

ЛИТЕРАТУРА

1. *Межсетевой экран «Цитадель МЭ»*, версия 2.0. <http://www.atlasnsk.ru/VPN/citadel.shtml>
2. *Межсетевой экран ЗАСТАВА*. http://www.zastava.ru/zastava_firewall.shtml
3. *Персональный экран (ПЭ) «Блокпост – Экран 2000/XP»*. <http://www.altx.ru/ekran.html>
4. *Атаки на WEP*. <http://www.telcon.ru/articles/analytics/1292/>
5. *Vebjorn Moen, Havard Raddum, Kjell J.Hole*. Weaknesses in the Temporal Key Hash of WPA. 2005, Dept. of Informatics, Univ. of Bergen.
6. *Обнаружение атак, сетевой или системный уровень?* Руководство по выбору технологии обнаружения атак. <http://www.citforum.ru/security/internet/netsys/netsys.shtml>
7. *Системы защиты: фокус на комплексные решения*. http://www.citforum.ru/security/articles/sec_systems/
8. *Реализация защиты на уровне сетевого драйвера промежуточного уровня*. <http://predpinimatel-cd.com.ru/book/Programming/Book.PogrammingSistemSecurity/Glava%204/Index15.htm>

ИСПОЛЬЗОВАНИЕ ВЫХОДНЫХ ДНЕЙ ДЛЯ РЕГЛАМЕНТНЫХ РАБОТ В ЦЕНТРЕ СЕРТИФИКАЦИИ MICROSOFT

П.В. Смирнов

МИФИ, г. Москва, kaf42@merphi.ru

Использование специального расписания публикации списков отзыва сертификатов (COC, англ. CRL) позволяет выполнять обязательства Удостоверяющего Центра (УЦ) перед клиентами по периодически-

сти издания CRL в рабочее время, тогда как в выходные часы проводить техническое обслуживание аппаратного и программного обеспечения УЦ, в том числе с отключением электропитания или компьютерной сети. Предлагается реализация специального расписания публикации путем встраивания модуля выхода (exit module) в Microsoft CA.

Списки отзыва сертификатов являются самым распространенным методом предоставления клиентам информации о статусах сертификатов. Формат и применение СОС описаны в рекомендациях X.509 [1] и RFC 3280 [2], что обуславливает поддержку СОС во всех продуктах, работающих с сертификатами открытых ключей.

СОС представляет собой список серийных номеров сертификатов, которые уникальны для сертификатов одного УЦ, с указанным для каждого номера временем отзыва и, возможно, другими атрибутами. В СОС также указываются времена thisUpdate и nextUpdate. Первое поле определяет момент выпуска данного СОС, а второе поле задает время, не позже которого будет выпущен новый СОС с более свежей информацией. Для указания адреса, по которому доступен СОС, в сертификаты включается дополнение CDP (CRL Distribution Point – точка распространения СОС).

УЦ часто несет обязательства перед клиентами, что информация об аннулировании сертификатов публикуется не позднее определенного интервала, например, 1 часа с момента обращения клиента, с учетом рабочего времени. Перед администратором УЦ, использующего службу сертификации, входящую в состав операционных систем Windows 2000 Server и Windows Server 2003, встает задача правильной настройки параметров службы для выполнения этого обязательства.

В работе [3] представлен расчет необходимых настроек параметров службы для выполнения обязательств УЦ. Получена формула $T_{\max} = T_o - 2s - o$, где T_o – максимальная задержка публикации информации об изменении статуса сертификата с момента обращения клиента, $T_{\max}$ – период публикации, o – интервал перекрытия СОС, s – максимальное расхождение часов с клиентами.

Для осуществления регламентных работ на УЦ, в том числе с отключением электропитания или компьютерной сети, можно использовать выходные (нерабочие) часы. В этом случае необходимо обеспечить помимо регулярного выпуска СОС с фиксированным периодом еще и публикацию списков на нерабочее время. Время действия таких списков желательно продлить от конца рабочего времени до начала следующего периода рабочего времени, что обеспечит непрерывность работы всех клиентов УЦ при выполнении его обязательств по периодичности публикации СОС в рабочее время. При этом точка CDP должна быть расположена на другом физическом компьютере, который не отключается от сети.

Архитектура Центра сертификации Microsoft позволяет встроить так называемый модуль выхода (exit module), который, реализуя определенный интерфейс, будет получать сообщения обо всех событиях выпуска сертификатов и СОС на Центре. Такой модуль может использоваться для изменения алгоритма публикации СОС Центром.

Предлагаемый алгоритм работы модуля выхода позволяет решить описанную проблему. Модуль выхода имеет настройки, в которых задается расписание рабочего времени, т.е. какие часы в какие дни недели являются рабочими. Получив оповещение о выпуске нового СОС, модуль выхода определяет, происходит ли это в рабочее время. Если да, то такой список без изменения публикуется в CDP. Иначе, модуль изменяет время nextUpdate этого СОС, продлевая его до начала следующего рабочего периода, подписывает измененный список и публикует его в CDP.

Таким образом, после окончания рабочего периода, можно дожидаться очередной публикации СОС или осуществить внеочередную публикацию, что приведет к появлению пролонгированного списка в CDP, после чего можно отключать УЦ для проведения регламентных работ. Кроме этого, использование пролонгированного списка исключает возможность отказа ПО клиентов из-за недоступности СОС в случае выхода из строя УЦ в нерабочее время, когда на месте нет администратора.

ЛИТЕРАТУРА

1. ITU-T Recommendation X.509 «Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks». ITU-T. March 2000.
2. Housley, R., Polk, W., Ford, W., Solo, D. «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile». IETF, RFC 3280. April 2002. <http://www.ietf.org/rfc/rfc3280.txt>.
3. *Смирнов П.В.*, Расписание публикации CRL для Центра сертификации Microsoft // Сб. научных трудов конференции «Безопасность информационного пространства». Екатеринбург. 2005.

МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ КЛИЕНТОВ ПРИ ДОСТУПЕ К ИНФОРМАЦИИ В ОБЪЕКТНЫХ СЕТЯХ ХРАНЕНИЯ ДАННЫХ

И.Л. Алферов

МИФИ, г. Москва, igor@alferov.net

Традиционно для хранения больших массивов данных применяют две широко распространенные архитектуры: сети хранения данных (СХД, англ. Storage Area Networks) и сетевые хранилища данных (Net-

work Attached Storage). Эти архитектуры обладают некоторыми недостатками, сужающими область их возможного практического применения. В частности, большинство реализаций СХД не обеспечивает полноценный разделяемый доступ к данным, а предполагает самостоятельную координацию доступа клиентскими приложениями. Сетевые хранилища в свою очередь обладают ограниченной масштабируемостью, так как доступ клиентов к данным осуществляется не непосредственно, а через специальные выделенные файл-серверы. В обеих архитектурах также используется блочный интерфейс работы с данными, не позволяющий реализовать эффективную модель безопасности. Это связано с тем, что управление доступом на уровне блоков требует чрезмерных затрат ресурсов, а на уровне логических разделов или устройств хранения данных – не обладает достаточной гибкостью. Блочный интерфейс также снижает интероперабельность клиентских приложений и эффективность хранения данных, так как все алгоритмы управления дисковым пространством реализуются на клиентской стороне и могут существенно варьироваться в различных приложениях.

Для преодоления упомянутых недостатков относительно недавно была предложена архитектура объектного хранения данных OSA [1,2]. Основная концепция, лежащая в основе этой архитектуры, заключается в хранении совокупности данных и метаданных в виде объектов. Объект является абстрактной сущностью и может представлять собой файл, запись базы данных или целую файловую систему. При этом функции управления дисковым пространством, синхронизации доступа и интеллектуального эширования выполняются самими устройствами хранения данных в зависимости от типов и атрибутов хранимых объектов. Одним из важнейших преимуществ данного подхода является возможность организации масштабируемого разделяемого доступа к информации с контролем на уровне объектов.

Так как технология объектного хранения данных является развивающейся, проблемам безопасности в объектных СХД до последнего времени уделялось мало внимания. Самым значительным событием стало принятие в 2004 г. стандарта ANSI, расширяющего интерфейс SCSI для взаимодействия с объектными устройствами хранения данных (OSD). В нем определена модель безопасности для объектных СХД, основанная на классической мандатной схеме. В рамках этой модели для доступа к некоторому объекту, хранящемуся в сети, клиент должен получить специальное криптографически защищенное удостоверение от доверенной третьей стороны, роль которой играет выделенный сетевой узел – менеджер безопасности. Удостоверение позволяет устройству хранения данных установить подлинность обратившегося клиента и проверить его права доступа к искомому объекту.

Анализ предложенного в стандарте подхода к аутентификации клиентов при доступе к информационным объектам позволяет выявить по крайней мере следующие его недостатки:

- отсутствие фиксированного механизма получения удостоверений от менеджера безопасности;
- отсутствие формального доказательства криптографических свойств протокола аутентификации;
- потребность в частых взаимодействиях между клиентами и менеджером безопасности для получения удостоверений, приводящая к наличию в сети единой точки отказа;
- отсутствие поддержки защищенных соединений между клиентами и устройствами хранения данных для передачи данных с обеспечением конфиденциальности и целостности;
- ориентированность на дискреционную модель управления доступом, требующую повышенных затрат ресурсов на сопровождение политики безопасности.

С целью устранения этих недостатков предлагается использовать альтернативный протокол аутентификации клиентов при доступе к информации в объектных СХД.

Сообщения протокола:

- (1) $A \rightarrow T: I_A, I_B, N_{A_1}$
- (2) $A \leftarrow T: E_{K_{AT}}(N_{A_1}, idKey_{AB}, roleList, L, I_B)$
- (3) $A \leftarrow B: N_B$
- (4) $A \rightarrow B: I_A, roleList, L, activeRoleList, E_{roleKey_{AB}}(I_A, N_B, N_{A_2}, k_A)$
- (5) $A \leftarrow B: E_{roleKey_{AB}}(N_{A_2}, k_B)$

Здесь:

$$idKey_{AB} =_{def} MAC_{K_{BT}}(I_A, H(roleList), L)$$

$$roleKey_{AB} =_{def} MAC_{idKey_{AB}}(activeRoleList)$$

$$k =_{def} f(k_A, k_B)$$

Обозначения: A – клиент СХД, B – устройство хранения данных, T – менеджер безопасности, $idKey_{AB}$ – личный ключ A для взаимодействия с B , $roleKey_{AB}$ – ролевой ключ A для взаимодействия с B , $roleList$ – полный список ролей A , $activeRoleList$ – список активируемых в сеансе ролей A , L – номер версии личного ключа $idKey_{AB}$, K_{AT} – общий секретный ключ A и T , K_{BT} – общий секретный ключ B и T , N – случайные числа, H – хэш-функция с трудно обнаружимыми коллизиями, k – сеансовый ключ защищенного соединения между A и B .

Протокол ориентирован на использование ролевой модели управления доступом и заключается в последовательном обмене клиента с доверенной третьей стороной – менеджером безопасности и устройством хранения данных. Клиент получает у менеджера безопасности личный ключ и вырабатывает из него ролевой ключ для установления защищенного сеанса связи с устройством хранения данных. Использование ролевых ключей позволяет распределить функции управления политикой безопасности между менеджером безопасности и устройствами хранения данных таким образом, что сеть может продолжать корректно функционировать в случае временной неработоспособности менеджера. Если клиент располагает действующим личным ключом, ему не требуется выполнять обмен сообщениями (1), (2) с менеджером безопасности.

В результате выполнения протокола клиент и устройство взаимно аутентифицируются и разделяют общий сеансовый ключ для установления защищенного соединения. При этом устройство хранения данных получает достоверную информацию о наборе активируемых в сеансе ролей пользователя. Эти свойства протокола формально доказаны на основе предположений о начальных областях доверия участников с использованием BAN-логики. Если для часов участников протокола обеспечивается защищенная синхронизация, то количество сообщений в протоколе может быть сокращено до четырех за счет использования метки времени вместо случайного числа N_B .

В настоящее время технология объектного хранения данных развивается стремительными темпами, и рассмотренный альтернативный механизм аутентификации клиентов может использоваться при разработке новых стандартов в области безопасности объектных СХД.

ЛИТЕРАТУРА

1. ANSI INCITS 400-2004 – Information Technology – SCSI Object-Based Storage Device Commands (OSD), Dec. 2004.
2. *Factor M., Nagle D., Naor D., Riedel E., Satran J.* The OSD Security Protocol // Proc. of the 3rd IEEE International Security In Storage Workshop, Dec. 2005.

К ВОПРОСУ О МОДЕЛИРОВАНИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

С.А. Чернокозинский

Москва, МИФИ, sa.chern@gmail.com

Процессы создания, модернизации и исследования защищенных систем обработки информации предполагают применение моделей, описывающих существенные стороны данного предмета. При создании

систем и процессов защиты информации используются различные классы моделей [1], применяемые на различных стадиях моделирования и представляющие собой взаимосвязанную систему с единым методологическим базисом.

