Федеральное агентство по образованию

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Посвящается
памяти профессора В.П. Бондаренко

НАУЧНАЯ СЕССИЯ ТУСУР-2007

Материалы докладов
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР-2008»
5–8 мая 2008 г.

В пяти частях

Часть 3

Тематический выпуск
«СИСТЕМНАЯ ИНТЕГРАЦИЯ И БЕЗОПАСНОСТЬ»

В-Спектр
Томск 2008

УДК 621.37/.39+681.518 (063)
ББК 32.84я431+32.988я431

Научная сессия ТУСУР-2008: Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. Тематический выпуск «Системная интеграция и безопасность». Томск, 5–8 мая 2008 г.: В пяти частях. Ч. 3. – Томск: В-Спектр, 2008. – 248 с.

ISBN 978-5-91191-080-8
ISBN 978-5-91191-083-9 (Ч. 3)

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, сетей электро- и радиосвязи, 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 и защиты информации. Представлены материалы по математическому моделированию в технике, экономике и менеджменте, по антикризисному управлению, автоматизации управления в технике и образовании. Широкому кругу читателей будет доступна информация о социальной работе в современном обществе, о философии и специальной методологии, экологии, о мониторинге окружающей среды и безопасности жизнедеятельности, инновационных, студенческих идеях и проектах.

УДК 621.37/.39+681.518 (063)
ББК 32.84я431+32.988я431

ISBN 978-5-91191-080-8
ISBN 978-5-91191-083-9 (Ч. 3)

Вступление

Настоящий сборник трудов посвящается памяти профессора, доктора технических наук, член-корр. Академии наук высшей школы Бондаренко Владимира Петровича.

Этот удивительно тактичный и интеллигентный человек был прекрасным педагогом, исследователем, ученым, многие годы он проработал в нашем научно-педагогическом коллективе кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС). Высочайшая научная эрудиция позволяла Владимиру Петровичу с легкостью решать самые сложные научные проблемы. Однако главной целью, темой его жизни было создание теоретических основ построения диалоговых систем, учитывающих особенности формирования и восприятия речи человеком. Работа над этой сложнейшей, еще не разрешенной проблемой, потребовала от профессора В.П. Бондаренко и его учеников решить следующие задачи: формирование концепции пространства состояний модели мира человека для определения текущей точки диалога; создание и исследование алгоритмов автоматической обработки речевого сигнала аналогично слуховой системе человека; исследование алгоритмов синтеза речи по правилам; исследование биологической обратной связи, возникающей при формировании просодии высказывания и учет ее по каналам: слуховому, костному, прогнозирующему; создание взаимодействующих моделей мира субъектов диалога на различных уровнях иерархии: физическом, синтаксическом, семантическом, прагматическом.

К сожалению, ему не удалось решить все перечисленные задачи в полном объеме. Мужественно сражаясь со страшной болезнью, он умер осенью 2007 года… Однако профессор В.П. Бондаренко заложил крепкий научный фундамент для продвижения смелых и, как оказалось, правильных идей.

Наш сборник трудов «Системная интеграция и безопасность» становится традиционным, и это не может не радовать.

В этот раз сборник является своеобразной трибуной в основном для молодых исследователей, которые только отыскивают свое место в мире научного познания.

В тематический выпуск «Системная интеграция и безопасность» включены доклады секций 10 и 12 «Научной сессии ТУСУР-2008», которые отражают научные интересы профессорско-преподавательского состава, аспирантов и студентов кафедры КИБЭВС и Центра технологий безопасности. Представлены доклады студентов и аспирантов других специальностей и вузов России, работающих над вопросами автоматизации технологических процессов, информационной безопасностью и защитой информации, отражают различные аспекты научных направлений, которые интенсивно и традиционно развиваются на кафедре КИБЭВС: разработка, изучение и внедрение в клиническую практику новых методов топической диагностики и аппаратуры для хирургического лечения; методы и системы защиты информации; информационная безопасность.

В докладах представлены результаты разработки интеллектуальных систем в области информационной безопасности автоматизированных систем, компьютерной безопасности, автоматизации, управления производства, образования, медицины. Ряд докладов посвящены речевым технологиям. Учитывается важный аспект безопасности – комплексность. Важным обстоятельством является то, что ряд представленных докладов стали возможны благодаря участию студентов, аспирантов и молодых ученых в работе над наукоемкими, инновационно-привлекательными проектами и бизнес-идеями, которые выполняются на кафедре КИБЭВС в рамках группового проектного обучения (ГПО). Система ГПО развивается на кафедре КИБЭВС согласно реализации ТУСУРом инновационной образовательной программы «Разработка и внедрение в практику системы подготовки специалистов, обеспечивающей генерацию новой массовой волны предпринимателей наукоемкого бизнеса» национального проекта России «Образование».

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

Всероссийская научно-техническая конференция студентов и молодых ученых «Научная сессия ТУСУР – 2008» 5–8 мая 2008 г.

ПРОГРАММНЫЙ КОМИТЕТ

- **Кобзев А.В.** – председатель, ректор ТУСУР, д.т.н., профессор
- **Рempe Н.Г.** – сопредседатель, проректор по НР ТУСУР, д.т.н., профессор
- **Шурыгин Ю.А.** – первый проректор ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор
- **Ехлаков Ю.П.** – проректор по информатизации ТУСУР, д.т.н., профессор
- **Уваров А.Ф.** – проректор по экономике ТУСУР, к.э.н.
- **Малютин** Н.Д. – заместитель проректора по НР ТУСУР, д.т.н., профессор
- **Казьмин Г.П.** – нач. отдела по инновационной деятельности Администрации г. Томска, к.т.н.
- **Малюк А.А.** – декан фак-та информационной безопасности МИФИ, к.т.н., г. Москва
- **Беляев Б.А.** – зав. лабораторией электродинамики Ин-та физики СО РАН, д.т.н., г. Красноярск
- **Разинкин В.П.** – к.т.н., доцент каф. ТОР НГТУ, г. Новосибирск
- **Лукин В.П.** – директор отд. распространения волн, почетный член Американского оптического общества, д.ф.-м.н., профессор, Ин-т оп-

тики атмосферы СО РАН, г. Томск

- **Кориков А.М.** – зав. каф. АСУ ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор
- **Московченко А.Д.** – зав. каф. философии ТУСУР, д.ф.н., профессор
- **Шарыгин Г.С.** – зав. каф. РТС ТУСУР, д.т.н., профессор
- **Пустынский И.Н.** – зав. каф. ТУ ТУСУР, заслуженный деятель науки и техники РФ, д.т.н., профессор
- **Шелупанов А.А.** – зав. каф. КИБЭВС ТУСУР, д.т.н., профессор
- **Пуговкин А.В.** – зав. каф. ТОР ТУСУР, 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 ТУСУР, д.ист.н., профессор

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

- **Ремпе Н.Г.** – председатель, проректор по НР ТУСУР, д.т.н., профессор
- **Ярымова И.А.** – зам. председателя, заведующий ОППО ТУСУР, к.б.н.
- **Акулиничев Ю.П.** - председатель совета по НИРС РТФ, д.т.н., профессор каф. РТС ТУСУР
- **Еханин С.Г.** – председатель совета по НИРС РКФ, д.ф.-м.н., профессор каф. КУДР ТУСУР
- **Коцубинский В.П.** – председатель совета по НИРС ФВС, зам. зав. каф. КСУП ТУСУР, к.т.н., доцент
- **Мицель А.А.** – председатель совета по НИРС ФСУ, д.т.н., профессор каф. АСУ ТУСУР
- **Орликов Л.Н.** – председатель совета по НИРС ФЭТ, д.т.н., профессор каф. ЭП ТУСУР
- **Казакевич Л.И.** – председатель совета по НИРС ГФ, к.ист.н., доцент каф. ИСР ТУСУР
- **Куташова Е.А.** – секретарь оргкомитета, инженер ОППО ТУСУР, к.х.н.

ЭКСПЕРТНЫЙ КОМИТЕТ

- **Рempe Н.Г.** – председатель, проректор по НР ТУСУР, д.т.н., профессор
- **Малютин Н.Д.** – заместитель проректора по НР ТУСУР, д.т.н., профессор
- **Уваров А.Ф.** – проректор по экономике ТУСУР, к.э.н.
- **Казьмин Г.П.** – нач. отдела по инновационной деятельности администрации г. Томска, к.т.н.
- **Авдзейко В.И.** – зам. руководителя НИЧ ТУСУР, к.т.н.
- **Шелупанов А.А.** – зав. каф. КИБЭВС, д.т.н., профессор
- **Мещеряков Р.В.** – к.т.н., доцент каф. КИБЭВС
- Представители фонда Бортника (по согласованию), г. Москва

Конференция **«Научная сессия ТУСУР – 2008»** вошла в число аккредитованных мероприятий по Программе «Участник молодежного научно-инновационного конкурса» (У.М.Н.И.К.) Фонда содействия развитию малых форм предприятий в научно-технической сфере (МП НТС) при поддержке Роснауки и Рособразования (фонд Бортника) (**http://www.fasie.ru/**).

Экспертным комитетом конференции при работе секции «У.М.Н.И.К.» будут отобраны молодые (до 28 лет включительно) ее участники – победители в номинации «За научные результаты, обладающие существенной новизной и среднесрочной (до 5–7 лет) перспективой их эффективной коммерциализации» с последующим финансированием проектов НИОКР.

ПОРЯДОК РАБОТЫ, ВРЕМЯ И МЕСТО ПРОВЕДЕНИЯ

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

Конференция проводится
с 5 по 8 мая 2008 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 **5 мая с 9:00 до 10:00**.