Сложность определения и формализации параметров моделей в области информационной безопасности связана с неполнотой данных и отсутствием статистической информации о значениях параметров элементов моделей или размытостью их оценок. Указанные особенности не позволяют в полной мере воспользоваться строгими аналитическими моделями [2].

В качестве перспективного подхода к моделированию систем и процессов обеспечения безопасности информации предлагается использование объектно-ориентированного моделирования (ООМ). Весь процесс ООМ предлагается разбить на два основных этапа: функциональное моделирование объекта защиты и непосредственное моделирование системы защиты.

Для построения моделей анализа функциональной составляющей объекта защиты предлагается применить методологию SADT (IDEF0) [3] или язык моделирования UML [4]. За счет гибкости UML, и понятий «цель» и «точка зрения» в SADT/IDEF0, данные методологии позволяют строить функциональную модель объекта с учетом аспекта защиты информации. При этом, диаграмма Эриксона-Пенкера языка UML предоставляет возможность использования SADT (IDEF0) и UML в качестве двух взаимозаменяющих друг друга аппаратов моделирования.

Несмотря на очевидные достоинства методологии SADT (IDEF0) и языка UML для функционального моделирования, таких как: удобство использования; графическое представление модели; применимость на разных стадиях создания системы; возможность строить масштабируемые и расширяемые модели системы, они обладают и рядом существенных недостатков. Главными из этих недостатков являются отсутствие возможности реализации условий на запуск входов и выходов компонентов моделей и невозможность моделирования динамических процессов, что важно при моделировании систем защиты информации.

Поэтому, для реализации второго этапа объектно-ориентированного моделирования предлагается использовать аппарат сетей Петри, который не диктует какого-либо специфического метода и предоставляет гибкий инструмент для моделирования [5], в том числе систем и процессов защиты информации.

Для выработки единой методики моделирования была разработана схема перехода от модели, построенной по методологии SADT (IDEF0) или UML к модели в терминах сетей Петри. В рамках данной схемы

функциональные блоки SADT-диаграммы и блоки диаграмм Эриксона-Пенкера языка UML, а также соответствующие им информационные потоки преобразуются в «переходы», «места» и ориентированные дуги сети Петри.

Построенная таким образом сеть Петри позволяет моделировать процесс защиты информации и впоследствии может анализироваться уже апробированными на практике методами [6].

ЛИТЕРАТУРА

1. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МИФИ, 1997.
2. В.А.Петров «О методологии построения моделей анализа систем и процессов защиты информации», МИФИ, 1997
3. Дэвид Л., МакГоуэн К., МакГоуэн М. Методология структурного анализа и проектирования. М: МетаТехнология, 1993
4. Ovidiu Noran. Business Modeling UML, IDEF. School of computing and information technology. Griffith University
5. Jensen, K., Coloured Petri Nets, 3 volumes, EATCS Monographs on Theoretical Computer Science, 1992, 1995, 1998, Springer-Verlag
6. Питерсон Дж. Теория сетей Петри и моделирование систем: Пер. с англ. М.: Мир, 1984. 264 с.

ДОЛГОВРЕМЕННОЕ ОБЕСПЕЧЕНИЕ ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

А.М. Бондарь, А.О. Меньшенин
МИФИ, г. Москва, kaf42@tephi.ru

В работе рассматривается проблема долговременного обеспечения подлинности электронных документов, заверенных ЭЦП, и предлагается архитектура долговременного архива, основанная на технологии «продления ЭЦП».

В настоящее время электронная цифровая подпись (ЭЦП) находит все большее применение в различных областях электронных взаимодействий. Действующее законодательство РФ, несмотря на существенные недостатки, предоставляет нормативно-правовую базу для использования ЭЦП, приравнивая ее юридическую значимость к значимости собственноручной подписи документа на бумажном носителе. В действительности, при соблюдении базовых принципов построения инфраструктур открытых ключей [1, 2] и требований по безопасному управлению ключевым материалом, ЭЦП является эффективным механизмом обеспечения целостности (и подлинности) электронных документов в оперативной работе.

Однако в случае заверения ЭЦП электронных документов, имеющих длительный срок хранения и/или использования, возникают серьезные проблемы [3]. Устаревание информационных технологий, уменьшение стойкости криптографических алгоритмов (и, как следствие, ограничение периода использования ключевого материала), а также программно-аппаратные ошибки приводят к тому, что действительность ЭЦП не может быть гарантирована спустя длительный промежуток времени. Тем не менее, в практике функционирования информационных систем нередко возникают ситуации, в которых для разрешения конфликтов требуется подтвердить подлинность документа на определенный момент времени в прошлом. Для разрешения таких ситуаций необходимо обеспечить долговременное хранение документов, заверенных ЭЦП, с целью обеспечения их подлинности в течение длительного промежутка времени.

Существует два основных подхода к решению данной задачи. Первый подход основан на применении специальных электронных архивов, обеспечивающих надежное долговременное хранение данных и невозможность их изменения в процессе хранения. ЭЦП проверяется перед помещением данных в архив, после чего документ помещается в архив уже без ЭЦП. Таким образом, долговременная подлинность документов в данном случае обеспечивается «доверием» к тому, что документ был действителен на момент помещения в архив и не был изменен при хранении. Такой подход, в основном, может быть использован при организации больших архивов электронных документов (например, государственных) ввиду высокой сложности и стоимости реализации.

Второй подход основан на продлении ЭЦП при хранении документов в долговременном архиве [4, 5]. Данный подход может быть применен для построения архивов, обеспечивающих подлинность электронных документов в течение сравнительно небольшого промежутка времени (до 10-15 лет).

В работе рассматривается обобщенная архитектура долговременного архива документов с ЭЦП, построенная на основе второго подхода. При построении архива используются усовершенствованные протоколы и форматы данных [6], предложенные рабочей группой IETF LTANS (Long-term Archive And Notary Service). Предложенная архитектура носит общий характер и может быть использована в различных информационных системах. На основании данной архитектуры, в частности, предлагается построить долговременный архив электронных отчетов в системе централизованного сбора, обработки и хранения информации «Аспирантура-Центр» в ВАК России.

Таким образом, долговременное обеспечение подлинности электронных документов в настоящий момент является достаточно актуальной проблемой, полноценного решения которой нет как в России, так и за рубежом. Предложенная архитектура долговременного архива электронных документов, заверенных ЭЦП, может быть с некоторыми ограничениями использована для решения данной проблемы.

ЛИТЕРАТУРА

1. *ITU-T Recommendation X.509 – Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*. March 2000.
2. *Технология PKI и ее реализация на платформе Microsoft .NET*. Учебный Центр безопасности информационных технологий Microsoft МИФИ, 2004.
3. *Храмцовская Н.А.* Проблемы долговременного хранения документов, подписанных электронно-цифровой подписью или ее аналогами. Делопроизводство и документооборот на предприятии, N 7, июль 2005 г.
4. Evidence Record Syntax (ERS), LTANS, Internet Draft, <<http://www.ietf.org/internet-drafts/draft-ietf-ltans-ers-02.txt>>, 2005.
5. Long-Term Archive Architecture, <<http://ltans.edelweb.fr/draft-ietf-ltans-arch-00.pdf>>, November 2003.
6. Internet-Draft – Long-term Archive Protocol (LTAP), <<http://ltans.edelweb.fr/draft-ietf-ltans-ltap-00.html>>, 2005.

ЦИФРОВАЯ СИСТЕМА СВЯЗИ, ОСНОВАННАЯ НА ПРОГРАММНОЙ МАНИПУЛЯЦИИ ТОКОМ ПОТРЕБЛЕНИЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

Р.Ю. Гаврильченко, Н.П. Лаврентьев

МИФИ, г. Москва, kaf42@merphi.ru

В данной работе исследуется возможность создания системы связи, используя программное манипулирование током потребления персонального компьютера. Нами был собран макет, реализующий такую систему связи, на котором была осуществлена односторонняя безошибочная передача текстового сообщения со скоростью 10 бод.

Идея создания такой системы связи возникла не случайно. На сегодняшний день все современные персональные компьютеры (ПК) снабжены программно-аппаратными средствами управления энергопотреблением. Все больше физических процессов в ПК происходит под контролем программных средств. К ним относятся: температура узлов, скорость вращения охлаждающих вентиляторов, уровень шума жестких дисков, уровень напряжений питания и уровень энергопотребления [1]. Последний объясняется тем, что современный уровень вычисли-

тельной мощности компьютеров и связанной с ней потребляемой мощности заставляет задуматься производителей об экономии электроэнергии. Программное управление энергопотреблением является необходимым этапом в развитии персональной вычислительной техники и насчитывает уже не один десяток лет [2]. С другой стороны, программная манипуляция энергопотреблением дает возможность воздействием на такой параметр, как электрический ток потребления ПК, сформировать сигнал в электросети. Этот сигнал может быть принят удаленно другим компьютером, имеющим специальное программно-аппаратное обеспечение.

Такая система связи является *односторонней*. Кроме того, частота манипуляции не может превышать удвоенной частоты напряжения в электросети, что ограничивает скорость передачи дискретного сигнала до *единиц бод*. Поэтому область применения такой системы весьма ограничена и специфична.

Однако привлечение внимания к возможности реализации такой системы связи важно по двум причинам. Во-первых, такая система может быть использована как *средство защиты* информации, например, в системах скрытого контроля доступа к компьютерам, во-вторых же, она может быть использована как *канал утечки* защищенной информации и указывает на уязвимость современных персональных компьютеров.

Нами был собран макет и разработано специальное программное обеспечение, реализующие такую систему связи. Макет состоял из двух персональных компьютеров с процессорами Pentium III 1000 МГц. На одном из них, названном условно «компьютер-передатчик», запускается программа – «программа-передатчик». В окне этой программы вводится тестовое сообщение. Затем по команде от пользователя программа начинает изменять ток потребления манипулируемого устройства в соответствии с изменением информационного сигнала в сообщении. В результате этого, через блок питания меняется и общий ток потребления всего компьютера. Эти колебания тока, посредством магнитного поля вокруг электропроводки, улавливаются расположенной рядом с ней магнитной антенной. Магнитная антенна преобразует изменение магнитного поля в Э.Д.С. индукции. Далее этот сигнал поступает на микрофонный вход звуковой карты, которая находится на втором компьютере, названном условно «компьютер-приемник». На этом компьютере запущена другая программа, названная условно «программа-приемник». Она считывает данные сигнала со звуковой карты и декодирует их в исходное тестовое сообщение.

В ходе эксперимента на собранном макете была осуществлена односторонняя безошибочная передача текстового сообщения со скоростью 10 бод.

В докладе не приводятся методы реализации такого канала, поэтому он не может служить руководством по его созданию, а лишь доказывается возможность его реализации. Все используемые в докладе сведения являются свободно доступными и общеизвестными.

ЛИТЕРАТУРА

1. Гуж М. Аппаратные средства IBM PC. Энциклопедия, 2-е изд. СПб.: Питер 2003.928 с.
2. «ACPI, OnNow и Instantly Available PC» www.itc.ua/article.phtml?ID=7308.

МОДЕЛИРОВАНИЕ РЕЧЕВОГО СИГНАЛА СУПЕРПОЗИЦИЕЙ ВЕЙВЛЕТОВ МОРЛЕ В ЗАДАЧАХ ЕГО ЗАЩИТЫ

А.М. Гилев

МИФИ, г. Москва, kaf42@mephi.ru

Использование более адекватных моделей речевых сигналов позволяет легче решать различные задачи обеспечения безопасности речевой информации. Описывается одна из таких перспективных моделей.

В задачах обеспечения безопасности речевой информации используются различные модели речевых сигналов. Применение более эффективных моделей позволяет повысить защищенность этой информации, улучшить качество связи и уменьшить количество требуемых вычислительных ресурсов. Кроме этого, это позволяет более эффективно решать задачи образного анализа речевой информации для оценки качества ее защиты, задачи адаптивного активного гашения помех, задачи асинхронного маскирования речевого сигнала и другие подобные задачи.

В последнее время очень активно развивается технология непрерывного вейвлет-анализа [1]. Появились многочисленные публикации по применению вейвлет-преобразований в системах сжатия, обработки и информационного анализа различного рода сигналов и изображений.

Для того чтобы некоторая функция могла называться вейвлетом, она должна удовлетворять следующим условиям:

1. Ее среднее значение на интервале определения должно быть равно нулю.
2. Функция должна быстро убывать при стремлении аргумента к бесконечности (то есть, она должна быть «быть локализована во временной области»).
3. Спектр функции должен быть сосредоточен в относительно узкой полосе частот (то есть, она должна «быть локализована в частотной области»).

В докладе рассматривается представление речевого сигнала в виде суперпозиции вейвлетов Морле. Последний представляет собой комплексную гармонику, взвешенную колоколообразным окном Гаусса. Таким образом речевой сигнал представляется в виде суммы узкополосных по Гильберту составляющих [2]:

$$s(t) = \sum_i^k A_i \cdot \exp\left(-\frac{t^2}{2\sigma_i^2}\right) \cdot \cos(\omega_i t + \varphi_i)$$

Тем не менее, для того, чтобы можно было эффективно применять описанную модель, требуется решить задачу быстрого разложения речевого сигнала на приведенную выше суперпозицию вейвлетов. В докладе рассматриваются возможные пути решения этой задачи.