СЕКЦИИ КОНФЕРЕНЦИИ

Секция 1. РАДИОТЕХНИЧЕСКИЕ СИСТЕМЫ И РАСПРОСТРАНЕНИЕ РАДИОВОЛН – *председатель* ***Шарыгин Герман Сергеевич,*** *зав. каф. РТС, д.т.н., профессор; зам. председателя* ***Тисленко Владимир Ильич,*** *к.т.н., доцент каф. РТС*

Секция 2. ЗАЩИЩЕННЫЕ ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ – *председатель* ***Голиков Александр Михайлович,*** *к.т.н., доцент каф. РТС*

Секция 3. АУДИОВИЗУАЛЬНАЯ ТЕХНИКА, БЫТОВАЯ РАДИОЭЛЕКТРОННАЯ АППАРАТУРА И СЕРВИС – *председатель* ***Пустынский Иван Николаевич,*** *зав. каф. ТУ, д.т.н., профессор; зам. председателя* ***Костевич Анатолий Геннадьевич,*** *к.т.н., доцент каф. ТУ*

Секция 4. ПРОЕКТИРОВАНИЕ И ТЕХНОЛОГИИ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ. ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ РАДИООБОРУДОВАНИЯ – *председатель* ***Масалов Евгений Викторович,*** *д.т.н., профессор каф. КИПР, зам. председателя* ***Михеев Евгений Николаевич,*** *м.н.с.*

Подсекция 4.1. ПРОЕКТИРОВАНИЕ БИОМЕДИЦИНСКОЙ АППАРАТУРЫ – *председатель* ***Еханин Сергей Георгиевич,*** *д.ф.-м.н., профессор каф. КУДР, зам. председателя* ***Молошников Василий Анатольевич,*** *аспирант каф. КУДР*

Подсекция 4.2. КОНСТРУИРОВАНИЕ И ПРОИЗВОДСТВО РАДИОЭЛЕКТРОННЫХ СРЕДСТВ – *председатель* ***Михеев Евгений Николаевич,*** *м.н.с.*

Секция 5. ИНТЕГРИРОВАННЫЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ – *председатель* ***Катаев Михаил Юрьевич,*** *д.т.н., профессор каф. АСУ, зам. председателя* ***Бойченко Иван Валентинович,*** *к.т.н., доцент каф. АСУ*

Секция 6. КВАНТОВАЯ, ОПТИЧЕСКАЯ И НАНОЭЛЕКТРОНИКА – *председатель* ***Шарангович Сергей Николаевич,*** *зав. каф. СВЧиКР, к.ф.-м.н., доцент; зам. председателя* ***Буримов Николай Иванович,*** *к.т.н., доцент каф. ЭП*

Секция 7. ФИЗИЧЕСКАЯ И ПЛАЗМЕННАЯ ЭЛЕКТРОНИКА – *председатель* ***Троян Павел Ефимович,*** *зав. каф. ФЭ, д.т.н., профессор*

Секция 8. РАСПРЕДЕЛЁННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ – *председатель* ***Ехлаков Юрий Поликарпович,*** *проректор по Информатизации ТУСУР, зав. каф. АОИ, д.т.н., профессор; зам. председателя* ***Сенченко Павел Васильевич,*** *к.т.н., доцент каф. АОИ*

Секция 9. ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ – *председатель* ***Ходашинский Илья Александрович,*** *д.т.н., проф. каф. АОИ; зам. председателя* ***Лавыгина Анна Владимировна,*** *аспирант каф. АОИ*

Секция 10. АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ – *председатель* ***Давыдова Елена Михайловна,*** *к.т.н., ст. преподаватель каф. КИБЭВС; зам. председателя* ***Конев Антон Александрович,*** *к.т.н. каф. КИБЭВС*

Секция 11. АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА В СИСТЕМАХ УПРАВЛЕНИЯ И ПРОЕКТИРОВАНИЯ – *председатель* ***Шурыгин Юрий Алексеевич,*** *первый проректор ТУСУР, зав. каф. КСУП, д.т.н., профессор; зам. председателя* ***Коцубинский Владислав Петрович,*** *зам. зав. каф. КСУП, к.т.н., доцент*

Подсекция 11.1. ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ПРОЕКТИРОВАНИЯ ТЕХНИЧЕСКИХ УСТРОЙСТВ – *председатель* ***Черкашин Михаил Владимирович,*** *к.т.н., ст. преподаватель каф. КСУП*

Подсекция 11.2. АДАПТАЦИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ИМИТАЦИИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ – *председатель* ***Коцубинский Владислав Петрович,*** *зам. зав. каф. КСУП, к.т.н., доцент*

Подсекция 11.3. ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ПОДДЕРЖКИ СЛОЖНОГО ПРОЦЕССА – *председатель* ***Хабибуллина Надежда Юрьевна,*** *к.т.н., ст. преподаватель каф. КСУП*

Подсекция 11.4. МЕТОДЫ СТЕРЕОСКОПИЧЕСКОЙ ВИЗУАЛИЗАЦИИ – *председатель* ***Дорофеев Сергей Юрьевич,*** *аспирант каф. КСУП*

Секция 12. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – *председатель* ***Шелупанов Александр Александрович,*** *зав. каф. КИБЭВС, д.т.н., профес-*

сор; зам. председателя ***Мещеряков Роман Валерьевич,*** *к.т.н., доцент каф. КИБЭВС*

Секция 13. ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И УСТРОЙСТВА – *председатель* ***Светлаков Анатолий Антонович,*** *зав. каф. ИИТ, д.т.н., профессор; зам. председателя* ***Шидловский Виктор Станиславович,*** *к.т.н., доцент каф. ИИТ*

Секция 14. РАДИОТЕХНИКА – *председатель* ***Титов Анатолий Александрович,*** *д.т.н., профессор каф. РЗИ; зам. председателя* ***Семенов Эдуард Валерьевич,*** *к.т.н., доцент каф. РЗИ;*

Секция 15. ПРОМЫШЛЕННАЯ ЭЛЕКТРОНИКА – *председатель* ***Михальченко Геннадий Яковлевич****, д.т.н., профессор каф. ПрЭ; зам. председателя* ***Семенов Валерий Дмитриевич,*** *зам. зав. каф. ПрЭ по НР, к.т.н., доцент каф. ПрЭ*

Подсекция 15.1. СИЛОВАЯ И ИНФОРМАЦИОННАЯ ЭЛЕКТРОНИКА В СИСТЕМАХ ПРЕОБРАЗОВАНИЯ ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ И АВТОМАТИЗАЦИИ – *председатель* ***Михальченко Геннадий Яковлевич****, д.т.н., профессор каф. ПрЭ; зам. председателя* ***Семенов Валерий Дмитриевич,*** *зам. зав. каф. ПрЭ по НР, к.т.н., доцент каф. ПрЭ*

Подсекция 15.2. ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ В УСТРОЙСТВАХ ПРОМЫШЛЕННОЙ И СИЛОВОЙ ЭЛЕКТРОНИКИ – *председатель* ***Селяев Александр Николаевич****, д.т.н., профессор каф. ПрЭ; зам. председателя* ***Шевелев Михаил Юрьевич,*** *к.т.н., доцент каф. ПрЭ*

Секция 16. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ В ТЕХНИКЕ, ЭКОНОМИКЕ И МЕНЕДЖМЕНТЕ – *председатель* ***Мицель Артур Александрович,*** *д.т.н., профессор каф. АСУ; зам. председателя* ***Зариковская Наталья Вячеславовна,*** *к.ф.-м.н., доцент каф. ФЭ*

Подсекция 16.1. МОДЕЛИРОВАНИЕ В ЕСТЕСТВЕННЫХ И ТЕХНИЧЕСКИХ НАУКАХ – *председатель* ***Зариковская Наталья Вячеславовна,*** *к.ф.-м.н., доцент каф. ФЭ*

Подсекция 16.2. МОДЕЛИРОВАНИЕ, ИМИТАЦИЯ И ОПТИМИЗАЦИЯ В ЭКОНОМИКЕ – *председатель* ***Мицель Артур Александрович,*** *д.т.н., профессор каф. АСУ; зам. председателя* ***Ефремова Елена Александровна,*** *аспирант каф. АСУ*

Подсекция 16.3. ИНФОРМАЦИОННЫЕ СИСТЕМЫ МЕНЕДЖМЕНТА – *председатель* ***Сергеев Виктор Леонидович,*** *д.т.н., профессор каф. АСУ*

Секция 17. ЭКОНОМИКА И УПРАВЛЕНИЕ – *председатель* ***Осипов Юрий Мирзоевич,*** *зав. отделением каф. ЮНЕСКО при ТУСУР, д.э.н., д.т.н., профессор; зам. председателя* ***Василевская Наталия Борисовна,*** *к.э.н., доцент каф. экономики*

Секция 18. АНТИКРИЗИСНОЕ УПРАВЛЕНИЕ – *председатель* ***Семиглазов Анатолий Михайлович,*** *д.т.н., профессор каф. ТУ; зам. председателя* ***Бут Олеся Анатольевна,*** *ассистент каф. ТУ*

Секция 19. ЭКОЛОГИЯ И МОНИТОРИНГ ОКРУЖАЮЩЕЙ СРЕДЫ – *председатель* ***Карташев Александр Георгиевич,*** *д.б.н., профессор каф. РЭТЭМ*

Секция 20. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ – *председатель* ***Хорев Иван Ефимович,*** *д.т.н., профессор каф. РЭТЭМ; зам. председателя* ***Полякова Светлана Анатольевна,*** *к.б.н., доцент каф. РЭТЭМ*

Секция 21. АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНОЙ РАБОТЫ В СОВРЕМЕННОМ ОБЩЕСТВЕ – *председатель* ***Грик Николай Антонович,*** *зав. каф. ИСР, д.ист.н., профессор; зам. председателя* ***Казакевич Людмила Ивановна,*** *к.ист.н., доцент каф. ИСР*

Секция 22. ФИЛОСОФИЯ И СПЕЦИАЛЬНАЯ МЕТОДОЛОГИЯ – *председатель* ***Московченко Александр Дмитриевич,*** *зав. каф. философии, д.ф.н., профессор; зам. председателя* ***Раитина Маргарита Юрьевна,*** *к.ф.н., доцент каф. философии*

Секция 23. ИННОВАЦИОННЫЕ ПРОЕКТЫ, СТУДЕНЧЕСКИЕ ИДЕИ И ПРОЕКТЫ – *председатель* ***Уваров Александр Фавстович,*** *проректор по экономике ТУСУР, к.э.н.; зам. председателя* ***Чекчеева Наталья Валерьевна,*** *зам. директора студенческого Бизнес-инкубатора (СБИ), к.э.н.*

Секция 24. АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ В ТЕХНИКЕ И ОБРАЗОВАНИИ – *председатель* ***Дмитриев Вячеслав Михайлович,*** *зав. каф. ТОЭ, д.т.н., профессор; зам. председателя* ***Андреев Михаил Иванович,*** *к.т.н., доцент ВКИЭМ*

Секция 25. ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ ШКОЛЬНИКОВ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – *председатель* ***Корнеева Татьяна Борисовна,*** *заместитель директора по методической работе ОЦ «Школьный университет»; зам. председателя* ***Нехорошева Юлия Геннадьевна,*** *начальник учебно-методического отдела ОЦ «Школьный университет», к.т.н., доцент*

Секция 26. СИСТЕМЫ И СЕТИ ЭЛЕКТРО- И РАДИОСВЯЗИ – *председатель* ***Пуговкин Алексей Викторович,*** *зав. каф. ТОР, д.т.н., профессор, к.т.н.; зам. председателя* ***Демидов Анатолий Яковлевич,*** *к.т.н., доцент каф. ТОР*

Материалы научных докладов,
представленные на конференцию, опубликованы в сборнике
«НАУЧНАЯ СЕССИЯ ТУСУР – 2008»
в пяти частях

1-я часть сборника включает доклады 1–7-й секций;
2-я часть – доклады 8, 9, 11, 13, 14, 15-й секций;
3-я часть – доклады 10 и 12-й секции;
4-я часть – доклады 16–18-й секций;
5-я часть – доклады 19–26-й секций.

Адрес оргкомитета:

634050, Россия, г. Томск,
пр. Ленина, 40, ГОУ ВПО «ТУСУР»,
Научное управление (НУ), к. 205
Тел.: 8-(3822)-51-47-57, 52-79-42
E-mail: eak@main.tusur.ru

СЕКЦИЯ 10

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

*Председатель – **Е.М. Давыдова**, к.т.н., доцент каф. КИБЭВС;*
*зам. председателя – **А.А. Конев**, к.т.н. доцент каф. КИБЭВС*

АНИМАЦИЯ РЕЧИ

М.С. Агапов, студент 4-го курса; Р.В. Мещеряков, доцент, к.т.н.
ТУСУР, г. Томск, ams@sibmail.com

Синтез речевого сигнала по печатному тексту является одной из «классических» задач в области обработки естественного языка и искусственного интеллекта. Кроме того, представляют интерес и сопутствующие задачи, формирующие идеологию «дружественного» интерфейса с компьютером. Одной из таких задач является визуализация процесса произнесения текста, как это делал бы человек.

Целью проекта является разработка и реализация системы анимации человеческой речи. Особое внимание будет уделено визуализации артикуляционных особенностей произношения.

Предполагается на первоначальном этапе использовать графическую модель человеческого лица в модели графического 3D редактора. Соответственно должно быть разработано алгоритмическое и программное обеспечение, которое будет управлять созданной графической моделью.

На вход системы подается файл, содержащий текст. На выходе получается изображение модели человеческого лица, проговаривающего входной текст (см. рисунок).

Управление графической моделью происходит на основе подаваемого программе текста. Программа управления считывает текст из заданного файла, а также управляющие команды по положению органов артикуляции и речеобразующего тракта; в зависимости от встречаемых команд задает положение намеченных точек у графической модели. Таким образом, создается визуальное впечатление проговаривания текста виртуальным лицом.

Очевидно, что возможно использование данной системы совместное с программами, озвучивающими текст. Это будет способствовать наиболее легкому восприятию информации и расширит сферу применения речевых технологий.

Данная система может применяться, например, для вещания с Интернет-сайтов – так называемые виртуальные ведущие. А также для анимации персонажей при разработке компьютерных игр и др.

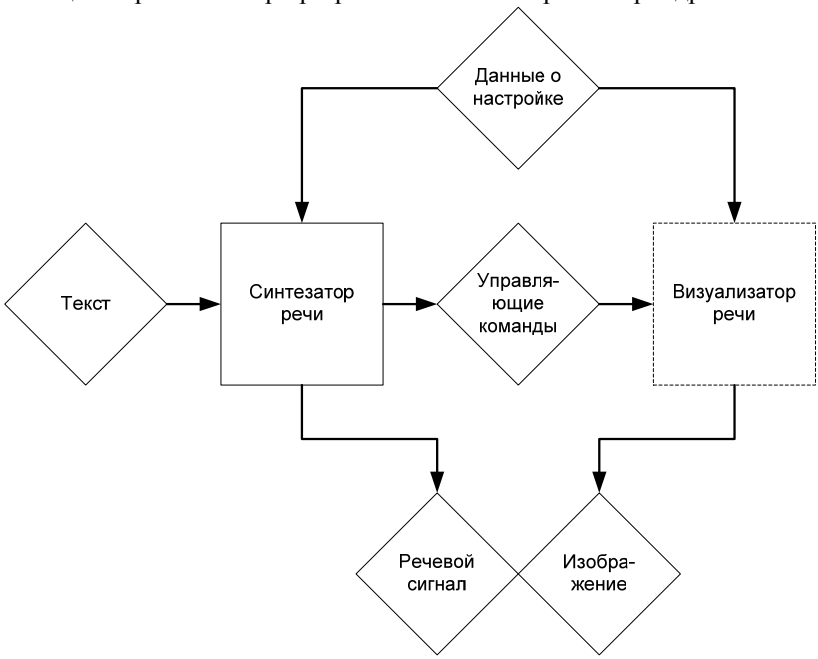


Схема аниматора речи

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ДОГОВОРОВ И ДОПОЛНИТЕЛЬНЫХ СОГЛАШЕНИЙ

Ю.С. Барисенок, студент 5-го курса
ТУСУР, г. Томск, Barissska@mail.ru

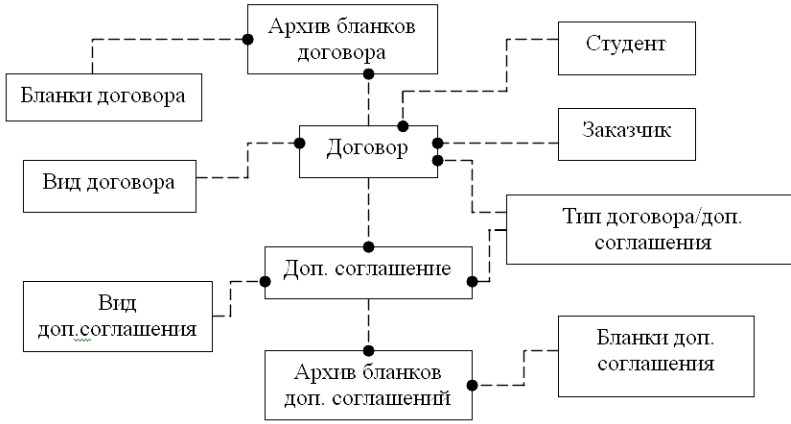
Целью данной работы является разработка автоматизированной системы учета договоров и дополнительных соглашений студентов для филиала ТУСУРа в г. Сургут.

Эта система должна обеспечить хранение и управление данными по договорам, дополнительным соглашениям, заказчикам, сметам, студентам, обучающимся с полным возмещением затрат.

В настоящее время часть документов представлена в бумажном виде, часть ведется в EXCEL, которая не дает таких возможностей, как ра-

бота по сети, многоуровневый доступ, хранение измененных данных, ведение архивов.

Вся информация в автоматизированной системе организована базой данных. Модель «сущность-связь» приведена на рисунке. База данных находится под управлением СУБД FireBird. Программная часть автоматизированной системы разрабатывается в среде Delphi.



Модель «сущность–связь»

Литература

1. *Ковязин А.Н., Востриков С.М.* Архитектура, администрирование и разработка приложений баз данных в InterBase Firebird Yaffil. Кудиц-Образ. М., 2002. 432 с.

2. *Архангельский А.Я.* Программирование в Delphi 7. М.: ООО «Бином-Пресс», 2003. 1152 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ДОКУМЕНТОВ ОПЛАТЫ И СМЕТ

К.Ю. Барняков, студент 5-го курса

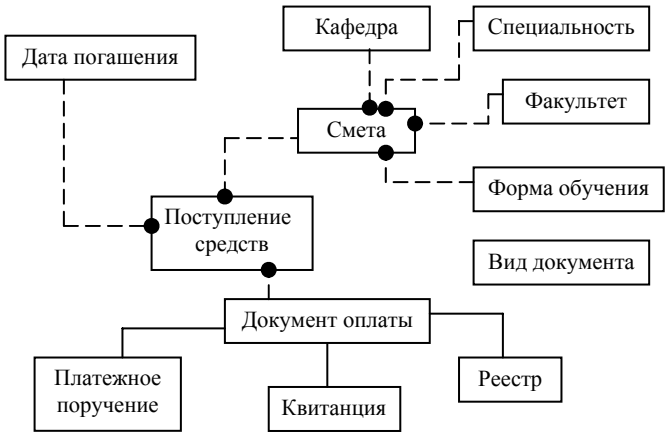
ТУСУР, г. Томск, Oskar1986@rambler.ru

Целью работы является разработка базы данных для автоматизированной системы учета документов оплаты и смет для филиала ТУСУРа в г. Сургут.

Система должна обеспечить хранение и управление данными по студенту, документами оплаты, сметами, отчислениями, платежными поручениями, квитанциями, реестрами.

В настоящее время в ТУСУРе уже существует автоматизированная система «Контингент», которая удовлетворяет всем требованиям, но, к сожалению, нет возможности пользоваться ей в Сургуте. Поэтому часть документов представлена в бумажном виде, часть ведется в EXCEL, которая не дает таких возможностей, как работа по сети, многоуровневый доступ, хранение измененных данных, ведение архивов.

Вся информация в автоматизированной системе организована базой данных. Модель «сущность-связь» приведена на рисунке. База данных находится под управлением СУБД FireBird. Программная часть автоматизированной системы разрабатывается в среде Delphi.



Модель «сущность–связь»

Литература

1. *Ковязин А.Н., Востриков С.М.* Архитектура, администрирование и разработка приложений баз данных в InterBase Firebird Yaffil. Кудиц-Образ. Москва 2002. 432 с.

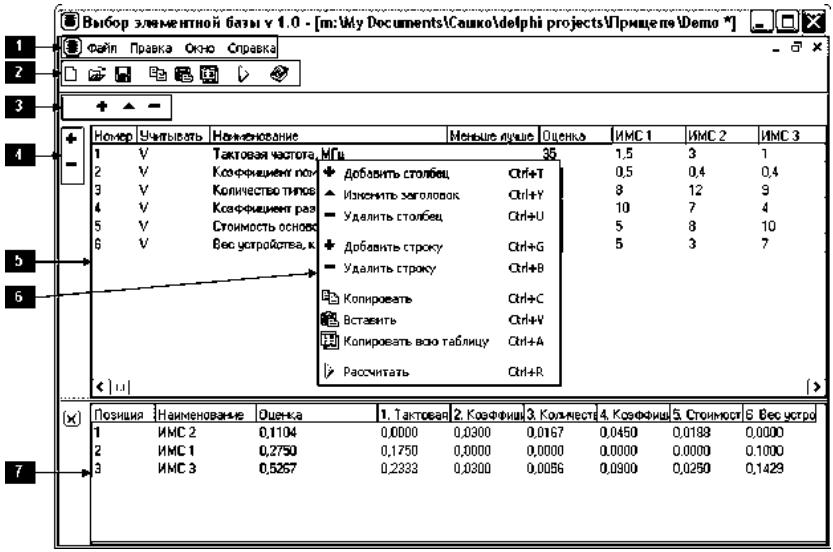
2. *Архангельский А.Я.* Программирование в Delphi 7. М.: ООО Бином-Пресс, 2003. 1152 с.

3. *Грабер М.* Введение в SQL. М.: Лори. 1996.

РЕАЛИЗАЦИЯ МЕТОДИКИ ВЫБОРА ЭЛЕМЕНТНОЙ БАЗЫ

А.С. Бондаренко, А.А. Николаев, студенты, 3-го и 5-го курсов
КИБЭВС, ТУСУР, г. Томск, boalse@yandex.ru

На рисунке представлен внешний вид пользовательского интерфейса реализованной программы.



Пользовательский интерфейс программы

Главное меню. В нем содержатся списки всех возможных команд для управления приложением.

Панель инструментов. Здесь сдублированы наиболее полезные команды из главного меню, предназначенные для работы с приложением, для более быстрого вызова этих команд.

Панель редактирования столбцов таблицы исходных данных (далее просто «Панель столбцов»). На этой панели сдублированы команды из главного меню над столбцами таблицы «5».

Панель редактирования строк таблицы исходных данных (далее просто «Панель строк»). На этой панели сдублированы команды из главного меню над строками таблицы «5».

Таблица исходных данных. В эту таблицу пользователем вводятся исходные данные, на основании которых в дальнейшем производится расчет.

Контекстное меню. Появляется при нажатии правой кнопки «мыши» на элементах «5» или «7». В контекстном меню сдублированы некоторые команды главного меню для более удобной работы с выделенным элементом.

Таблица результатов. Эта таблица появляется только после ввода исходных данных и проведения расчетов, в ней отражены результаты проделанных расчетов.