ЛИТЕРАТУРА

1. *Воробьев В.И., Грибунин В.Г.* Теория и практика вейвлет-преобразования. С.-Петербург, Новые информационные технологии, 1999.
2. *Дворянкин С.В.* Речевая подпись. Москва, МТУСИ, 2003.

ПОСТРОЕНИЕ СИСТЕМЫ МОБИЛЬНОГО БЕЗОПАСНОГО ДОСТУПА К ИНФОРМАЦИИ НА БАЗЕ JAVA ME

М.В. Дубовицкая

МИФИ, г. Москва, kaf42@mephi.ru

Целью данной работы является рассмотрение проблемы защиты информации в мобильных системах и разработка системы безопасного доступа к данным для мобильных приложений. Такая система позволит расширить возможности по применению мобильных устройств и снизить риск утечки информации при их использовании.

В настоящее время мобильные телефоны, карманные компьютеры, смартфоны, коммуникаторы, и другие так называемые «цифровые гаджеты» являются неотъемлемой частью нашей повседневной жизни. Компактность и мобильность данных устройств наряду с достаточно большими техническими возможностями позволяют использовать их в корпоративных решениях и проектах многих компаний для увеличения прибыли. Однако, несмотря на то, что эти миниатюрные устройства приносят пользу компании, масштабируя проекты и в значительной мере облегчая жизнь ее сотрудникам, нельзя забывать, что они могут являться источниками уязвимостей действующей системы, давая возможность злоумышленнику нанести вред компании.

Технология Java2ME позволяет создавать кроссплатформенные, легко переносимые бизнес-приложения для мобильных устройств. В

большинстве случаев это клиент-серверные приложения. Вся основная работа выполняется сервером – к нему нужно обеспечить мобильный доступ, причем только авторизованных пользователей. [1] Также мобильный телефон или КПК сотрудника может содержать электронную почту, в том числе и конфиденциальную, различные корпоративные документы, интеллектуальную собственность компании, информацию, которую можно использовать для взлома и проникновения в корпоративную сеть. Поэтому нельзя допустить возможность утечки информации с портативного устройства сотрудника.

Спектр возможных уязвимостей информации при использовании цифровых гаджетов, к сожалению, достаточно широк. Во-первых, миниатюрность телефонов одновременно увеличивает риск их потери или кражи. Во-вторых, перехват трафика при использовании GPRS – сетей и пересылки SMS становится для мобильных устройств не меньшей проблемой, чем в стандартных сетях. Наконец, в-третьих, синхронизация при передаче данных с мобильного устройства, возможность скопировать с SIM-карты и из памяти телефона информацию позволяют получить доступ практически ко всем данным в мобильном устройстве [2].

Не смотря на эти угрозы, защита в мобильном телефоне порой ограничивается лишь наличием четырехзначного PIN-кода, а иногда отключается и это.

Использование паролей, привязка приложения к определенному аппарату или SIM-карте и прозрачное шифрование являются ключевыми моментами в обеспечении безопасности информации в мобильных приложениях. [3]

Однако, длинные пароли сложны для запоминания, хранение же паролей в телефоне увеличивает риск несанкционированного доступа. Маломощный процессор не позволяет полноценно использовать криптографию с открытым ключом, так как необходимые для генерации ключей и проверки подписи вычисления требуют значительных временных затрат, что неудобно при доступе к данным или безопасном соединении с сервером. В этом случае пользователь вынужден проводить несколько минут в ожидании выполнения необходимых вычислений [4, 5] .

Таким образом, построение надежной, удобной, а главное быстрой системы защиты для мобильных приложений является актуальной и сложной задачей. Ее решение позволит расширить возможности по применению мобильных устройств и снизит риск утечки информации при их использовании.

ЛИТЕРАТУРА

1. «MIDP Application Security 3: Authentication in MIDP» by Jonathan Knudsen December, 2002.

2. «*Maximum Security, Optimum Usability Version 1.0*»; April, 2005.
forum.nokia.com
3. «*MIDP Application Security 4: Encryption in MIDP*» by Jonathan Knudsen, September, 2005.
4. «*Data security in mobile Java applications*» by Michael Juntao Yuan, December, 2002.
5. «*Mobile Security Starts To Grow Up*» by Steve Wallace, October, 2004

ПОСТРОЕНИЕ И ПРОВЕРКА ПУТЕЙ СЕРТИФИКАЦИИ В ИНФРАСТРУКТУРАХ ОТКРЫТЫХ КЛЮЧЕЙ

В.Ю. Липовецкий

МИФИ, г. Москва, kaf42@mephi.ru

В работе рассмотрены практические и теоретические аспекты построения и проверки путей сертификации в инфраструктурах открытых ключей. Предложен алгоритм одновременного построения и проверки путей сертификации. Разработан и испытан программный комплекс построения и проверки путей сертификации.

В работе рассматриваются практические и теоретические аспекты построения и проверки путей сертификации в инфраструктурах открытых ключей (ИОК). Одна из основных проблем практического применения асимметричной криптографии – обеспечение доверия к открытому ключевому материалу, хранящемуся в общедоступных источниках. Сегодня данная задача решается построением инфраструктур открытых ключей – сетей доверия, основанных на издании особых электронных документов – сертификатов открытых ключей [1, 2].

Построение и проверка путей сертификации – процесс, позволяющий определить применимость сертификата, полученного из удаленного источника, для определенных целей [3]. Опыт российских и зарубежных компаний говорит о том, что наиболее актуальными проблемами, связанными с построением и проверкой путей сертификации, на сегодняшний день являются:

1. разработка универсального алгоритма построения и проверки путей сертификации;
2. разработка программного комплекса построения и проверки путей сертификации, способного работать в сложной разнородной среде;

Для решения поставленных задач в работе используются методы теории графов, теории автоматов, технологии объектно-ориентированного программирования.

Существующие в рамках теории графов подходы и алгоритмы можно считать базисными по отношению к математическим методам, разрабатываемым в данной работе[4][5]. Предлагаемый в данной работе алгоритм параллельного поиска и проверки путей сертификации (АППиППС) основан на абстрактных алгоритмах поиска в ширину и в глубину.

Использование современных технологий программирования – основа для создания эффективного программного комплекса, способного работать в разнородной среде. Объектно-ориентированный подход позволяет строить программный комплекс модульно. Модули, имеющие строго оговоренные интерфейсы, могут быть использованы в том числе в других продуктах.

В данной работе удалось добиться следующих результатов

1. Предложена теоретико-графовая модель ИОК.
2. Предложены критерии эффективности алгоритма построения и проверки путей сертификации.
3. Разработан универсальный многопоточный алгоритм построения и проверки путей
4. Разработан программный комплекс построения и проверки путей сертификации для семейства операционных систем семейства MS Windows. Построены стенды для испытания средств построения и проверки путей сертификации, на которых испытан разработанный продукт.

Практическая значимость данной работы в России станет очевидной в ближайшие несколько лет, когда начнется широкомасштабное внедрение ИОК в промышленности и административной сфере.

Экономическую выгоду результатов данной работы пока трудно оценить, однако можно предполагать, что внедрение разработанных подходов и программного обеспечения позволит существенно упростить межорганизационное электронное защищенное взаимодействие.

ЛИТЕРАТУРА

1. *ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection -The Directory: Public-key and Attribute Certificate Frameworks*, March 2000.
2. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. М.: Горячая линия –Телеком, 2004. 248 с.
3. Cooper M., Dzambasow Y., Hesse P., Joseph S., Nicholas R. «Internet X.509 Public Key Infrastructure Certification Path Building», December 2003.
<http://www.ietf.org/internet-drafts/draft-ietf-pkix-certpathbuild-03.txt>
4. Т. Корчмен, Ч. Лейзерсон, Р. Ривест. Алгоритмы: построение и анализ. ЦПНМО, 2001.
5. Shasha, D., T.L. Wang, J., Guigno., R. Algorithmics and Applications of tree and Graph Searching. 2002.
<<http://web.njit.edu/~jason/publications/ARTICLES/pods2002.ps>>

РАЗРАБОТКА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ВЗАИМОДЕЙСТВИЯ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ С УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

*А.И. Лучник, А.О. Меньшенин
МИФИ, г. Москва, kaf42@merphi.ru*

В работе проводится анализ особенностей функционирования УЦ МИФИ, как корпоративной системы и обзор существующих УЦ. На основании этого анализа выработаны требования к системе взаимодействия конечного пользователя с удостоверяющим центром. Практическая часть работы заключается в реализации этой системы в виде набора сценариев, написанных на интерпретируемых языках высокого уровня X-Parser и JavaScript для взаимодействия с RSA Keon CA 6.5.1.

Повсеместное использование ЭВМ ведет к увеличению информации, хранящейся и обрабатываемой в цифровом виде. Кроме того, использование сети Интернет в учебном процессе становится инициативой не только отдельных преподавателей, но уже предпринимаются попытки создать централизованную систему для ведения электронной переписки студентов и преподавателей, обмена материалами и даже интерактивного тестирования.

Эти тенденции отразились и в электронной сфере деятельности МИФИ. На данный момент введена в эксплуатацию новая централизованная Служба электронной почты МИФИ (СЭП МИФИ) [1]. Также на сайте www.pkilab.ru лаборатории «Инфраструктура открытых ключей» (ИОК), созданной на базе кафедры №42, планируется создать обширную электронную библиотеку посвященную PKI. В библиотеке предполагается разместить рефераты, написанные студентами при прохождении курса «ИОК», а так же дополнительные статьи по теме. Кроме основного функционала, требуется обеспечить безопасность этих служб, например, осуществить разграничение доступа к материалам сайта и реализовать возможность аутентификации сообщений, передаваемых с использованием СЭП.

Для решения этих и других задач, связанных с обеспечением информационной безопасности целесообразно применение асимметричной криптографии. Несмотря на то, что математические основы криптографии с открытым ключом достаточно хорошо исследованы, при практическом ее применении возникает необходимость решения ряда серьезных задач, связанных с управлением ключами. Для решения этих задач, служит ИОК. Сертификат открытого ключа является центральным понятием ИОК. Он связывает открытый ключ с информацией о его владельце. Все это, подписывается при помощи секретного ключа удостоверяющего центра (УЦ). В соответствии с Федеральным законом

об электронной цифровой подписи (ЭЦП) [2], необходимо создавать и сертифицировать УЦ для того, что бы иметь возможность проверки ЭЦП. Поэтому очевидна необходимость создания УЦ МИФИ, с возможностью его последующей интеграции в систему удостоверяющих центров Министерства образования и науки РФ, с целью обеспечения защиты электронного документооборота в интегрированной автоматизированной информационной системе сферы образования.

На базе лаборатории «ИОК» создан УЦ с использованием программного обеспечения RSA Keon CA 5.6.1 [3]. Данное программное обеспечение служит для создания и обеспечения функционирования центров сертификации. При этом функции центра регистрации требуется реализовывать дополнительно с использованием предоставляемых RSA Keon CA 5.6.1 возможностей.

В работе был проведен анализ особенностей МИФИ как корпоративной системы. В связи с этими особенностями были выдвинуты требования к УЦ МИФИ и к характеристикам интерфейса взаимодействия конечных пользователей с УЦ. На данный момент существует ряд крупных УЦ [4-6], которые выдают сертификаты по всему миру и обладают обширными функциональными возможностями, но такие решения дороги и не позволяют гибко решать существующие задачи.

Практическая часть работы заключалась в разработке логической архитектуры УЦ и повышении уровня его безопасности за счет выноса набора функций в отдельный модуль – центр регистрации. Так же был создан веб-интерфейс УЦ МИФИ, и была произведена интеграции его с сайтом лаборатории ИОК. Был создан набор сценариев, позволяющий осуществлять формирование и отправку запроса нового сертификата, поиск сертификатов среди уже изданных, просмотр их статуса и параметров.

В ходе дальнейшей работы планируется расширить функциональность интерфейса, для предоставления более гибких возможностей конечным пользователям, а так же расширить функциональность самого УЦ с помощью использования схем ЭЦП со специальными свойствами.

ЛИТЕРАТУРА

1. *Информация о СЭП МИФИ* <http://www.mephi.ru>
2. *Федеральный закон об электронной цифровой подписи*
3. *RSA Keon Certificate Authority 6.5 Administrator's Guide.*
4. *Информация об удостоверяющем центре Verisign* <http://www.verisign.com>.
5. *Идентификационный код VeriSign*
<http://www.microsoft.com/rus/winlogo/software/verisign.mspx>.
6. *Информация об удостоверяющем центре Thawte* <http://www.thawte.com/>
7. *Molly E. Holzschlag. HTML and CSS. Addison Wesley Professional, 2005.*
8. *Powell T., Schneider F. JavaScript 2.0: The Complete Reference, Second Edition. McGraw-Hill/Osborne, 2004*

ПОСТРОЕНИЕ РАСПРЕДЕЛЕННЫХ СИСТЕМ БЕЗОПАСНОСТИ НА БАЗЕ АГЕНТНЫХ ПЛАТФОРМ

А.А. Любко

МИФИ, г. Москва, kaf42@merphi.ru

При построении системы безопасности для корпоративных сетей одной из основных задач является задача обеспечения комплексности и надежности системы защиты. Комплексность системы защиты часто подразумевает интеграцию различных механизмов защиты в единую систему. Кроме того, вся система безопасности должна соответствовать развивающейся инфраструктуре предприятия, не снижать производительности работников и быть масштабируемой.