После запуска приложения доступны только два пункта главного меню: «Файл» и «Справка». В меню «Файл» доступны только две команды: «Создать» и «Открыть…». После успешного выполнения одной из этих команд откроется новое окно, в котором можно вносить и редактировать исходные данные и выполнять на их основании расчет. Также станут доступными пункты главного меню «Правка», «Окно» и новые кнопки на панели инструментов.

При помощи команд «Создать» и «Открыть…» можно создавать и открывать сколько угодно файлов для расчетов, каждый файл будет открываться в новом окне.

Исходные данные вводятся в соответствующую таблицу. В строки таблицы заносятся характеристики параметров, по которым будут сравниваться электрические элементы, а также сами значения для каждого элемента. Зеленые колонки – характеристики параметров, белые колонки – характеристики электрических элементов.

Чтобы добавить строку, можно воспользоваться кнопками на панели строк, либо командами из главного или контекстного меню. При добавлении строки система запросит название параметра, которое введется в колонку «Наименование» и при желании его потом можно будет изменить. Колонка «Номер» хранит порядковый номер параметра в таблице. В колонке «Учитывать» отражается флаг, учитывать ли данный параметр при расчетах: если флаг (галочка) не установлен, то параметр будет игнорироваться при расчете. Если по какому-то параметру меньшее значение соответствует лучшему элементу (например, параметр «Цена», чем элемент дешевле, тем он для нас лучше), то в колонке «Меньше лучше» должен быть установлен флаг.

В колонке «Оценка» отражается оценка важности данного параметра по отношению к самому важному. Самый важный параметр должен иметь самую высокую оценку. Его пользователь выбирает сам, все остальные параметры имеют оценку меньшую или равную максимальной. Сумма оценок всех учитываемых параметром не должна равняться нулю. Параметры с нулевой оценкой игнорируются при расчете.

Одновременно с добавлением строк можно добавлять столбцы, в которых фиксируются названия сравниваемых элементов и их характеристики по каждому из параметров. Чтобы добавить столбец, можно воспользоваться кнопками на панели столбцов, либо командами из главного или контекстного меню. При добавлении столбца система запросит название параметра, которое введется в заголовок столбца, и при желании его можно будет изменить, используя соответствующую команду. Ни одно значение в белых столбцах не должно равняться нулю. Возможен ввод отрицательных значений. Количество строк и столбцов в таблице практически не ограничено.

После ввода исходных данных можно выполнить команду «Рассчитать», при этом откроется таблица результатов, в которой будут представлены электрические элементы в порядке ухудшения их оценки. Общая оценка элемента отражается в колонке с соответствующим именем. Чем больше оценка элемента, тем хуже элемент, чем выше элемент находится в таблице результатов, тем он лучше. В столбцах белого цвета представлена оценка по каждому из параметров. Сумма оценок для элемента по всем параметрам дает общую оценку.

Если таблица окрашена в оттенках красного цвета и над ней отображено сообщение «Возможно, исходные данные были измены, результаты расчетов могут быть неактуальны!», то можно провести расчет заново на обновленных исходных данных, чтобы результаты опять стали актуальными.

Если данные из какой-либо таблицы нужно перенести в другое приложение, то, используя команды главного или контекстного меню «Копировать», «Копировать всю таблицу», можно перенести выделенный фрагмент таблицы или все ее содержание в буфер обмена, а из буфера обмена вставить в нужное приложение.

Литература

1. *Прищепа Л.С.* Аппаратные средства вычислительной техники. Разд. 5. М.: В-Спектр, 2006. 154 с.

ИССЛЕДОВАНИЕ СИСТЕМЫ ЧПУ КООРДИНАТОГРАФОМ С ШАГОВЫМ ДВИГАТЕЛЕМ

А.В. Боталов, Ю.А. Лазарь, студенты 5-го курса ФВС
ТУСУР, г. Томск, office@keva.tusur.ru

Современные системы ЧПУ характеризуются широким применением микро-ЭВМ, микропроцессоров и БИС различного назначения, что, в первую очередь, связано с прогрессом в области вычислительной техники. Встроенная микро-ЭВМ позволяет легко воспринимать информацию от внешних запоминающих устройств или других ЭВМ более высокого уровня. Характерной особенностью ЭВМ является их способность к работе в реальном масштабе времени, т.е. в темпе, диктуемом потребностями объекта управления. Программирование облегчается применением языков высокого уровня и вводом программы с пульта управления.

Координатограф – устройство для автоматического вычерчивания с высокой точностью графического изображения функций, заданных в аналитическом виде. Применяют в картографии, метеорологии, при конструировании, в системах автоматического регулирования и других.

Большинство современных графопостроителей получают информацию непосредственно от ЭВМ или используют данные, хранящиеся на промежуточных носителях информации – перфолентах, перфокартах, магнитных лентах и т.п. Поступившие данные преобразуются в сигналы, управляющие перемещением исполнительного органа – чертежной головки. Основные элементы графопостроителя: средство регистрации (бумага), чертежная головка, привод чертежной головки (электродвигатель) и устройство управления.

Координатограф преобразует вращение ротора шагового двигателя в линейное перемещение исполнительного органа.

В состав координатографа входят два шаговых электродвигателя типа ШД-5Д1М. Через редуктор ШД по оси *X* вращает барабан, на котором закрепляется лист бумаги, по оси *Y* через резьбовой винт перемещает исполнительный орган – каретку с пишущим пером. Один шаг шагового двигателя соответствует линейному перемещению на 0,01 мм.

Барабан и каретка оснащены кулачками, которыми при движении осей нажимается соответствующий конечный выключатель, и в контроллер ШП поступает сигнал. Координатограф оснащен пультом ручного управления с кнопками, сигналы от которых поступают в контроллер ШП.

В системах ЧПУ шаговые двигатели (ШД) применяются и как двигатели, обеспечивающие перемещение исполнительного органа по координатам, и как преобразователи импульсной информации в угол поворота задатчика программы для силовых следящих электро- или гидроприводов.

По принципу действия ШД представляет собой дискретный синхронный двигатель, ротор которого поворачивается дискретно после каждого импульса на входе системы управления и остается неподвижным, когда импульсы не поступают. В системах ЧПУ наибольшее применение нашли индукторные ШД.

Ротор индукторного ШД имеет зубчатую структуру. Зубцами с таким же шагом снабжены полюса статора. Шаг и число зубцов на роторе и полюсах статора выбираются так, чтобы между зубцами ротора и зубцами полюса, который в данный момент не возбужден, существовал сдвиг на 1/3 зубцового шага. Обмотки каждой пары противолежащих полюсов включены последовательно и образуют одну фазу. Поворот ротора ШД осуществляется коммутацией тока в фазах.

При использовании шагового двигателя в системах ЧПУ важное значение имеет оценка его быстродействия при отработке единичного шага. При высоких частотах коммутации токи в обмотках могут не достигать установившихся значений, и электромагнитный момент ШД будет снижен. Чтобы сохранить работоспособность шагового электропривода в таком режиме, необходимо снижать и момент нагрузки.

Максимальный скачок частоты, при котором информация не теряется, называется частотой приемистости шагового электропривода. Обычно максимальная частота режима «равномерного» движения в несколько раз превышает частоту приемистости. Выход шагового электропривода на максимальную скорость должен осуществляться при плавном или ступенчатом нарастании частоты. Это относится и к режимам остановки и снижения скорости. Законы нарастания и спада частоты формируются в программно-задающей части систем ЧПУ устройством разгона-торможения.

ШД имеют более низкие энергетические показатели, чем регулируемые двигатели непрерывного действия. Поэтому применение их на большие моменты нагрузки не всегда целесообразно. Кроме того, с увеличением габаритов ШД снижается допустимая частота, что приводит к увеличению шага при заданной скорости исполнительного органа. Это снижает качество обработки изделий.

Электродвигатель должен разгоняться и работать без сбоев (при импульсной форсировке) – при скачкообразном изменении частоты управляющих импульсов от 0 до 1100 Гц с последующим плавным изменением частоты до 16000 Гц при номинальном моменте инерции нагрузки и вращающем моменте нагрузки не более 0,1 Н×м за время не менее 0,4 с.

Коммутация фаз двенадцатитактная с поочередным включением двух и трех фаз.

Максимальный скачок частоты, при котором информация не теряется, называется частотой приемистости шагового электропривода. Обычно максимальная частота режима «равномерного» движения в несколько раз превышает частоту приемистости. Выход шагового электропривода на максимальную скорость должен осуществляться при плавном или ступенчатом нарастании частоты. Это относится и к режимам остановки и снижения скорости. Законы нарастания и спада частоты формируются в программно-задающей части систем ЧПУ устройством разгона-торможения.

Литература

1. *Дорф Р., Бимор Р.* Современные системы управления. 2004. п. 13/2 (Анализ цифровых систем управления).

2. *Филипс Ч., Харбор Р.* Системы управления с обратной вязью. 2001.

СОЗДАНИЕ И РАЗРАБОТКА САЙТА

Д.М. Брыкова, студент 5-го курса ФВС
КИБЭВС, ТУСУР, г. Томск, 13kalista@sibmail.com

Сайт – это набор из нескольких десятков, сотен или даже тысяч веб-страниц (HTML- или XML-документов), связанных вместе единой темой, общим оформлением, взаимными гипертекстовыми ссылками и, как правило, близким по интернетовским меркам размещением (обычно в пределах одного домена, хотя части сайта вполне могут располагаться на нескольких узловых компьютерах, обслуживаться несколькими серверами и даже принадлежать к разным доменам). Это значит, в частности, что иногда, в зависимости от контекста, один и тот же набор страниц может рассматриваться либо как самостоятельный сайт, либо как часть какого-то другого сайта.

Использование гиперссылок – одно из основополагающих свойств Web-сайтов. Гипертекстовые ссылки, или гиперссылки, или просто ссылки (l*i*nks) – это выделенные области документа («подсвеченные» слова и фразы или выделенные изображения), позволяющие при нажатии на них переходить к другому документу, содержащему связанную информацию. Переход осуществляется вне зависимости от того, где располагается этот документ. С помощью ссылок осуществляется как навигация по сайтам, так и переход на другие сайты.

Навигацией называется система, организующая «путешествие» пользователя по сайту с помощью ссылок, а также переход на другие сайты.

Назначения навигации: помочь пользователю найти то, что он ищет; указать текущее местоположение; помогает понять, что здесь находится; навигация помогает понять, как пользоваться сайтом; от навигации зависит степень доверия пользователей к разработчикам сайта.

Веб-дизайнеры используют термин «постоянная навигация», или «глобальная навигация» для описания навигационных элементов, которые появляются на каждой странице сайта.

Факт того, что навигация появляется в одном и том же месте на каждой странице и имеет при этом одинаковый вид, служит для пользователя мгновенным подтверждением того, что он находится на том же сайте, – а это намного важнее, чем может показаться на первый взгляд. А унификация внешнего вида навигации дает возможность пользователю только один раз узнать, как она работает, и затем уже использовать ее, не задумываясь.

На любом сайте между страницами существуют связи, которые определяют структуру. Основные типы: древовидные (иерархические);

линейные (последовательные); табличные; смешанные (комбинация древовидной и линейной структуры).