Современные корпоративные сети постоянно усложняются, что приводит к проблемам с управлением и настройкой, как самих сетей, так и систем безопасности. Кроме того, наличие мобильных пользователей приводит к проблемам построения периметра безопасности и управления системами защиты мобильных пользователей.

Для построения защиты систем со сложной архитектурой, нечеткими периметрами и мобильными пользователями удобно использовать политики безопасности. Фактически построение системы защиты основывается не на архитектуре самой системы, а на определении политики безопасности для пользователей, компьютеров и других объектов системы[1]. Данный подход позволяет решить проблемы с управляемостью подобных систем, но он не обеспечивает простоту установки и расширения систем. При добавлении новых пользователей или компьютеров, для управления политиками безопасности необходимо первоначально устанавливать программное обеспечение, которое может управляться посредством политик безопасности. Кроме того, при нарушении работоспособности программного обеспечения, администратор должен самостоятельно восстанавливать или переустанавливать его. Проблема стоит особенно остро, при распространении нового программного обеспечения системы безопасности при наличии в системе мобильных пользователей.

Для решения данных проблем удобным является применение агентных платформ [2] в качестве базовой среды функционирования системы безопасности.

Агентные платформы представляют один из способов построения распределенных систем и позволяют описать и предоставить доступ всех приложений, работающих на агентной платформе к необходимым им сервисам. Кроме того, одной из функций агентной платформы является распределение агентов, аудит их функционирования и управление ими[3, 4].

При построении систем защиты на базе агентных платформ появляется возможность использовать все положительные стороны агентной архитектуры и разрешить часть проблем современных систем безопасности.

Для построения системы безопасности на базе агентной платформы все компоненты системы безопасности необходимо представить в виде сервисов и агентов платформы. Язык общения агентов стандартизирован[3], что обеспечит бесшовную интеграцию компонент системы. Интеграция новых механизмов защиты также не составит труда. Для этих целей достаточно ввести новые сервисы и агенты в систему. Построение систем безопасности на базе агентных платформ позволяет организовать управление жизненным циклом программного обеспечения, входящего в состав платформы[5].

Таким образом используя политики безопасности для управления настройками, правилами функционирования и взаимодействия объектов системы безопасности и агентную платформу в качестве базовой платформы управления жизненным циклом объектов системы возможно построить расширяемую, управляемую и отказоустойчивую систему безопасности.

ЛИТЕРАТУРА

1. *Distributed Policy-based Management*, Mads Dam, Gunnar Karlsson, Babak Sadighi Firozabadi2 и Rolf Stadler
2. *Agent Technology Glossary*
<http://www.objs.com/agility/tech-reports/9909-agent-glossary.html>
3. *An Agent Platform for Reliable Asynchronous Distributed Programming*, L. Bellissard, INRIA Rhône-Alpes, N. de Palma, INRIA Rhône-Alpes, A. Freyssinet, INRIA Rhône-Alpes, M. Herrmann, INRIA Rhône-Alpes, S. Lacourte, INRIA Rhône-Alpes, 18th IEEE Symposium on Reliable Distributed Systems
4. *A FIPA Compliant Agent Platform for Federated Information Systems*, M. Panti, L. Penserini, L. Spalazzi and S. Valenti, Computer Science Department – University of Ancona.
5. *Developing Secure Agent Systems Using Delegation Based Trust Management*, Lalana Kagal, , Tim Finin, Anupam Joshi, University of Maryland

ФОРМАТ СИГНАТУРЫ ДЛЯ ВЫЯВЛЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ И КОРРЕКТНОЙ РЕАКЦИИ НА НИХ

А.А. Матрочов

МИФИ, г. Москва, kaf42@mephi.ru

Целью данной работы является рассмотрение проблемы разработки формата сигнатур, который позволял бы корректно реагировать на

событие системы обнаружения вторжения в реальном времени. Такой подход, повышает скорость обработки событий в системе обнаружения вторжений, и предоставляет возможность реагирования в реальном времени.

На данный момент существует большое количество различных систем для выявления сетевых вторжений, но многие из них могут только эффективно обнаружить и регистрировать несанкционированные действия злоумышленника в сетевом трафике, а связать обнаруженное сетевое вторжение с предотвращающим атаку действием в могут единицы.

При создании Интернет и стека протоколов связи для него никто не задумывался о возможных атаках основанных на уязвимостях самих протоколов связи и о возможности реализации гибридных атак. После обнаружения этой проблемы стали разрабатываться программно-аппаратные комплексы для выявления сетевых атак, такие комплексы получили название систем обнаружения вторжений. В данной работе стояла задача разработки формата сигнатуры, как для эффективного обнаружения атаки, так и для корректной реакции на действия злоумышленника. Для решения поставленной задачи необходимо было удовлетворить следующие требования:

- Быстрая сериализация сетевого трафика и данных из сигнатуры;
- Ассоциирование каждой атаки с конкретной реакцией;
- Оптимизация реакций по классам сетевых атак;

Для удовлетворения первого требования использовался унифицированный формат описания данных XML(Extensible Markup Language), так как для него существует развитый механизмы сериализации, он стандартизирован, и реализован инструментарий сериализации для различных языков программирования.

Для удовлетворения второму требованию был разработан механизм описания в сигнатуре не только самой атаки, но и действий совершаемых системой в момент обнаружения сетевого вторжения. Это дало возможность при выявлении совпадения содержимого сетевого трафика и данных из сигнатуры, ассоциировать действия злоумышленника с конкретной реакцией на них. Такой подход к ассоциированию атаки и реакции на нее, дал возможность без промедления реагировать на вторжение.

Для удовлетворения третьему требованию был разработан механизм ранжирования различных сетевых атак по классам, путем отбора похожих атак, как по способу их реализации, так и по осуществляемому ими деструктивному воздействию на систему. Данный подход позволяет реализовать «слоистую» архитектуру системы обнаружения вторжений, что позволяет различные классы атак обнаруживать на разных уровнях разбора сетевого трафика. Это влечет за собой оптимиза-

цию обнаружения и реакции на атаку по принадлежности к конкретному классу. Такой метод классификации позволяет нам, к примеру, обнаруживать те атаки, которые не требуют полной сборки сеанса связи для обнаружения вторжения на стадии получения сетевых пакетов из канала связи.

Разработанный формат сигнатуры позволяет оптимизировать поиск данных в сетевом пакете, путем жесткого указания в сигнатуре смещения для поиска данных от начала сетевого пакета. Данный метод ускоряет процесс обнаружения, так как поиск данных из сигнатуры осуществляется не по всему разделу с данными сетевого пакета, а лишь в том блоке, к которому указывает заданное смещение.

ЛИТЕРАТУРА

1. *Матросов А.А.* «Проектирование системы обнаружения вторжений на основе структурного анализа типовых нарушений безопасности в сети» // 2005 «Технологии Microsoft в теории и практике программирования», МГТУ им. Н.Э. Баумана.
2. *А. Лукацкий* «Обнаружение вторжений – 2-е изд.» СПб.: BHV, 2003.
3. *Милославская Н.Г., Толстой А.И.* Интрасети: доступ в Internet, защита. М.: Юнити, 1999.
4. *Гилл А.* Введение в теорию конечных автоматов. М., «Мир», 1965.
5. *Глушков В.М.* Синтез цифровых автоматов. Физматгиз, 1962.
6. *Frohwerk R.A.* Signature Analysis: A New Digital Fild Service Method. Hewlett-Packard. May. 1977.
7. *Nadig H.J.* Signature Analysis – Concepts, Examples, and Guidelines. Hewlett-Packard. May. 1977.
8. *Chan A.V.* Easy-to-ase Signature Analyzer Accurctely Trouble-shoots Complex Logic Circuits. Hewlett-Packard, May 1977.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ И БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ

А.Ю. Кишуков

МИФИ, г. Москва, ait@mephi.ru

Сочетание методов электронной цифровой подписи (ЭЦП) и биометрической аутентификации позволяет повысить уровень защищенности ЭЦП. В данной работе это показано на базе использования разработанной ранее теоретической модели биометрического устройства (БУ), добавив к ней подсистему генерации ключей электронной цифровой подписи (ПГкЭЦП).

Предлагается следующий порядок регистрации:

1. БУ переводится в режим регистрации.
2. При появлении в зоне действия БУ персоны происходит считывание одного или нескольких биометрических характеристик.

3. Блок считывания (БС) формирует биометрический образ (БО) данной персоны в виде некой числовой последовательности однозначно соответствующей данной и только данной персоне.

4. Путем комбинированного математического преобразования использующего случайную числовую последовательность, выработанную датчиком случайных чисел происходит генерация Биометрического Ключа Персоны 1 (БКП1) и занесение его в базу данных. В базу данных также заносится соответствующий данному БМК1 биометрический образ.

5. Регистрируются конкретные права доступа (например: чтение запись) к конкретному объекту доступа для данного конкретного БМК1.

Подсистема генерации ключей ЭЦП, может быть включена как составная часть в биометрическое устройств или представлена как внешний программный продукт.

Внутренняя ПГкЭЦП использует при генерации физический датчик случайных чисел ДСЧ, чем обеспечивается необходимое криптографическое качество ключа ЭЦП. В данном случае предлагается следующий порядок генерации электронной цифровой подписи:

1. Активируется ПГкЭЦП, вырабатывается открытый и секретный ключ ЭЦП для данной персоны, открытая часть ключа передается на СВТ, а секретная часть ЭЦП шифруется на ключе хранения БМК1 и записывается в энергонезависимую память. При этом в энергонезависимой памяти задается однозначное соответствие БО, БМК1 и ЭЦП

2. В случае перерегистрации субъекта (перегенерации БМК1) происходит автоматическая смена (перегенерация) ключа ЭЦП.

3. В случае когда секретная часть ключа помещается на жесткий диск СВТ, в матрице доступа прописывается права доступа к файлу с зашифрованным на ключе хранения БМК1 секретным ключом ЭЦП

4. В случае, когда ключ записывается на внешнем носителе секретная часть ЭЦП шифруется на ключе хранения БМК1 и записывается на внешний носитель.

Предполагается, что в нашей модели обеспечивается необходимая длина ключа (например, 256 бит). Это позволяет его использование в качестве ключа хранения секретной части электронной цифровой подписи, которая в свою очередь может располагаться в различных вариантах: Секретная часть ЭЦП может быть размещена в зашифрованном на ключе хранения БМК1 на следующих носителях: на внешнем носителе (дискета, смарт-карта или ТМ ключ), на жестком диске компьютера, во внутренней энергонезависимой памяти.

В случае вызова процедуры подписания электронного документа производится повторная процедура идентификации персоны.

Использование описанного выше алгоритма работы позволит защитить секретную часть ЭЦП от несанкционированного использования

т.к. для его использования субъект доступа (персона) должна пройти процедуру биометрической идентификации.

Данный поход может быть использован при работе в корпоративной сети. Для этого в работе подробно рассмотрены порядок регистрации и работы в сети.

Разработка конкретных устройств в соответствии с описанной моделью позволяет решить задачу реализации возможности работы с ЭЦП в защищенном виде

МОДЕЛИРОВАНИЕ БИОМЕТРИЧЕСКИХ УСТРОЙСТВ, ОБЕСПЕЧИВАЮЩЕГО ВЫСОКИЙ УРОВЕНЬ ЗАЩИТЫ ОБЪЕКТОВ ДОСТУПА

А.Ю. Кишуков

МИФИ, г. Москва, ait@mephi.ru

Биометрическая аутентификация является современным методом, используемым в системах контроля и управления доступом (СКУД). При создании устройств, реализующих биометрическую аутентификацию, с целью их оптимизации возможно использовать функциональные модели. В данной работе предлагается такая модель, относящаяся к устройствам защиты от несанкционированного доступа для системных блоков персональных компьютеров либо более мощных серверов.

Функциональные составляющие модели: сам человек – биологическая персона (БП); биометрический считыватель (БС); центральный процессор. (ЦП); энергонезависимая память (ЭНП; база данных учетных записей (БУЗ); датчик случайных чисел (ДСЧ) . Подсистема отвечающая за генерацию случайных чисел; монитор безопасности (МБ); объекты доступа.

Для каждой составляющей модели сформулированы требования, выполнение которых должно обеспечить оптимальность характеристик устройства биометрической аутентификации.