Интернет является самым динамично развивающимся средством масс-медиа в истории человечества. За короткий промежуток времени массового использования (6 лет) Всемирная сеть уже насчитывает более 300 млн пользователей во всем мире (по данным Nua Surveys). Наличие огромного числа разнообразных сайтов привело к необходимости их классификации. Поскольку наука об Интернете еще не создана, однозначной классификации на данный момент не существует, и попытки ее синтезировать, как правило, приводят к ее однобокости и нерепрезентативности.

С точки зрения причастности к бизнесу можно разделить все сайты на 2 категории – некоммерческие и коммерческие.

С точки зрения контента, т.е. содержимого сайта, можно выделить много различных групп. В их числе: личные страницы; различные авторские проекты, посвященные хобби или какой-либо сфере интересов; новостные сайты; информационные сайты (содержащие различные статьи и обзоры по определенной теме); корпоративные сайты, направленные на стимулирование получения прибыли в реальном бизнесе; сайты, ориентированные на виртуальный бизнес, т.е. продажи в Сети – интернет-магазины; сайты дистанционного обучения и образования…

Разработку Web-сайта можно разделить на несколько основных этапов: планирование; реализация (разработка информационного наполнения сайта, разработка структуры сайта и структуры отдельно взятой страницы, разработка системы навигации, составление технических заданий на дизайн и программирование, дизайн, программирование, HTML-верстка); тестирование; публикация (подготовка сайта к индексации, выбор доменного имени или дизайн URL, регистрация сайта); рекламирование сайта (виды рекламы); сопровождение сайта.

Литература

1. *Алексеев Ю.М.* Быстро и легко создаем, программируем, шлифуем и раскручиваем web-сайт. М.: Лучшие книги, 2005. 420 с.

БЛОК ОБРАБОТКИ ДАННЫХ С УПРАВЛЯЕМЫМИ ШИНАМИ «МОНТАЖНОЕ ИЛИ»

Ю.Б. Часовникова, А.А. Шилов, студенты ФВС
ТУСУР, КИБЭВС, г. Томск

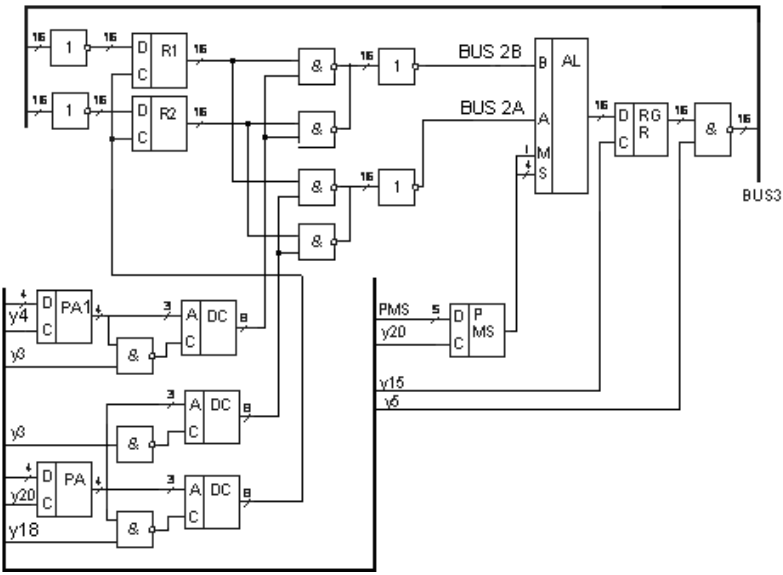
Блок обработки данных является ядром микропроцессорной системы, входит в состав регистрового АЛУ и предназначен для непосредст-

венного исполнения микроопераций. Блок обработки данных структурно подразделяется на файл регистров РОН (R0-R7), приемники из шины BUS3, передатчики на шину BUS3, арифметико-логического устройства (АЛУ), предназначенного для выполнения 16 операций, регистра результата (RGR), регистра кода операции (PMS) и устройства управления. К устройству управления относятся два регистра адреса и два дешифратора (рисунок).

Файл РОН подключается к арифметико-логическому устройству через внутренние шины:

– управляемая шина BUS 2:A с логикой «Монтажное ИЛИ» для передачи в АЛУ первого операнда;

– управляемая шина BUS 2:B для передачи в АЛУ второго операнда команды.



Структурная схема блока обработки данных
с индивидуальными шинами «Монтажное ИЛИ»

Шина BUS3 используется для передачи результатов обработки на регистры РОН (0–7) и возможно в порт ввода-вывода.

В блоке обработки данных используются 8 шестнадцатиразрядных регистров R0-R7, чтение и запись в которые синхронизируются управляющими сигналами y3, y18 соответственно.

Использование логики «Монтажное ИЛИ» в схеме подключения к АЛУ подразумевает одновременную передачу операндов на входы АЛУ. На первом шаге интерпретации команды будет произведено чтение адреса (который записан в поле PMS микрокоманды) второго операнда команды и передача этого операнда на вход управляемой шины BUS 2:B, а на втором шаге подача первого операнда на вход АЛУ, будет произведена по управляемой шине BUS 2:A, синхронизируемой y3.

Регистр кода операции PMS сохраняет и передает дешифрованный код операции на вход кода операции АЛУ. Регистр результата RGR сохраняет результат выполнения операции с выходов АЛУ и загружает данными шину BUS3, откуда их можно передать на регистры РОН или рабочие регистры RA или RD1 и далее в канал

Направление информационных потоков в порт ввода вывода и блок обработки данных различают по старшему разряду адреса a_3 a_2 a_1 a_0 в регистр РА. Если a_3=1 – это указывает на порт ввода-вывода, если a_3=0 – на блок обработки данных.

Для записи данных на регистры, в регистр РА адреса со стороны порта ввода/вывода подается адрес РОН, в который будет производится запись, и управляющий сигнал y18 на вход синхронизации дешифратора, выходы которого соединены со входами синхронизации РОН.

Для чтения данных с регистров, адресуемых РА1 и РА, подается сигнал синхронизации y3 на вход дешифраторов, выходы которых соединены с передатчиками на шину BUS 2:A и BUS 2:Б.

Последовательность обработки данных БОД покажем на примере выполнения команды ADD R1,R2. Пусть R1 = 0101, R2= 0011, тогда микропрограмма интерпретации выглядит следующим образом (табл.).

	Линии микрокомандного канала и биты управления		
	21 20 19 18 17 16 15 14 13 12 11 10 9	87654	321
МКК	y21 y20 y19 y18 y17 y16 y15 y14 y13 y3 y4	PMS	0
МК	y5 y6	00001	PA
1	1 0 0 0 0 0 0 0 0 0 1 0 0	00010	000
2	1 1 0 0 0 0 1 0 0 1 0 0 0	00000	0
3	1 0 0 1 0 0 0 0 0 0 0 1 0		001
			0
			001
			0

1. y4) PA1(8-4):=адрес второго операнда (R1) ; R1=0101.
2. y20) PA(4-1):=адрес первого операнда (R2) ; R2=0011.
   и PMS(8-4):=код операции сложения ; PMS=2.
   y3) BUS 2A:= первый операнд.
   и BUS 2:B:= второй операнд.

у15) RGR:=АУ ; фиксация результата.

3. у5) BUS3:= RGR ; загрузка шины.

у18) R2:=BUS3.

В результате исполнения микроопераций в регистре R2 будет находиться результат сложения содержимого R1 и R2, т.е. R2=1000.

Литература

1. *Прищепа Л.С.* Проектирование центральных и периферийных устройств ЭВС: Учеб. пособие. Ч. 1. Разд. 2.

2. *Прищепа Л.С.* Компьютерные средства в системах автоматизации и управления: Учеб. пособие. Ч. 1.

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДА ОПРЕДЕЛЕНИЯ ВРЕМЕНИ ПРЕБЫВАНИЯ МАТЕРИАЛА В ТЕХНОЛОГИЧЕСКИХ АГРЕГАТАХ, ПРИБЛИЖАЮЩИХСЯ К АППАРАТАМ ИДЕАЛЬНОГО ВЫТЕСНЕНИЯ

А.Л. Рутковский, С.В. Сошкин, Д.Н. Дюнова

Северо-Кавказский горно-металлургический институт (государственный технологический университет), Научно-производственный комплекс «Югцветметавтоматика»

Одним из параметров, определяющих технико-экономические показатели большинства металлургических процессов, является время пребывания реагирующих веществ в реакционной зоне аппарата. Рассмотрим способ определения времени пребывания материала на примере процесса прокалки кокса во вращающихся печах, которые в первом приближении могут быть отнесены к аппаратам идеального вытеснения.

Скорость движения, а соответственно и время пребывания в аппарате антрацита определяет физико-химические условия его взаимодействия с поверхностью футеровки и потоками газа, а также расход топлива и производительность печи.

Среди известного многообразия работ по данной тематике можно выделить исследования механизма движения антрацита с учетом фракционного состава сырья дискретным способом. Практическое применение методов непрерывного определения скорости движения материала в соответствующей зоне печи не дает положительных результатов. Кроме того, периодический контроль скорости движения делает невозможным оперативное воздействие на ход процесса.

Оценить время пребывания материала в непрерывном режиме возможно при наличии информации о расходах сырья и готового продукта.

Источником таких сведений могут быть записи технических средств контроля массы загружаемого в печь и выгружаемого из холодильника материала, например автоматических весоизмерителей ВКТ-3.

Расход антрацита и расход прокаленного кокса являются случайными величинами. Несмотря на их изменение, закономерности процесса в целом остаются постоянными. Это позволяет процесс прокалки кокса рассматривать как стационарный. Вероятностную зависимость между указанными величинами характеризует взаимно корреляционная функция:

$$R_{xy}(\tau)=\frac{1}{T-\tau}\int_{0}^{N-\tau}\left[x(t)-m_x\right]\left[y(t+\tau)-m_y\right]dt\,, \qquad (1)$$

где T – длина реализации процесса; m_x, m_y – оценки математического ожидания, полученные по непрерывной реализации случайных процессов на входе и выходе объекта соответственно.

Для решения поставленной задачи величины расходов материала на входе и выходе объекта рассматриваем как эргодические процессы. С учетом сделанного допущения при переходе к конечным суммам зависимость (1) принимает вид:

$$R_{xy}\left(\frac{1}{N-n}\right)=\frac{1}{N-n}\sum_{i=1}^{N-n}\left[x(t_i)-m^*_x\right]\left[y(t_{i+m})-m^*_y\right], \qquad (2)$$

где $N=T/\tau$ – общее число точек реализации, τ – расстояние между соседними точками реализации, $n=\frac{\tau N}{T}$ – количество разбиений реализации.

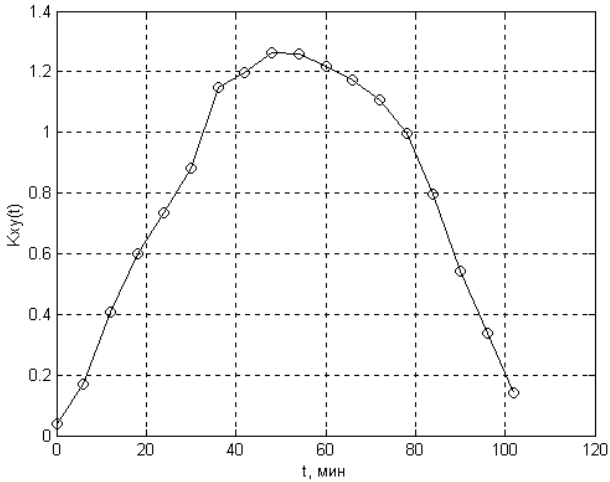


График взаимно корреляционной функции

Способ определения времени пребывания заключается в следующем. В соответствии с записями реализаций входного и выходного случайных процессов создается массив значений расхода сырья $x(t_i)$ и массив значений расхода готового продукта $y(t_{i+m})$. Число точек реализации определяется из априорно известных данных для конкретной печи. По массиву исходных данных рассчитывается оценка взаимно корреляционной функции и определяется значение τ, при котором $R_{xy}(\tau)$ максимально. Вычисленному значению τ соответствует время нахождения материала в системе «печь-холодильник» с известным общим расстоянием движения материала, что, в свою очередь, позволяет прогнозировать значение скорости материала в печи.

Пример использования данного алгоритма приведем для вращающейся печи длиной 45 м, диаметром 2,4 м и холодильником длиной 10 м при средней производительности 25 т/ч по прокаленному коксу. Массив исходных данных сформирован по результатам обработки диаграмм с записью текущих значений расхода сырого и прокаленного кокса ($N=70$ и $\tau=6$ мин). График взаимно корреляционной функции представлен на рисунке, согласно которому время пребывания материала в системе «печь-холодильник» составляет ≈ 52 мин.

Заключение. Представленный метод позволяет в промышленных условиях достаточно точно определять текущие потери кокса и оценивать его качество при различной загрузке печи.

КОМПЛЕКС СЧПУ «КЕМЕК» С ФАЗОВЫМ ДАТЧИКОМ ПОЛОЖЕНИЯ

К.Л. Еремин, студент* 5-*го курса ФВС
ТУСУР, г. Томск, rw9urd@sibmail.com

Автоматизация производства во всех отраслях промышленности выдвигает ряд проблем, связанных с улучшением качества управления агрегатами и технологическими объектами, основным видом регулируемого электропривода которых служит тиристорный электропривод (ТЭП) постоянного тока. Электрический привод является в современном производстве основным средством превращения электрической энергии в механическую и определяет технические возможности повышения эффективности труда и качества его результатов во всех сферах, связанных с реализацией механической энергии и точным воспроизведением требуемых движений.

Возросшие требования к скорости и точности выполняемых электроприводом движений, необходимость обеспечить взаимную связь одновременных движений нескольких рабочих органов машины или ряда агрегатов технологической цепи при оптимальных показателях и заданных ограничениях существенно усложнили функции управления ТЭП. Полная автоматизация технологических комплексов и АСУ потребовала расширения и усложнения функций управления в связи с необходимостью осуществлять обмен информацией с устройствами управления различных уровней, обеспечивать непрерывную автоматическую диагностику состояния, а также надежную и селективную защиту от нарушения нормального режима.

СЧПУ с комплектным тиристорным электроприводом «КЕМЕК» предназначена для управления текущим угловым положением вала двигателя соответственно управляющей программе, данные в которой заданы в цифровой форме. Данная система используется в учебной лабораторной установке, на которой студенты изучают вопросы программирования, наладки и эксплуатации реальных систем ЧПУ.

Основными компонентами СЧПУ являются:

– объект управления – электропривод «КЕМЕК» с управляемыми координатами положения и скорости вращения вала электродвигателя;

– ЭВМ, которая обслуживает управляющую программу и информационные сигналы о текущем положении вала двигателя и формирует сигналы управления электродвигателем;

– устройство сопряжения (УС) для сопряжения ЭВМ и электропривода «КЕМЕК».

В качестве объекта управления используется электропривод «КЕМЕК» с двигателем постоянного тока со встроенным тахогенератором и фазовым датчиком углового положения вала двигателя.

ЭП включает в себя ряд электротехнических, электронных и механических устройств, в результате чего он представляет собой электромеханическую систему.

Структурная схема электропривода показана на рисунке.

В комплект привода входят:

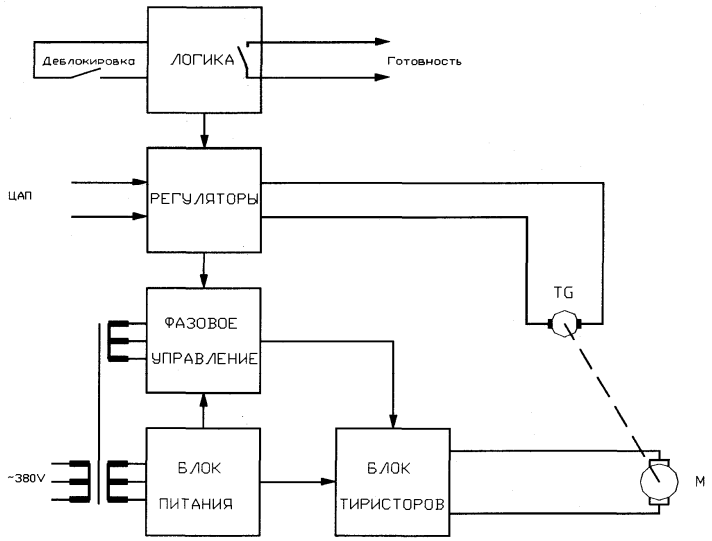
– шестипульсный реверсивный тиристорный преобразователь типа 2РЕВ16;

– высокомоментные электродвигатели серии 1 ПИ;

– силовой трансформатор типа ПЕВ.

Технические характеристики привода полностью удовлетворяют требованиям «Интерэлектро», диапазон регулирования частоты вращения составляет 1:10000, суммарная погрешность на минимальной частоте не превышает четырех процентов. Конструкция-преобразователь блочная, максимально унифицированная с широко распространенной

серией электроприводов типа «КЕМРОН». Степень защиты IP00. Преобразователь предназначен для встройки в станцию управления.



Структурная схема преобразователя «КЕМЕК»

В электроприводе используется электродвигатель 1ПИ-12. 11-11-202М со встроенными тахогенератором и резольвером.

Управление скоростью двигателя осуществляется изменением задающего постоянного напряжения на входе регулятора скорости в пределах от 0 до ±10 В. При этом скорость двигателя изменяется соответственно в пределах от 0 до 1000 оборотов в минуту.

Преобразователь выполнен по трехфазной реверсивной мостовой схеме выпрямления, применено классическое подчиненное регулирование с ПИ-регуляторами скорости и тока. Управление раздельное, без уравнительных токов. Нелинейное токоограничение обеспечивает ограничение максимально допустимого тока якоря в функции частоты вращения. Предусмотрено адаптивное регулирование коэффициента усиления и постоянной времени интегрирования в функции частоты вращения. СИФУ выполнено по вертикальному принципу с возможностью регулировки начального тока якоря. Разветвленная цепь электронных защит и сигнализации обеспечивает удобство эксплуатации и быстроту устранения возможных неисправностей.

Схема привода имеет следующие блоки: РС – регулятор скорости, РТ – регулятор тока, АР – адаптивный регулятор, КЗ – корректирующее звено, МТ*I* – схема выделения модуля напряжения тахогенератора, ФП – функциональный преобразователь, ПЭ – пороговый элемент, БНТО – блок нелинейного токоограничения, РНТ – регулятор начального тока якоря, БЛ – блок логики раздельного управления, СИФУ – система импульсно-фазового управления, ТР – силовой трансформатор, Я – электрическая цепь якоря двигателя, ТГ – тахогенератор, Sh – шунт, ДУ – дифференциальный усилитель тока, ОС – защита от перегрузки по току, OL – защита от длительной перегрузки, OS –защита от превышения максимальной частоты вращения, TG – защита от обрыва цепи тахогенератора, СР – защита от неправильного подключения, RD – готовность, ON – сигнал «Работа» (Деблокировка), БЗ – блок защиты, К – коммутатор, БП – блок питания.

Литература

1. *Подлесный Н.И., Рубанов В.Г.* Элементы систем автоматического управления и контроля: Учебник. Киев: Высш. шк., 1991. 461 с.

2. *Лебедев А.М.* Следящие электроприводы станков с ЧПУ. М.: Энергоатомиздат, 1988. 223 с.

3. *Москаленко В.В.* Электрический привод: Учеб. для электротехн. спец. техн. М.: Высш. шк., 1991. 430 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ДАННЫХ ПО ГОС II И III ПОКОЛЕНИЯ

Н.А. Новгородова, асистен каф. КИБЭВС; Е.Ю. Ерлыков, студент

ТУСУР, г. Томск, e-mail: pna@keva.tusur.ru

На кафедре КИБЭВС разрабатывается система электронного документооборота. Предпосылками ее создания явились: отсутствие синхронизации работы с документами, необходимость автоматизации планирования и контроля учебного процесса.

В решении задачи автоматизации процесса обучения в ВУЗах необходимо изначально закладывать хранение информации о ГОС. Такая задача является актуальной, так как по ГОС и выстраивается дальнейшая программа обучения студентов (учебные планы, рабочие программы дисциплин и пр.).

Учитывая тот фактор, что в данное время разрабатывается ГОС ВПО III поколения, необходимо при разработке системы для работы с государственным образовательным стандартом обратить особое внимание на ее гибкость, чтобы при принятии ГОС ВПО III поколения была возможность учитывать новые данные по ГОС.

В ГОС ВПО I и II поколения профессиональная квалификация выпускников вузов характеризовалась требованиями к знаниям, умениям и в какой-то степени навыкам, которые должен был приобрести выпускник в процессе обучения по тому или иному циклу дисциплин и в ходе аттестации. В ГОС ВПО III поколения данный подход заменяется на компетентностный. Результаты обучения оцениваются с помощью компетенций (компетенция – способность применять знания, умения и личностные качества для успешной деятельности в определенной области). Логика этого понятия применительно к сфере высшего образования такова. Студент получает в вузе по избранному профилю образования: а) определенный необходимый объем базовых (теоретических) знаний; б) совокупность методологий и методик применения этих знаний в практической деятельности; в) определенный опыт подобного применения (в ходе учебных, производственных и иных практик и т. п.). Все эти параметры должны оцениваться равнозначно, поэтому их все и объединяет термин «компетенция».

Для контроля и учета учебного материала, освоенного студентом, применяется принцип определения трудоемкости. Однако измерять трудоемкость придется не только в академических или астрономических часах, но и в особых условных единицах – кредитах.

Разрабатываемая система позволяет вести учет трудоемкости как в часах, так и в кредитах, и характеризовать квалификацию выпускников как требованиями к знаниям и умениям, так и компетенциями. Это обеспечивает совместимость данной системы учета данных по ГОС с готовящимися к введению государственными образовательными стандартами нового образца.