Модель предполагает следующий порядок режима регистрации:

1. При появлении в зоне действия БС происходит считывание одного или нескольких биометрических характеристик
2. БС формирует биометрический образ (БО) в виде некой числовой последовательности, однозначно соответствующей данной БП.
3. Путем комбинированного математического преобразования использующего случайную числовую последовательность, выработанную ДСЧ, происходит генерация Биометрического Ключа Персоны 1 (БМК1) и занесение его в базу данных (по аналогии) в базу учетных записей зарегистрированных персон. В базу данных также заносится соответствующий данному БМК1 биометрический образ.

4. Администратором системы регистрируются конкретные права доступа (например: чтение запись или односторонний, двухсторонний проход) к конкретному объекту доступа для данного конкретного БМК1

Режим идентификации, представленный в модели:

1. При появлении в зоне действия БС персоны происходит считывание одного или нескольких биометрических характеристик

2. БС формирует биометрический образ данной персоны в виде некой числовой последовательности однозначно соответствующей данной и только данной персоне.

3. ЦП ищет в базе данных соответствующий данному БО БМК1. В случае отсутствия соответствия ни с одной записью БО производится отказ доступа. В случае наличия в базе данных нужного БО происходит считывание БМК1

4. Для данного БМК1 производится проверка конкретных прав доступа к конкретным объектам доступа в соответствии с таблицей доступа. В случае отсутствия зарегистрированных прав в матрице доступа производится отказ в доступе.

Отличительные свойства модели:

- БО и БП является тождеством т.е. данному Б.О. соответствует одна и только одна персона

- ДСЧ является устройством, генерирующим абсолютно случайные числа нужной длины.

- БМК 1 имеет определенное время жизни. В случае истечения периода жизни для БМК1 происходит генерация БМК2. При этом используется тот же БО и новое случайное число.

- БС обладает функциями защиты от угроз типа предъявления точной копии биометрической характеристики, используя многофакторный анализ на комплексе биометрических характеристик. Включает в себе соответствующие алгоритмы распознавания и решает все проблемы связанные с ошибками типа FRR, FAR.

Использование описанного выше алгоритма работы БУ позволит обеспечить:

1. Существенное снижение величин ошибок типа FRR и FAR..
2. Время срабатывания, незаметное для пользователя.
3. Достаточное количество зарегистрированных пользователей.
4. Стойкость к угрозам предъявления к распознаванию точных копий.
5. Автономность работы устройства от защищаемого объекта доступа.
6. Защищенность всей критичной информации по зарегистрированным пользователям

7. Работу на «низком» уровне (проведение проверки прав доступа до активизации операционной системы ЭВМ).

ТЕХНОЛОГИЯ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДЕНЕГ

М.В. Момот, ст. преподаватель каф.МИГ

*Юргинский технологический институт Томского политехнического
университета (ЮТИ ТПУ), г. Юрга, т. 6-06-43,
mvmomot@yrg.kuzbass.net*

Существующие в настоящее время технологии позволяющие осуществлять электронные денежные расчеты очень многообразны: 1) клиент-банк, 2) банковские карты с магнитной полосой, 3) микропроцессорные банковские карты, 4) системы интернет платежей – по принципу PayCash, 5) системы интернет платежей – по принципу WebMoney, 6) мобильные платежные системы, 7) системы построенные по принципу Mondex, 8) системы построенные по патенту RU2165101. Приведем их в таблице проанализировав по ряду показателей: 1) работоспособность системы в отсутствие связи с центральным узлом (доступ к базе данных) в зависимости от продолжительности каждая строка от 0% до 100% (100% – полностью работоспособна): 1 – 4 ч, 8 ч, до 2 дней, более 2 дней, более 20 дней; 2) защищенность пользовательского рабочего места в процентах: от вскрытия: (max –30%), от порчи: (max – 30%), возврат средств, при утере инструмента пользователя: (max – 40%); 3) широта пространственного диапазона с возможностью осуществления операций: городская зона (25% max), удаленность до 50 км (25% max), удаленность до 200 км (25% max), труднодоступные районы (25% max); 4.)доверие пользователей к системе: 30% max –знания не требуются, 30% max – фактов нет, 40% возможны в полном объеме.

В результате проведенного анализа (приведен в таблице) можно получить обобщенную оценку надежности анализируемых систем. Как показано в строке «суммарная оценка...» таблицы наиболее надежны системы с «умными» и защищенными от несанкционированного доступа пользовательскими инструментами.

Сформулируем систему свободную от ряда недостатков, которые присущи проанализированным системам и предлагающую к использованию наличность, но в электронной форме, имеющую высокую степень защиты от подделки и функционирующую в режиме взаиморасчетов. Систему, которая не требует постоянной либо периодической связи с банком. Возьмем за основу использование электронной цифровой подписи (ЭЦП) и микропроцессорные устройства – микроконтроллеры с защитой от считывания данных и программного кода извне, подобные же принципы защиты лежат в основе банковских микропроцессорных карт. ЭЦП будем использовать для защиты транзакций от фальсификации, а защищенные микроконтроллеры (ЗМ) как основу для создания электронных денежных модулей (ЭДМ), которые и будут являться носителями электронной наличности.

Оценка надежности электронных платежных технологий

Системы / показатели	1	2	3	4	5	6	7	8
1.1. (%)	0	0	95	95	0	0	99	99
1.2. (%)	0	0	90	85	0	0	98	95
1.3. (%)	0	0	87	50	0	0	95	90
1.4. (%)	0	0	68	30	0	0	90	70
1.5. (%)	0	0	0	0	0	0	80	10
Итого (%):	0	0	68	52	0	0	92,4	72,8
2.1.	15	10	29	5	5	15	29	29
2.2.	20	10	25	20	20	15	25	25
2.3.	40	30	40	5	5	40	10	35
Итого (%):	75	50	94	30	30	70	64	89
3.1. (%)	25	25	25	25	25	25	25	25
3.2. (%)	25	25	25	25	25	25	25	25
3.3. (%)	12,5	12,5	25	12,5	12,5	0	25	25
3.4. (%)	0	0	25	0	0	0	25	25
Итого (%)	87,5	87,5	87,5	87,5	87,5	50	100	100
4.1. (%)	10	20	20	10	10	20	25	15
4.2. (%)	25	10	25	25	20	30	25	30
4.3. (%)	40	5	5	35	40	0	40	40
Итого:	75	35	50	70	70	50	90	85
Суммарная оценка (%):	59	43	75	60	47	43	87	87

Реальная денежная система имеет структуру с неограниченным числом участников. ЭДМ – носители денежной наличности должны будут создаваться при уже работающей системе, что делает довольно проблематичной проверку ЭЦП ЭДМ если первоначально на них не имелись открытые ключи (ОК) ЭЦП друг друга. Реализуем схему, в которой перед началом обмена наличностью ЭДМ обмениваются своими ОК в защищенном от подделки виде, а затем передаваемую информацию подписывают своими ЭЦП.

Важно организовать многоступенчатую защиту. Для этой цели можно использовать ЭДМ состоящий из нескольких ЗМ, которые хранят данные, имеют разные ЭЦП, и возможно разную основу ЗМ. Этим же реализуется функцию возврата средств с неисправных ЭДМ за счет дублирования информации в разных ЗМ одного ЭДМ, неисправность одного ЗМ приведет к неработоспособности ЭДМ, но исправные ЗМ будут хранить правильные данные.

Для электронной наличности возможны и другие качества исходящие из программной основы ЭДМ. Например, возможен возврат средств с утеранных ЭДМ. Организовать данную функцию можно сле-

дующим способом: закрыть доступ к управлению ЭДМ паролем; некоторую небольшую часть средств ЭДМ разрешить использовать даже при неправильном вводе данного пароля некоторое число раз подряд, при этом основная часть средств ЭДМ под руководством его управляющей программы блокируется, снимается с баланса ЭДМ и формируется в специальный блок – код инкассации (КИ). При попытке воспользоваться подобным ЭДМ код инкассации передается на взаимодействующий ЭДМ. ЭДМ получивший КИ не может его использовать кроме как для передачи другому ЭДМ или в ЦЭ (передачи происходят автоматически). ЦЭ после получения КИ может вернуть средства владельцу. Конечно, возврат возможен только, если утерянный ЭДМ был использован, в противном случае денежная стоимость ЭДМ потеряется.

Автор видит реальную возможность перехода от бумажной наличности на электронную, более защищенную и позволяющую проводить операции взаиморасчетов с очень низкой себестоимостью, что позволит сократить и связанную с оборотами наличных денег преступность. В этой сфере автором ведутся разработки и получен патент на группу изобретений [2].

ЛИТЕРАТУРА

1. *Воскобойников А.* Киберденьги – новая виртуальная реальность // The Retail Finance. 2005. № 2.
2. *Момот М.В.* Электронная денежная система, способ передачи сообщений в электронной денежной системе, способ проведения платежа, способ возврата утерянных денежных средств, способ защиты от вскрытия электронной денежной системы, способ возврата средств с неисправных электронных денежных модулей // Описание изобретения к патенту RU2260207. ФСИСПТЗ. 2005. № 25.
3. *Розен Ш.С.* Электронная денежная система (варианты), электронная банкнота, способ предъявления пароля сети электронной денежной системы, способ изъятия денег с банковского счета, способ внесения депозита, способ произведения платежа, способ обмена иностранной валюты // Описание изобретения к патенту RU2165101. ФСИСПТЗ. 2001.

ФОРМИРОВАНИЕ КРИПТОГРАФИЧЕСКИ ЗАЩИЩЕННОЙ ЭЛЕКТРОННОЙ ПОЧТОВОЙ СЕТИ

*С. Ю. Сеченов, студент 5 курса гр. СБ-101
факультета Компьютерных наук*

*Омский государственный университет им. Ф.М. Достоевского
(ОмГУ), г. Омск, т. 8-913-604-0-391, ssl_25@pochta.ru*

Сейчас большинство почтовых программ снабжены функциями шифрования писем. Так The Bat! имеет наиболее функциональные воз-

возможности в данном плане (это и ЭЦП отправляемых писем и шифрование с использованием криптостойких алгоритмов на больших ключах). Однако на фоне широкого внедрения данных функций из вида опускается важный факт – распространение ключевой информации. Во всех почтовых программах ключи распространяются путем отправки их в открытом виде на почтовые ящики тех пользователей, от которых хотелось бы принимать зашифрованную корреспонденцию. Так при проведении атаки «посредника» можно произвести «вброс» ложной информации.

Была поставлена задача смоделировать систему, в которой будет сведена к минимуму данная атака.

Результатом решения поставленной задачи стал проект почтовой системы и её практическая реализация.

Целью предлагаемого проекта ставится организация почтовой сети, обеспечивающей конфиденциальность корреспонденции путем шифрования информации по стандарту AES[1]. Для реализации проекта используется стандартный набор почтовых протоколов. Почтовая сеть реализована как набор приложений на базе операционной системы Windows.

В предлагаемой системе вводится выделенный сервер, на который передается функция предоставления ключевой информации, а первоначальное общение клиента и сервера осуществляется с использованием алгоритма шифрования Диффи – Хелмана.

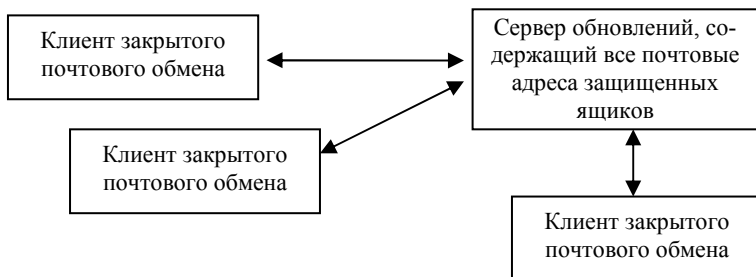
Построение защищенной почтовой сети сталкивается с рядом проблем построения защищенного канала связи между N пользователями. Данная проблема может быть решена с помощью шифрования на стойком алгоритме с достаточно длинным ключом. Но при этом возникает ряд проблем:

- при использовании симметричного шифрования, необходимо каждому участнику сообщить ключи шифрования остальных абонентов. И, как следствие, во-первых необходимо построить защищенный канал для передачи ключей, а во-вторых компрометация таблицы ключей у одного из пользователей автоматически разрушит всю систему защищенного канала;

- при использовании асимметричного шифрования возникают трудности с генерацией ключевой информации и медлительностью работ по расшифровыванию;

- необходимость при каждом новом сеансе производить смену сеансового ключа, исключает возможность использования любого из описанных выше способов по отдельности. Откуда вытекает необходимость построения комбинированной схемы шифрования.

Поддержка защищенной почтовой сети осуществляется сервером, на котором хранится список всех почтовых ящиков, хозяева которых хотели бы получать корреспонденцию в зашифрованном виде. При этом участники зашифрованного почтового обмена имеют возможность производить прием писем как в зашифрованном, так и в открытом виде. Выделенный сервер служит для снятия с пользователей вопрос рассылки ключевой информации.



Каждый «клиент» при установке (настройке почтового ящика через который будет происходить отправка и прием писем) автоматически сообщает на «сервер» о том, что данный почтовый ящик предназначен для приема шифрованных писем. Так же «клиент» при активации производит генерацию открытого и закрытого ключей шифрования методом RSA[2] (BigOpenRSAKey и BigCloseRSAKey), затем, используя протокол Диффи – Хелмана[2], серверу отсылается BigOpenRSAKey.

«Сервер», получив от «клиента» информацию о почтовом ящике и BigOpenRSAKey, отвечает списком известных ему других почтовых адресов и связанных с ними BigOpenRSAKey, а полученную информацию заносит в список обновлений, который потом будет передан другим «клиентам». Чтобы быть постоянно в курсе изменений, производимых на сервере, клиенты регулярно производят обновления своих баз данных, скачивая обновления с «сервера».

При отправке письма, «клиент» проверяет наличие введенного адреса в базе для шифрования. Если адрес получателя присутствует в базе шифрования, то «клиент» генерирует «сеансовый ключ», на котором зашифровывает все письмо. После этого шифруется «сеансовый ключ» на BigOpenRSAKey адресата, результат шифрования конкатенируется с письмом, и результат отправляется получателю. При отсутствии адреса получателя в базе шифрования письмо отправляется в открытом виде.

При получении письма, проверяется наличие адреса отправителя в базе шифрования. При наличии адреса отправителя в базе шифрования, определяется BigCloseRSAKey, по которому восстанавливается «сеансовый ключ» и расшифровывается письмо.

При необходимости создания полностью зашифрованного документооборота, существует возможность отказаться от приема писем с почтовых адресов, не содержащихся в базе клиентов.

Для «клиента» предлагается использовать съемный носитель информации для хранения секретного ключа пользователя (BigCloseRSAKey) на случай переустановки «клиента».

Сервер при получении сообщения об изменении BigOpenRSAKey клиента, добавляет его в файл обновлений. Клиенты, получив обновления, содержащие сведения об изменении BigOpenRSAKey, заменяют в своих базах данное поле.

Данный проект решает проблему построения защищенной сети почтовых сообщений, используя методы как симметричного, так и асимметричного шифрования.

ЛИТЕРАТУРА

1. Зензин О.С., Иванов М.А. «AES - стандарт криптографической защиты. Конечные поля», ИД КУДИЦ-ОБРАЗ, 2003
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. «Основы криптографии. Учебное пособие», Гелиос АРВ, 2001

ИССЛЕДОВАНИЕ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ГОСТ 34.10-2001

*А.М. Федосеев, студент 5 курса фак-та Компьютерных наук
Омский государственный университет им. Ф.М. Достоевского
(ОмГУ), amf@rol.ru. +7 9043 292953*

Скрытый канал – тайный канал связи, по которому передаются сообщения, сами по себе не содержащие секретной информации.

Густавус Симмонс выдвинул концепцию создания скрытого канала с помощью обычных алгоритмов цифровой подписи. [1]

В работе Б. Шнайера [2] были приведен «типичный» протокол скрытого канала: отправитель, используя секретный ключ, общий с получателем, подписывает невинное сообщение, пряча в подписи скрытое сообщение. Также в работе Шнайера были приведены алгоритмы создания подобных каналов с использованием схем Онга-Шнорра-Шамира, Эль-Гамала, E-SIGN и DSA.

Алгоритмы, описанные в [1], для внедрения скрытого сообщения опираются на свойства операций в кольце, и подмену генерируемого случайного числа.

Целью данной работы являлось исследование электронной цифровой подписи ГОСТ 34.10-2001, и попытка переложения каналов, описанных Б. Шнайером [2].

Исследуя Российский стандарт ГОСТ Р 34.10-2001 [3], описывающий алгоритмы формирования и проверки ЭЦП основанной на эллиптических кривых, было сделано предположение, что данная цифровая подпись не лишена возможности внедрения скрытой информации. Более того, цифровой дайджест этой подписи достаточно велик (512 бит), что позволяем сделать предположение о достаточности объема скрываемой информации.

Самый простой способ организации скрытого канала, является подмена генерируемой, при формировании подписи, псевдослучайного числа k , на скрываемую информацию. По алгоритму формирование подписи число k должно быть меньшим простого числа q ($2^{254} < q < 2^{255}$). Следовательно, можно «спрятать» до 255 бит.

Попытку перехвата (обнаружения) данного канала можно серьезно усложнить путем шифрования секретной информации. В этом случае, тесты на случайность (псевдослучайной) не смогут гарантировано выявить подмену.

Остальной ряд подходов, описанных Шнайером [2], достаточно тяжело или невозможно переложить на ГОСТ.

Однако, следует заметить, что без предварительной договорённости обеих сторон о ключах, создание достаточно стойкого скрытого канала невозможно.

Литература

1. *Simmons G.J.* The Subliminal Channel and Digital Signatures, *Advances in Cryptology: Proceedings of EUROCRYPT 84*, Springer-Verlag, 1985, pp. 364–378.
2. *Шнайер Б.* Прикладная криптография. М.: Триумф, 2003.
3. ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

СОДЕРЖАНИЕ

Информационное сообщение.....	3
-------------------------------	---

СЕКЦИЯ 8

РАСПРЕДЕЛЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

*Председатель – Ехлаков Ю.П. проректор по Информатизации
ТУСУР, зав. каф. АОИ, д.т.н., профессор;
зам. председателя – Сенченко П.В., к.т.н., доцент каф. АОИ*

Егорова Е.А., Боровской И.Г.

РЕАЛИЗАЦИЯ СПОСОБА ИЗВЛЕЧЕНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ ИЗ ПРОИЗВОЛЬНОГО ОКНА ОС WINDOWS.....	9
---	---

Коновалова Е.В., Веберова И.И.

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ВЕДЕНИЯ НАУЧНО-СПРАВОЧНОГО АППАРАТА АРХИВОВ	11
--	----

Коришупов А.А., Веберова И.И.

ПРОБЛЕМА ИНФОРМАЦИОННОЙ СОВМЕСТИМОСТИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРИ МЕЖВЕДОМСТВЕННОМ ВЗАИМОДЕЙСТВИИ.....	13
---	----

Кровякова Т.С., Соловьев Д.А.

ОСНОВНЫЕ ФАКТОРЫ РАНЖИРОВАНИЯ И ИНДЕКСАЦИИ В ПОИСКОВЫХ СИСТЕМАХ. МЕТОДЫ ПОИСКОВОЙ ОПТИМИЗАЦИИ	15
---	----

Лакеев И.С., Юркин Е.И.

ПРИНЦИПЫ ПОСТРОЕНИЯ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ПРОСТРАНСТВЕННОГО АНАЛИЗА ОБЪЕКТОВ ЭЛЕКТРОННОГО ГЕНПЛАНА	18
--	----

Никитин Е.В., Сенченко П.В.

«УМНЫЕ КЛИЕНТЫ» – ОПТИМАЛЬНЫЙ ТИП КЛИЕНТСКИХ ПРИЛОЖЕНИЙ	20
--	----

Ощепков С.С.

ТЕХНОЛОГИЯ ВЕДЕНИЯ ПРОСТРАНСТВЕННЫХ ДАННЫХ ОБ ОБЪЕКТАХ ИНЖЕНЕРНОЙ ИНФРАСТРУКТУРЫ В WEB-ОРИЕНТИРОВАННЫХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ.....	23
---	----

Отчалко А.В.

ТЕХНОЛОГИЯ WEB-ОПУБЛИКОВАНИЯ ПРОСТРАНСТВЕННЫХ ДАННЫХ.....	25
--	----

Рыбалов Н.Б.	
ПОДСИСТЕМА ВЕДЕНИЯ АРХИВНЫХ ДОКУМЕНТОВ В СРЕДЕ ЭЛЕКТРОННОГО ГЕНЕРАЛЬНОГО ПЛАНА	27
Сергеев А.С., Веберова И.И.	
ПРИНЦИПЫ ПОСТРОЕНИЯ ЕДИНОЙ СИСТЕМЫ КЛАССИФИКАЦИИ И КОДИРОВАНИЯ ИНФОРМАЦИИ	30
Осетров Д.Г., Шелковников З.А., Чаунин С.С., Шибельгут С.А., Глушков Я.А.	
ПОСТРОЕНИЕ КОМПЬЮТЕРНОЙ СЕТИ ДЛЯ IP ТЕЛЕФОНИИ	32
Силич В.В.	
ТЕХНОЛОГИИ ИНТЕРАКТИВНОГО ВЗАИМОДЕЙСТВИЯ ВЕБ-ПРИЛОЖЕНИЙ В СРЕДЕ ИНТЕРНЕТ	35
Степанов А.В.	
ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ AUTODESK MAPGUIDE LITEVIEW ДЛЯ ПРЕДСТАВЛЕНИЯ ДИНАМИЧЕСКИХ РАСТРОВЫХ КАРТ В WEB-ПРИЛОЖЕНИЯХ	38
Курбацкий В.Г., Томин Н.В.	
НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЗАДАЧЕ ПРОГНОЗИРОВАНИЯ РЕЖИМНЫХ ПАРАМЕТРОВ И ХАРАКТЕРИСТИК В ЭНЕРГОСИСТЕМАХ	40
Труфакина А.И., Русановский А.С., Замятин Д.Н.	
ЛАБОРАТОРНАЯ ИНФОРМАЦИОННО-МЕНЕДЖМЕНТСКАЯ СИСТЕМА	43
Вагнер Д.П.	
ИНФОРМАЦИОННО-СПРАВОЧНЫЙ ПОРТАЛ БЫСТРОГО РАЗВОРАЧИВАНИЯ КОММЕРЧЕСКИХ САЙТОВ	44
Вишняков В.Ю.	
АИС «ОБЪЕКТЫ ИНЖЕНЕРНЫХ СЕТЕЙ»	47
Важдаев А.Н.	
УПРАВЛЕНИЕ РАСПРЕДЕЛЕННЫМИ БАЗАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВЕТЕРИНАРНОГО УЧРЕЖДЕНИЯ ГОРОДА И РАЙОНА	50
Юркин Е.И., Лакеев И.С.	
ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ УЧЕТА ПРОИЗВОДСТВЕННЫХ ЗДАНИЙ И СООРУЖЕНИЙ В СРЕДЕ ЭГП ООО «ТОМСКНЕФТЕХИМ»	53
Юсупова Ю.Т., Боровской И.Г.	
РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ ОФИСНЫХ ПРИЛОЖЕНИЙ MS WORD И MS EXCEL ДЛЯ РЕШЕНИЯ СТАТИСТИЧЕСКИХ ЗАДАЧ	55

СЕКЦИЯ 10

АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА В СИСТЕМАХ УПРАВЛЕНИЯ И ПРОЕКТИРОВАНИЯ

Председатель – Шурыгин Ю.А., первый проректор ТУСУР,

зав. каф. КСУП, д.т.н., профессор;

зам. председателя – Коцубинский В.П., зам. зав. каф. КСУП, к.т.н., доцент

Абушаев Р.Р., Аркатова О.Е.

ПРОГРАММНЫЙ МОДУЛЬ «МЕНЕДЖЕР СМК» ДЛЯ ОРГАНИЗАЦИИ
УПРАВЛЕНИЯ ДОКУМЕНТАЦИЕЙ В СЛУЖБЕ КАЧЕСТВА
ИОА СО РАН58

Андреев И.Ю.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА
ОПЕРАТОРА АСУ ТП ГАЗОПРОВОДА «МЫЛЬДЖИНО-ВЕРТИКОС»60

Чертов А.А.

ВЕКТОРИЗАЦИЯ ДВУЦВЕТНЫХ ИЗОБРАЖЕНИЙ
С ИСПОЛЬЗОВАНИЕМ ТРИАНГУЛЯЦИИ63

Драганов В.А.

ИНТЕГРАЦИЯ БИЗНЕС-ПРИЛОЖЕНИЙ В АВТОМАТИЗИРОВАННЫХ
СИСТЕМАХ УПРАВЛЕНИЯ МАРКЕТИНГОМ65

Фофонов А.В.

МНОГОСЛОЙНАЯ АРХИТЕКТУРА В ТЕХНОЛОГИЧЕСКИХ
ПРОГРАММНЫХ СИСТЕМАХ67

Канский Е.А., Кузяков О.Н.

СОЗДАНИЕ СВЕТОДИОДНОГО ТАБЛО С МЕХАНИЧЕСКОЙ
ГОРИЗОНТАЛЬНОЙ РАЗВЕРТКОЙ НА БАЗЕ МК АТ89S825270

Макеева Н.Л., Кромин Л.А.

ПРИМЕНЕНИЕ UML КАК РЕШЕНИЕ ПРОБЛЕМЫ ПРИ
ПРОЕКТИРОВАНИИ ВСТРАИВАЕМЫХ СИСТЕМ ЦИФРОВОЙ
ОБРАБОТКИ СИГНАЛОВ73

Миргородский С.К.

ПРОГРАММА ДЛЯ ОБРАБОТКИ ДАННЫХ ДЕФОРМИРУЕМОЙ
ТВЕРДОЙ ПОВЕРХНОСТИ75

Моисеев А.А.