Для учета данных по ГОС необходимо первоначально занести их в базу данных. В соответствии с методологией IDEF0 процесс заполнения базы данных по ГОС представлен в виде блока, на входе имеем данные для заполнения, на выходе соответственно заполненную базу, в качестве управляющих условий выступают: Федеральное агентство по образованию, нормативно-правовые документы и ВУЗ, в роли механизмов выступают сотрудник ВУЗа и ЭВМ.

Данный процесс можно разбить на 2 составляющие, представленные на рисунке (т.е. провести его декомпозицию).

После определения всех существующих объектов, их свойств и отношений в данной предметной области была создана концептуальная модель базы данных, сущности, атрибуты, связи которой в дальнейшем были определены в терминах конкретной СУБД.

Таким образом, была получена база данных, содержащая данные ГОС II и III поколений. Далее планируется создание экспертной системы, основанной на этих данных.

Результат декомпозиции функции – Заполнить ГОС

Литература

1. www.edu.ru

2. *Методология* Функционального Моделирования IDEF0. РД IDEF0 – 2000.

3. *Коннолли Т., Бегг К., Страчан А.* Базы данных: проектирование, реализация и сопровождение. Теория и практика. М.: Диалектика, 2000. 1120 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЛЯ РАБОТЫ С БАЗАМИ ДАННЫХ ГИБДД

Г.А. Праскурин, ассистент каф. КИБЭВС; А.Е. Евтюшкин, студент

ТУСУР, г. Томск, Evtushkin@yahoo.com;

В основе проекта лежит разработка баз данных для государственной службы ГИБДД и программы управления этими базами данных, а также разработка web-приложения для общественного пользования в качестве информационного портала.

Эта тема очень актуальна на сегодняшний день, так как служба ГИБДД является государственной службой. В наше время государственные службы, в отличие от частных служб, предприятий, фирм, не предоставляют своим клиентам практически никакой информации, а если и представляют, то только в специально отведенных для этого местах. Отсюда и огромные очереди в этих учреждениях, малоинформативность клиентов. Рассмотрим конкретный пример. Чтобы человеку зарегистрировать автомобиль, ему нужно проехать через весь город в здание обл. ГИБДД, для того чтобы только узнать, какие документы нужны для регистрации. Чтобы непосредственно подать документы, нужно пробыть в здании ГИБДД не один и даже не два часа, а практически весь день, отстояв не одну очередь… Или взять обычную частную фирму. Что мы имеем здесь: полная информативность клиента как через onl*i*ne, так и через средство массовой информации, индивидуальный подход к клиенту (здесь я не буду рассматривать «качество» предоставляемой услуги, потому что это отдельная тема, не имеющая отношения к данному проекту). Избежать подобных мучений при работе с государственными службами поможет автоматизированная обработка данных сотрудниками этих служб и более распространенная и доступная для всех информация о работе данной службы.

Этот проект поможет автоматизировать, ускорить обработку информации, а размещение веб-сайта внесет доступную и достоверную информацию о работе службы ГИБДД.

На сайте предполагается размещение основной информации, документах, необходимых для определенного действия, а также информация о штрафах и нарушениях, которая может быть получена индивидуально,

используя персональные данные, и реализована через привязку к сайту базы данных, содержащую эту информацию.

Сам проект разработан непосредственно для работников службы ГИБДД и не может быть доступен для обычного пользователя, так как эта информация не разглашается.

Для проекта создаются гибкие системы баз данных и программы управления ими, что позволяет свести кучу рутинной письменной работы к автоматизированной обработке той же самой информации. Реализованы все необходимые функции: поиск, контроль совпадений (где это необходимо), формирование отчета по определенным критериям, вывод на печать и т.д.

Используя сайт, пользователь, вводя персональные данные (ФИО, номер паспорта), может не выходя из дома просмотреть все свои штрафы, сформировать квитанцию со всеми реквизитами для оплаты в банке. Таким образом, ему не придется посещать ГИБДД для получения этой информации. Оплатив соответственный счет, пользователь вводит номер квитанции, и уже непосредственно в ГИБДД эти данные регистрируются и обновляются. Это очень удобно как для ГИБДД, так и для их клиентов.

Таким образом, эта тема очень актуальна и требует детальной проработки каждой детали, с целью разработки единого информативного удобного комплекса программ и приложений для работы службы ГИБДД.

АНАЛИЗ ПРИНЦИПА ПРОГРАММНОГО УПРАВЛЕНИЯ РОБОТОМ ТУР-10

И.Г. Мишаткин, В.В. Николаев, Е.В. Хабаров, студенты 5-го курса
КИБЭВС, ТУСУР, г. Томск, www86@sibmail.com

Для управления манипулятором и выдачи технологических команд на оборудование роботизированного технологического комплекса применяется устройство числового программного управления (УЧПУ) УПМ-772. УЧПУ построено по принципу синхронного микропрограммного автомата управления с конечным числом состояний и жестким циклом управления [3].

1. Алгоритм управления.

В соответствии с техническими характеристиками устройства алгоритм обеспечивает работу в следующих режимах:

– ручного управления;
– обучения;
– разметки зоны;
– программы.

2. Ручное управление.

После ввода режима ручного управления и нажатия кнопки «ПУСК» управление манипулятором может осуществляться с выносного пульта оператора, обеспечивающего перемещение исполнительных органов манипулятора. Функция устройства управления в этом режиме сводится к переключению манипулятора на управление с выносного пульта и обеспечению последующего перехода в исходное состояние.

3. Режим обучения.

После выбора режима обучения и нажатия кнопки «ПУСК» управление перемещением исполнительных органов манипулятора может осуществляться с выносного пульта, что позволяет оператору вывести исполнительный орган в заданную точку рабочего пространства. С помощью соответствующих органов пульта управления оператор осуществляет набор информации, заносимой в кадр. Нажатие кнопки «ЗАПИСЬ КАДРА» вызывает перепись информации кадра в ячейки рабочей памяти. В процессе записи осуществляется вычисление контрольной суммы кадра и занесение ее в соответствующую ячейку памяти текущего кадра. Затем осуществляется переход к анализу нарушения формата кадра при преднаборе. При нарушении формата кадра прекращается выполнение операции обучения, и устройства переходят в исходное состояние. Если формат кадра выдержан, устанавливается в «1» триггер автоматического управления и осуществляется переход к исполнению занесенного в ячейки памяти кадра. Сбрасывается триггер подготовки и производится контрольное суммирование информации кадра. При обнаружении ошибки устанавливается в «1» триггер ошибки КХ и устройства переходят в исходное состояние. При нормальном завершении операции контрольного суммирования осуществляется рассылка управляющей и технологической информации по рабочим регистрам устройств. При наличии признака совмещения исполнения технологической команды (ТК) и отработки геометрической информации осуществляется выдача ТК на внешнее оборудование.

Затем осуществляется переход к блоку отработки геометрической информации для проверки правильности задания положения исполнительного органа. Так как триггер подготовки сброшен, то последовательно опрашиваются датчики обратной связи, и информация о положении исполнительных органов заносится в ячейки памяти начальных координат. После окончания загрузки ячеек памяти начальных координат устанавливается в «1» триггер подготовки. Информация с датчика обратной связи текущей координаты принимается в регистр устройств. Триггер разгона при этом находится в исходном состоянии. Константа заданной скорости заносится в регистр текущей скорости. Вычисляется

величина рассогласования между текущим и заданным положениями. Если рассогласование отсутствует, то устанавливается в «1» триггер конца отработки геометрической информации по текущей координате и сбрасывается содержимое регистра скорости и триггера движения.

При наличии рассогласования устанавливается в «1» триггер движения и анализируется величина рассогласования. Если рассогласование не превышает величины, определяемой степенью точности позиционирования, запрограммированной в текущем кадре, то устанавливается в «1» триггер конца отработки геометрической информации координаты, иначе этот триггер сбрасывается. В соответствии с динамическими характеристиками привода координаты выбирается величина наклона кривой торможения и вычисляется значение кода текущей скорости в режиме торможения. Затем устанавливается в «1» триггер разгона и после опроса датчиков вычисляется путь, пройденный исполнительным органом координаты от начального положения. Выбирается величина наклона характеристики и вычисляется значение кода текущей скорости в режиме разгона.

На основании сравнения из трех номеров скорости, а именно: заданной, торможения и разгона, выбирается наименьший, и соответствующий ему код скорости заносится в регистр скорости текущей координаты. На этом отработка текущей координаты завершается и осуществляется переход к анализу конца отработки геометрической информации кадра. Если отработка не завершена, то опрашивается датчик обратной связи очередной координаты и цикл обработки геометрической информации повторяется. По окончании отработки геометрической информации кадра осуществляется переход к анализу конца отработки всего кадра. С этой целью анализируется состояние триггера окончания техкоманды. Если выполнение указанной команды было начато, но не завершено, то осуществляется переход в режим ожидания их завершения. При этом исполнительные органы поддерживаются в заданном положении. Если триггера окончания указанной команды возведены, то анализируется, не требуется ли выдача команды в конце кадра. Эта ситуация может возникнуть, если в кадре задано точное позиционирование. Если техкоманда не выдана, то анализируется последовательность исполнения техкоманды схвата. Если команда схвата должна быть исполнена перед техкомандой, то возведенное состояние триггера ее выдачи и окончания свидетельствует о завершении ее исполнения. Выдается техкоманда и осуществляется переход к ожиданию ее завершения, иначе выдается команда на схват. Если техкоманда выдана и исполнена, то анализируется состояние триггера выдачи команды схвата. Если триггер находится в сброшенном состоянии, то выдается команда на схват, иначе осуществляется переход к завершению операции «Запись кадра». При

этом триггеры выдачи команд схвата и технологических команд сбрасываются, в счетчик кадров заносится номер очередного кадра. Затем номер очередного кадра высвечивается на табло пульта управления, и устройства переходят в исходное состояние.

После завершения занесения всей программы или ее очередной зоны в ячейки рабочей памяти оператор может осуществить перепись информации на внешний носитель – магнитную ленту.

Литература

1. 4СМ3.900.013 ПС Робот промышленный «ТУР-10» паспорт, 1983. 62 с.

2. Устройство числового программного управления УПМ772. Техническое описание. 1975. 147 с.