ИСПОЛЬЗОВАНИЕ МНОГОСПЕКТРАЛЬНЫХ ДАННЫХ ПРИБОРА
MODIS ДЛЯ ОБНАРУЖЕНИЯ ПОЖАРОВ79

Никитин Е.С.

ИЗУЧЕНИЕ ВЗАИМОСВЯЗИ ПАРАМЕТРОВ СИГНАЛОВ
АКУСТИЧЕСКОЙ ЭМИССИИ С МЕХАНИЧЕСКИМ НАПРЯЖЕНИЕМ
В ДЕФОРМИРУЕМЫХ МЕТАЛЛАХ82

Пешехонов С.В.	
ОБНАРУЖЕНИЕ КУСОЧНО-ПЛОСКОСТНЫХ ОБЪЕКТОВ ПО ДАННЫМ ЛАЗЕРНОГО ЗОНДИРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ПОВЕРХНОСТНОЙ ТРИАНГУЛЯЦИИ	87
Попов А.Н.	
МНОГОФУНКЦИОНАЛЬНАЯ СИСТЕМА ОХРАНЫ И КОНТРОЛЯ ДОСТУПА	90
Аксенова А.А.	
АВТОМАТИЗИРОВАННАЯ СИСТЕМА СКЛАДСКОГО УЧЕТА МЕДИКА- МЕНТОВ ДЛЯ АПТЕЧНОГО ОТДЕЛЕНИЯ НА ПЛАТФОРМЕ «1С: ПРЕДПРИЯТИЕ. ОПЕРАТИВНЫЙ УЧЕТ 7.7»	92
Аллянов А.А., Одинокоев В.В.	
ЗАЩИЩЕННЫЙ РЕЖИМ РАБОТЫ МИКРОПРОЦЕССОРА INTEL	94
Андреев С.М., Аркатова О.Е.	
АВТОМАТИЗИРОВАННАЯ СИСТЕМА АНАЛИЗА РЕЗУЛЬТАТОВ ВНУТРЕННЕГО АУДИТА СМК В ИОА СО РАН	95
Андреев С.М., Андреев В.И.	
АВТОМАТИЗАЦИЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ЭЛЕКТРОМАГНИТНЫХ ПРОЦЕССОВ В ЭЛЕКТРОМЕХАНИЧЕСКИХ ПРЕ- ОБРАЗОВАТЕЛЯХ	97
Бугреев А.В., Одинокоев В.В.	
СИСТЕМА МОНИТОРИНГА ПРОГРАММНОГО И АППАРАТНОГО ОБЕСПЕ- ЧЕНИЯ СЕРВЕРНЫХ СТАНЦИЙ. КЛИЕНТСКАЯ ЧАСТЬ	100
Бурлаков Р.О.	
АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС ДЛЯ ИЗМЕРЕНИЯ И КОНТРОЛЯ ТОПОГРАФИИ МАГНИТНОГО ПОЛЯ МНОГОПОЛЮСНЫХ МАГНИТНЫХ СИСТЕМ	102
Васильев Л.Л., Черкашин М.В.	
ПРОГРАММА «ДИАГРАММА СМТА»	104
Вершинин Д.Н.	
АВТОМАТИЗАЦИЯ ПРОЦЕССА ИЗМЕРЕНИЯ ФОКУСНЫХ РАССТОЯНИЙ ОПТИЧЕСКИХ ЭЛЕМЕНТОВ	105
Гайдамака О.А., Рыбалка Е.Н.	
РАЗРАБОТКА БАЗЫ ДАННЫХ «РЕМОНТ» ДЛЯ КОМПЬЮТЕРНОЙ ФИРМЫ «ИНСТАЛ»	108
Гаськов А.М.	
РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЦЕНКИ ТЕХНИЧЕСКОГО СОСТОЯНИЯ ПРОМЫШЛЕННОГО ОБОРУДОВАНИЯ	109
Горбылев И.В., Коцубинский В.П.	
ДЕКОМПОЗИЦИЯ ЗАДАЧИ СИНТЕЗА РЕЧИ	111

Горбылев И.В., Коцубинский В.П. СИСТЕМНЫЙ ПОДХОД К ЗАДАЧЕ СИНТЕЗА РЕЧИ	114
Горев Е.В., Орлова Т.И., Рыбалка Е.Н. РАЗРАБОТКА ИНТЕРНЕТ-МАГАЗИНА ПО ПРОДАЖЕ ОТДЕЛОЧНЫХ МА- ТЕРИАЛОВ	117
Гриц О.А. ПРОЕКТ «ЭЛЕКТРОННАЯ КАФЕДРА»	118
Губина С.А., Рыбалка Е.Н. ОПТИМИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ ПРОДАЖ.....	120
Гусельников Г.М. ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА КОМПЬЮТЕРОВ И ОРГТЕХНИКИ НА ПРЕДПРИЯТИИ.....	121
Даниэльс Н.Н., Рыбалка Е.Н. РАЗРАБОТКА WEB – САЙТА ТУРИСТИЧЕСКОГО АГЕНТСТВА	123
Клименко А.Я., Дашиева Ж.Ц УПРАВЛЕНИЕ СЧЕТАМИ ПРОЦЕССИНГОВОЙ КОМПАНИИ.....	125
Долин А.В., Авдеев С.В., Андреев М.И. АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО ВРАЧА АНЕСТЕЗИОЛОГА-РЕАНИМАТОЛОГА	127
Елистратов Д.С. Андреев М.И. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПТИЧЕСКОГО КАНАЛА ЛИДАРА	129
Жулин Р.Г. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ МОНОЛИТНОГО ПОЛЕВОГО ТРАНЗИСТОРА.....	131
Звонков Д.А. ИНСТРУМЕНТАЛЬНАЯ СИСТЕМА СОЗДАНИЯ ТРЕНАЖЕРОВ ПО КУРСАМ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И МОДЕЛИРОВАНИЯ СИСТЕМ	132
Изюмов А.А., Хабибулина Н.Ю. ПРОГРАММНЫЙ МОДУЛЬ «НЕЧЕТКИЕ МНОЖЕСТВА»	136
Изюмов А.А. ПРОГРАММНЫЙ МОДУЛЬ «НЕЙРОННЫЕ СЕТИ»	138
Изюмов А.А., Хабибулина Н.Ю. АВТОМАТИЗИРОВАННАЯ ОБУЧАЮЩАЯ СИСТЕМА ПО ТЕМАМ «НЕЧЕТКИЕ МНОЖЕСТВА» И «НЕЙРОННЫЕ СЕТИ»	139
Исаенко А.А. СИСТЕМА АВТОТРЕКИНГА ДЛЯ СИСТЕМ БЕСПРОВОДНОЙ ОПТИЧЕСКОЙ СВЯЗИ	141
Каримов И.Х., Ковшов А.В. УЛЬТРАЗВУКОВОЙ ДОПЛЕРОВСКИЙ НЕИНВАЗИВНЫЙ ИЗМЕРИТЕЛЬ СКОРОСТИ КРОВОТОКА.....	144

Квашин А.Ю., Бабак Л.И. СПЕЦИАЛИЗИРОВАННЫЙ ГРАФИЧЕСКИЙ РЕДАКТОР ДЛЯ ВВОДА СХЕМ СВЧ-УСТРОЙСТВ.....	146
Китлер С.В. РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА «НАХОЖДЕНИЕ ЭКСТРЕМУМОВ МНОГОЭКСТРЕМАЛЬНЫХ ФУНКЦИЙ ПРИ ПОМОЩИ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ»	147
Климович А.С., Пономарев А.А. ИНТЕРАКТИВНАЯ СИСТЕМА ВЫБОРА КОНДЕНСАТОРОВ И АВТОМАТИЧЕСКАЯ УСТАНОВКА ИХ НА СХЕМУ ЭЛЕКТРИЧЕСКУЮ ПРИНЦИПИАЛЬНУЮ.....	180
Коркач Е.В., Хабибулина Н.Ю. КОРПОРАТИВНАЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА РЕКЛАМНОЙ КОМПАНИИ.....	152
Коротин О.П. РАЗРАБОТКА СИСТЕМ АТМОСФЕРНОЙ ОПТИЧЕСКОЙ СВЯЗИ.....	154
Крахмаль А.В., Крохмаль Е.В. ПРОГРАММНЫЙ КОМПЛЕКС МОДЕЛИРОВАНИЯ ТЕПЛОВЫХ И ДЕФОРМАЦИОННЫХ ПРОЦЕССОВ ПРИ ИНДУКЦИОННОМ НАГРЕВЕ ОСЕСИММЕТРИЧНЫХ СОПРЯЖЕННЫХ ТЕЛ	157
Кригер Д.В., Кригер А.В. БАЗА ДАННЫХ ДОЛЖНИКОВ КРЕДИТНОГО ОТДЕЛА СТРАХОВОЙ КОМ- ПАНИИ ООО «СК КОМЕСТРА-ТОМЬ»	158
Кузнецов И.В. РАЗРАБОТКА КОММУНИКАЦИОННОГО ДРАЙВЕРА ДЛЯ КОНТРОЛЛЕРА CONTROLLOGIX 5500.....	160
Кунтаев А.Н., Рыбалка Е.Н. АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА В СТРОИТЕЛЬНОЙ КОМПА- НИИ	162
Ледовских А.В., Клименко А.Я. АЛГОРИТМЫ И ПРОГРАММЫ ТИПОВОГО РЕШЕНИЯ ЗАДАЧ УПРАВЛЕНИЯ СПРАВОЧНИКАМИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ.....	164
Линник О.Ю., Столбов И.А. КОМПЬЮТЕРНЫЙ ТРЕНАЖЕР ДЛЯ ОБУЧЕНИЯ ОРИЕНТИРОВАНИЮ ПО СРЕДСТВАМ ЛАЗЕРНОЙ НАВИГАЦИИ.....	165
Лощилов И.Г., Нефедьев А.В., Бабак Л.И. РАЗРАБОТКА ПРОГРАММЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ТРАНЗИСТОРНЫХ СВЧ-УСИЛИТЕЛЕЙ НА ОСНОВЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ	168

Лощилов И.Г., Бабак Л.И.	
АВТОМАТИЗИРОВАННЫЙ СТРУКТУРНЫЙ СИНТЕЗ ТРАНЗИСТОРНЫХ СВЧ-УСИЛИТЕЛЕЙ С ИСПОЛЬЗОВАНИЕМ МУТАЦИОННОГО ГЕНЕТИЧЕСКОГО АЛГОРИТМА	170
Максименко П.В.	
АВТОМАТИЧЕСКАЯ ОПТИЧЕСКАЯ ЛОКАЦИОННАЯ СИСТЕМА.....	173
Медведева М.М., Меццержаков Р.В.	
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА RSA	175
Момот Д.С.	
ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ IP-СЕТИ	179
Николаев А.В., Аркатова О.Е.	
ПРОГРАММНЫЙ МОДУЛЬ «МЕНЕДЖЕР СМК» ДЛЯ ОРГАНИЗАЦИИ УПРАВЛЕНИЯ И ВЗАИМОДЕЙСТВИЯ ПРОЦЕССАМИ СМК В ИОА СО РАН	181
Овчаренко А.Н., Рождественский Д.А.	
РАЗРАБОТКА ЛАБОРАТОРНЫХ МАКЕТОВ НА БАЗЕ ПИД-РЕГУЛЯТОРА ТРМ101	183
Погребских О.Я., Столбов И.Л.	
СИСТЕМА ОПТИЧЕСКОГО СКАНИРОВАНИЯ НА БАЗЕ ГИСТЕРЕЗИСНОГО ЭЛЕКТРОДВИГАТЕЛЯ С ПУСТОТЕЛЫМ ВАЛОМ.....	185
Потапова Е.А.	
АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА «КОНТИНГЕНТ КАФЕДРЫ»	186
Румынская Е.С., Рождественский Д.А.	
ИЗУЧЕНИЕ MASTER-SCADA	188
Савельев А.С., Клименко А.Я.	
ПОДСИСТЕМА ВЕДЕНИЯ ДОГОВОРОВ ПАКЕТА ПРОГРАММ BASK-OFFICE ОПЕРАЦИОННОГО ЦЕНТРА	191
Синянская И.В., Черкашин М.В.	
БАЗА ДАННЫХ «ВЫПУСКНИКИ КАФЕДРЫ КСУП»	192
Солодучина Н.В., Хабибуллина Н.Ю.	
РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ ОБУЧАЮЩЕЙ СИСТЕМЫ НА БАЗЕ WEB-ТЕХНОЛОГИЙ	194
Тимофеев Д.Е.	
ПРОГРАММА ЧИСЛЕННОЙ ИДЕНТИФИКАЦИИ ПАРАМЕТРОВ МОДЕЛИ СВЧ-ТРАНЗИТОРА	196
Томина Ю.А., Удод А.С.	
КОНФИГУРИРОВАНИЕ ПРОГРАММИРУЕМОГО ЛОГИЧЕСКОГО КОНТРОЛЛЕРА ЭЛСИ-ТМ	198

Трунов С.А., Телицын Е.А., Каневский О.И.	
ПРОЕКТИРОВАНИЕ УСТАНОВКИ ЛАЗЕРНОЙ РЕЗКИ	199
Хрущев Р.С.	
ПРИНЦИПЫ ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ КОМПОНОВКИ ТЕХНИЧЕСКИХ ОБЪЕКТОВ В ЗАДАННОМ ОБЪЕМЕ	201
Царегородцев К.Ю., Андреев М.И.	
АВТОМАТИЗИРОВАННЫЙ ЛАБОРАТОРНЫЙ СТЕНД ПО ДИСЦИПЛИНЕ «ТЕОРИЯ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ».....	202
Черепанов А.М.	
РЕДАКТОР СХЕМ ДЛЯ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО СИНТЕЗА СВЧ-УСТРОЙСТВ.....	204
Чижик Е.Г.	
ЭЛЕКТРОННЫЙ ИЗМЕРИТЕЛЬ СКОРОСТИ ВЕТРА	206
Шеерман Ф.И., Барышников А.С., Нехорошев М.В., Вьюшков В.А., Бабак Л.И.	
ИНТЕГРИРОВАННЫЙ ИНСТРУМЕНТ ДЛЯ СИНТЕЗА СОГЛАСУЮЩИХ ЦЕПЕЙ В СРЕДЕ ПРОЕКТИРОВАНИЯ СВЧ-УСТРОЙСТВ MICROWAVE OFFICE.....	207
Штихлинг Е.А., Решетникова Г.Н.	
УПРАВЛЕНИЕ ПОСТАВКАМИ НЕСКОЛЬКИХ ВИДОВ ТОВАРОВ.....	210
Щербаков Ф.К.	
ЭЛЕКТРОННЫЙ ПНЕВМОГРАФ	213
Юндин Е.А., Одинокое В.В.	
СИСТЕМА МОНИТОРИНГА ПРОГРАММНОГО И АППАРАТНОГО ОБЕСПЕЧЕНИЯ СЕРВЕРНЫХ СТАНЦИЙ. СЕРВЕРНАЯ ЧАСТЬ	215

СЕКЦИЯ 11

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Председатель – **Ильющенко В.Н.**, проректор по ИР ТУСУР,
зав. каф. РЗИ, д.т.н., профессор;
зам. председателя – **Загоскин В.В.**, к.ф.-м.н., доцент каф. РЗИ

Аюпова А.Р., Кромина Л.А.	
ЗАЩИТА ОПТИЧЕСКИХ ДИСКОВ КАК РЕШЕНИЕ ПРОБЛЕМЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА	217
Копытков Д.Ю.	
ИДЕНТИФИКАЦИЯ ОБЪЕКТОВ В АСИНХРОННЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМАХ.....	220

Копытков Д.Ю.

ПРОБЛЕМЫ ОБЪЕДИНЕНИЯ ОДНОВРЕМЕННО ИЗМЕНЕННЫХ ДАННЫХ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ С АСИНХРОННЫМ ТИРАЖИРОВАНИЕМ	223
--	-----

Космачев А.В.

СПАМ. МЕТОДЫ ПРОТИВОДЕЙСТВИЯ	225
------------------------------------	-----

Курило А.П., Малюк А.А., Михайлов С.Ф., Сенаторов М.Ю., Толстой А.И.

ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ	229
---	-----

Малюк, А.А. Толстой А.И., Попова З.В.

СЕРТИФИКАЦИЯ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ	231
---	-----

Сапрыкин А.А., Спицын В.Л.

СОЗДАНИЕ БЛОКА ПЕРЕСТАНОВОК НА ОСНОВЕ ОБОБЩЕННОЙ РЕШЕТКИ КАРДАНО	233
---	-----

Шейда В.В.

МОДИФИКАЦИЯ ПРОТОКОЛА TCP ДЛЯ ПРИМЕНЕНИЯ В SSL-VPN СЕТЯХ	235
---	-----

Архангельская А.В.

ОБ ОПРЕДЕЛЕНИЯХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ОСНОВАННЫХ НА ЭНТРОПИИ ВЫРАБАТЫВАЕМОЙ ПОСЛЕДОВАТЕЛЬНОСТИ	237
---	-----

Архангельская А.В., Запечников С.В.

КРИПТОГРАФИЧЕСКИЕ ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ С РАСПРЕДЕЛЕННЫМ СЕКРЕТНЫМ КЛЮЧОМ	240
---	-----

Запечников С.В.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КЛЮЧЕВОЙ СИСТЕМЫ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОЙ СРЕДЕ	243
--	-----

Алексеев П.К.

ТЕХНОЛОГИЯ СОЗДАНИЯ ЭЛЕКТРОННЫХ АРХИВОВ, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ	246
--	-----

Берестов А.А., Петров В.А.

МЕТОД СОЗДАНИЯ МНОГОАГЕНТНЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ЭВМ	248
--	-----

Борискин Д.А.

ПРОБЛЕМЫ СОЗДАНИЯ СИСТЕМЫ ИСКУССТВЕННОЙ ДЕВЕРСИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	250
--	-----

Лекшин О.С.

МЕТОДЫ КОНТЕНТ-АНАЛИЗА СОЦИАЛЬНО-ДИНАМИЧЕСКИХ ПРОЦЕССОВ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	252
--	-----

Рудик К.П.

ВЫЯВЛЕНИЕ ИСТОЧНИКОВ РАССЫЛКИ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ ПРОТОКОЛА SMTP	253
---	-----

Ткаченко С.И.

ПРЕДЛОЖЕНИЕ ТЕХНОЛОГИИ ПОСТРОЕНИЯ АИС, ПОВЫШАЮЩЕЙ УРОВЕНЬ ДОСТУПНОСТИ ДАННЫХ И СОХРАНЯЮЩЕЙ ЗАДАННЫЙ УРОВЕНЬ СЛОЖНОСТИ АДМИНИСТРИРОВАНИЯ	255
---	-----

Ткаченко С.И.

РАССМОТРЕНИЕ ПРОБЛЕМ, ВОЗНИКАЮЩИХ ПРИ ШИФРОВАНИИ ДАННЫХ В БАЗЕ ДАННЫХ	257
--	-----

Филатов С.Г.

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ ПЕРЕДАВАЕМЫХ ПО СЕТИ ДАННЫХ СУБД ORACLE	259
--	-----

Чибилов М.О.

ВЫБОР ТЕОРЕТИКО-ИГРОВОЙ МОДЕЛИ ОПИСАНИЯ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ	260
--	-----

Чугунов Е.И.

РАЗРАБОТКА АРМ ДЛЯ ПРОВЕДЕНИЯ ПЕРВИЧНЫХ ИССЛЕДОВАНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ПРЕДМЕТ ВЫЯВЛЕНИЯ СВОЙСТВ, ПОДПАДАЮЩИХ ПОД ДЕЙСТВИЕ 28 ГЛАВЫ УК РФ: МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЙ ПРОГРАММНЫХ СРЕДСТВ СКРЫТОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ (ПССИВ)	261
--	-----

Велигодский С.С. , Милославская Н.Г.

АУТЕНТИФИКАЦИИ В КОРПОРАТИВНЫХ ПОРТАЛАХ	263
---	-----

Зубенко Г.В.

ПОСТРОЕНИЕ РКІ НА ОСНОВЕ ЦИФРОВОЙ ПОДПИСИ С ОПЕРЕЖАЮЩЕЙ БЕЗОПАСНОСТЬЮ	265
--	-----

Мясумов М.М.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ И РЕАЛИЗАЦИИ СХЕМ РАСПРЕДЕЛЕННОГО БЛОЧНОГО ШИФРОВАНИЯ	267
---	-----

Полянская О.Ю.

СОВРЕМЕННЫЕ БИЗНЕС-МОДЕЛИ И РЕШЕНИЯ РАЗВЕРТЫВАНИЯ РКІ	269
--	-----

Зыков С.В.

ОБОБЩЕНИЕ СХЕМЫ ПРОЕКТИРОВАНИЯ ПОРТАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ	271
--	-----

Зыков С.В.

УПРАВЛЕНИЕ ИНТЕРНЕТ-КОНТЕНТОМ: СЕМАНТИЧЕСКИЙ ПОДХОД	273
---	-----

Зыков С.В.	
ИНТЕГРАЦИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОРПОРАЦИИ НА ОСНОВЕ ПОРТАЛЬНОЙ ТЕХНОЛОГИИ.....	275
Станкевичус А.А.	
РАЗРАБОТКА ПЕРСОНАЛЬНОГО МЕЖСЕТЕВОГО ЭКРАНА С ВОЗМОЖНОСТЬЮ ШИФРОВАНИЯ СЕТЕВОГО ТРАФИКА	277
Смирнов П.В.	
ИСПОЛЬЗОВАНИЕ ВЫХОДНЫХ ДНЕЙ ДЛЯ РЕГЛАМЕНТНЫХ РАБОТ В ЦЕНТРЕ СЕРТИФИКАЦИИ MICROSOFT	279
Алферов И.Л.	
МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ КЛИЕНТОВ ПРИ ДОСТУПЕ К ИНФОРМАЦИИ В ОБЪЕКТНЫХ СЕТЯХ ХРАНЕНИЯ ДАННЫХ	281
Чернокозинский С.А.	
К ВОПРОСУ О МОДЕЛИРОВАНИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ	284
Бондарь А.М., Меньшенин А.О.	
ДОЛГОВРЕМЕННОЕ ОБЕСПЕЧЕНИЕ ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ.....	286
Гаврильченко Р.Ю., Лаврентьев Н.П.	
ЦИФРОВАЯ СИСТЕМА СВЯЗИ, ОСНОВАННАЯ НА ПРОГРАММНОЙ МАНИПУЛЯЦИИ ТОКОМ ПОТРЕБЛЕНИЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА	288
Гилев А.М.	
МОДЕЛИРОВАНИЕ РЕЧЕВОГО СИГНАЛА СУПЕРПОЗИЦИЕЙ ВЕЙВЛЕТОВ МОРЛЕ В ЗАДАЧАХ ЕГО ЗАЩИТЫ.....	290
Дубовицкая М.В.	
ПОСТРОЕНИЕ СИСТЕМЫ МОБИЛЬНОГО БЕЗОПАСНОГО ДОСТУПА К ИНФОРМАЦИИ НА БАЗЕ JAVA ME.....	291
Липовецкий В.Ю.	
ПОСТРОЕНИЕ И ПРОВЕРКА ПУТЕЙ СЕРТИФИКАЦИИ В ИНФРАСТРУКТУРАХ ОТКРЫТЫХ КЛЮЧЕЙ.....	293
Лучник А.И., Меньшенин А.О.	
РАЗРАБОТКА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ВЗАИМОДЕЙСТВИЯ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ С УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ.....	295
Любка А.А.	
ПОСТРОЕНИЕ РАСПРЕДЕЛЕННЫХ СИСТЕМ БЕЗОПАСНОСТИ НА БАЗЕ АГЕНТНЫХ ПЛАТФОРМ.....	297
Матросов А.А.	
ФОРМАТ СИГНАТУРЫ ДЛЯ ВЫЯВЛЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ И КОРРЕКТНОЙ РЕАКЦИИ НА НИХ	298

Кишук А.Ю.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ И БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ.....	300
--	-----

Кишук А.Ю.

МОДЕЛИРОВАНИЕ БИОМЕТРИЧЕСКИХ УСТРОЙСТВ, ОБЕСПЕЧИВАЮЩЕГО ВЫСОКИЙ УРОВЕНЬ ЗАЩИТЫ ОБЪЕКТОВ ДОСТУПА	302
---	-----

Момот М.В.

ТЕХНОЛОГИЯ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДЕНЕГ	304
---	-----

Сеченов С.Ю.

ФОРМИРОВАНИЕ КРИПТОГРАФИЧЕСКИ ЗАЩИЩЕННОЙ ЭЛЕКТРОННОЙ ПОЧТОВОЙ СЕТИ.....	306
--	-----

Федосеев А.М.

ИССЛЕДОВАНИЕ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ГОСТ 34.10-2001	308
--	-----

Научное издание

Научная сессия ТУСУР – 2006

Материалы

Всероссийской научно-технической конференции
студентов, аспирантов и молодых специалистов

4–7 мая 2006 года, Томск, Россия

В пяти частях

Часть 2

**Печатается без редактирования по текстам,
предоставленным авторами**

Верстка **В.М. Бочкаревой**

Дизайн обложки **В.Глушко**

Издательство «В-Спектр»

Сдано на верстку 04.04.2006. Подписано к печати 25.04.2006.

Формат 60×84¹/₁₆. Печать трафаретная.

Печ. л. 19. Усл. печ. 18,6.

Тираж 150 экз. Заказ 14.

Тираж отпечатан в издательстве «В-Спектр»

ИНН/КПП 7017129340/701701001, ОГРН 1057002637768
634055, г. Томск, пр. Академический, 13-24, Тел. 49-09-91.

E-mail: bmwm@list.ru