3. *Бейнарович В.А.* Основы автоматики и систем автоматического управления. Ч. 2. Технические средства автоматики. Измерительно-преобразовательные устройства. Томск: ТУСУР, 2003. 102 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПОСТРОЕНИЯ И ЗАПОЛНЕНИЯ ЖУРНАЛА ПРЕПОДАВАТЕЛЯ

Н.В. Хорошев, студент; Н.А. Новгородова, ассистент каф. КИБЭВС

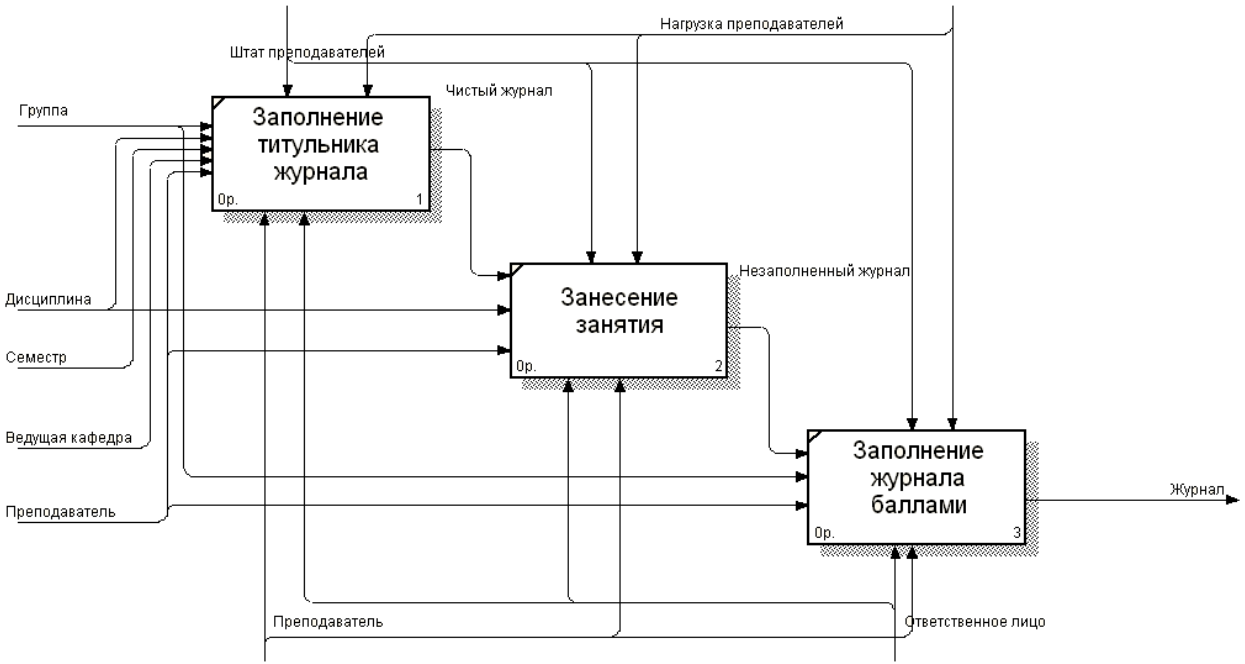
ТУСУР, г. Томск, e-mail: pna@keva.tusur.ru

В настоящее время на кафедре КИБЭВС разрабатывается система электронного документооборота. Актуальность данной разработки обусловлена тем, что отсутствие единого электронного архива документов порождает многократное тиражирование бумажных экземпляров, неудобства в организации одновременной работы нескольких исполнителей с документом, неэффективность поиска документов в текущем архиве и архиве за прошлые периоды. Разрабатываемая система строится на основе гибкой базы данных по технологии клиент/сервер, которая позволяет хранить в серверной базе данных большие объемы информации, накапливать статистику.

Одним из главных документов является журнал преподавателя. Он предназначен для мониторинга процесса обучения студентов каждой группы по каждой дисциплине в каждом семестре учебного года. В нем записаны данные о ведущей кафедре, фамилия преподавателя, а также расписание данной дисциплины для преподавателя.

Журнал учета посещаемости и текущей успеваемости студентов содержит список всех студентов группы, который при необходимости разбивается на подгруппы (в случаях лабораторных и практических работ).

Если преподаватель ведет учет посещаемости занятий, то он ставит соответствующую пометку напротив фамилии каждого студента группы в определенный день.



Процесс составления и заполнения журнала преподавателя в соответствии с методологией *I*DEF0

В связи с введением в ТУСУРе рейтинговой системы на каждом занятии студент может получить баллы, что также отображается в журнале. Также в определенные даты преподаватель подсчитывает текущую успеваемость студентов по дисциплине и выставляет соответствующий балл в поле контрольная точка 1 (КТ1) или КТ2.

В большинстве случаев для каждого занятия указываются темы и основные источники, в которых студент может ознакомиться с материалом занятия.

Преподаватель лабораторных работ указывает требования к защите (отчет и/или устная защита) и выставляет баллы каждому студенту по итогам проделанной работы.

В соответствии с методологией IDEF0 процесс создания и заполнения журнала преподавателя можно представить в виде блока, на входе которого мы имеем группу, дисциплину, семестр, ведущую кафедру и преподавателя, а на выходе уже заполненный журнал, в котором для каждого студента определенной группы ведется мониторинг посещаемости и успеваемости.

В качестве управляющих условий выступают: штат преподавателей и нагрузка преподавателей, а в роли механизмов – преподаватель и ответственное лицо, заполняющее журнал.

После проведения декомпозиции контекстной диаграммы, функция «заполнение журнала» представлена следующими функциями:

1) заполнение титульного листа;

2) занесение занятия;

3) заполнение журнала баллами.

Результат декомпозиции приведен на рисунке.

Литература

1. *Маклаков С.В.* Bpwin и Erwin.CASE – средства разработки информационных систем. 2-е изд., перераб. и доп. М.: ДИАЛОГ, 2001. 304 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПОСТРОЕНИЯ УЧЕБНЫХ ПЛАНОВ В ВЫСШЕМ УЧЕБНОМ ЗАВЕДЕНИИ

Н.А. Новгородова, ассистент каф. КИБЭВС; С.Ю. Исхаков, студент
ТУСУР, г. Томск, e-mail: pna@keva.tusur.ru

На кафедре КИБЭВС разрабатывается система электронного документооборота. Предпосылками ее создания явились: отсутствие синхронизации работы с документами, необходимость автоматизации планирования и контроля учебного процесса.

Обучение в высшем учебном заведении (ВУЗ) осуществляется по установленной образовательной программе, которая представляет собой целый комплект документов, определяющих, как должен быть построен учебный процесс в ВУЗе: какие дисциплины будут изучать студенты, в какой последовательности, в каком объеме и т.д.

Основным в этом комплекте является учебный план. Данный документ разрабатывается образовательным учреждением, в котором реализуется данная образовательная программа. При разработке учебных планов ВУЗ руководствуется государственным образовательным стандартом. Однако варьируя список изучаемых дисциплин и их количество в пределах, установленных государственным образовательным стандартом, ВУЗ формирует образовательный процесс с учетом специфики обучения и изменений в обществе.

Таким образом, в решении задачи автоматизации процесса обучения в ВУЗах необходимо автоматизировать построение и работу с учебными планами, что позволит четко отслеживать траекторию обучения студентов и своевременно реагировать на изменения ситуации в окружающем мире, внося соответствующие изменения и повышая тем самым качество образования.

Учебный план является структурозадающим документом в процессе получения высшего образования. Он определяет набор дисциплин, изучаемых на данной специальности с указанием общего числа часов по семестрам, неделям и разделением их по видам обучения. Основываясь на требованиях ГОС, ВУЗ уточняет дисциплины и оптимально располагает их во времени учебного процесса.

В связи с участием нашей страны в Болонском процессе сейчас проводится реформа высшего образования, призванная сделать российское образование равноправным с образованием в любой другой стране.

Томский государственный университет систем управления и радиоэлектроники является инновационным ВУЗом и в ближайшее время планирует внедрение такой системы образования.

Зачетные единицы, называемые также кредитами, исчисляются исходя из количества часов, затраченных на освоение конкретного материала. Они отражают трудоемкость данного материала.

Разрабатываемая система позволяет вести учет нагрузки студента как в часах, так и в кредитах, обеспечивает совместимость с готовящимися к введению государственными образовательными стандартами нового образца

Вся информация по учебным планам в системе организована в реляционную базу данных.

Процесс составления учебного плана может быть представлен следующими функциями:

1) выбор соответствующего ГОС на специальность;
2) выбор обязательных дисциплин;
3) выбор региональных компонентов;
4) согласование общего количества часов на каждую дисциплину;
5) выбор обучающей кафедры для каждой дисциплины;
6) разделение дисциплин по семестрам с видом отчетности;
7) разделение дисциплины по видам обучения;
8) расчасовка по видам обучения по неделям;
9) формирование учебного плана;
10) утверждение учебного плана.

Литература

1. *Давыдова Е.М., Новгородова Н.А.* Базы данных: Учеб. пособие. Томск: ТУСУР, 2005. 127 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПОДДЕРЖКИ ОБУЧЕНИЯ НА КАФЕДРЕ

Н.А. Новгородова, ассистент каф. КИБЭВС; С.С. Карпачев, студент
ТУСУР, г. Томск, pna@keva.tusur.ru

В настоящее время на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ведется разработка автоматизированной системы ведения документооборота кафедры. Актуальность данной разработки обусловлена тем, что отсутствие единого электронного архива документов порождает многократное тиражирование бумажных экземпляров, неудобства в организации одновременной работы нескольких исполнителей с документом, неэффективность поиска документов в текущем архиве и архиве за прошлые периоды.

Одними из основных частей системы являются модуль отображения расписания занятий учебного процесса и модуль заполнения рейтинга журнала преподавателя и его отображение. Задача автоматизации работы бюро расписаний на данный момент не ставится по причине большого количества входных данных и ограничений, накладываемых на эти данные. Исходя из этого, возникает необходимость в проектировании функциональной части базы данных, отвечающей за составление расписания без учета ограничений, накладываемых на количество часов, отведенных на дисциплину в неделю, нагрузку на преподавателя, ведущего занятие, вместимость аудитории и др. Данная часть базы данных необходима для создания автоматизированного модуля отображения распи-

сания учебного процесса. Впоследствии, на модуль составления расписания могут быть наложены перечисленные выше ограничения.

Основными входными данными для модуля составления расписания без учета ограничений являются рабочие планы занятий и извещения о поручениях кафедрам.

Рабочий план занятий (РПЗ) – документ, содержащий информацию о распределении по неделям общего количества часов дисциплин изучаемых группами одной специальности в семестре. Извещение о поручениях кафедре – документ, содержащий информацию о количестве часов на каждый вид обучения для групп одной специальности, обучаемых данной кафедрой. Таким образом, список групп и список дисциплин, изучаемых группой, при составлении расписания получают из рабочего плана занятий для года обучения, семестра, факультета. Список преподавателей, ведущих занятие выбранной дисциплины, содержится в ведомости распределения нагрузки между преподавателями.

Заключительным этапом создания автоматизированной системы поддержки обучения на кафедре является этап создания электронного журнала преподавателя. Данный модуль визуализирует журнал учета посещаемости и текущей успеваемости студентов, а также текущее задание для группы, студента. Предоставляется работа с журналом на уровнях «студент» и «преподаватель», определяющих права и возможности пользователей.

Литература

1. *Давыдова Е.М., Новгородова Н.А*. Базы данных: Учеб. пособие. Томск: ТУСУР, 2005. 127с.

2. *Бег К., Конноли Т., Страчан А.* База данных. Проектирование, реализация и сопровождение. Теория и практика. М.: Вильямс, 2000. 1120 с.

ПРОГРАММНАЯ МОДЕЛЬ ОЦИФРОВКИ ДАННЫХ ФОТОИМПУЛЬСНОГО ДАТЧИКА ПОЛОЖЕНИЯ В СИСТЕМЕ «КЕМЕК»

В.В. Кириченко, студент 5-го курса ФВС

ТУСУР, г. Томск. vink@sibmail.com

Эволюция технических средств персональных ЭВМ привела к повсеместному вытеснению операционной системы MS-DOS более мощными системами Windows, программирование для которых существенно сложнее. Разработчики систем программирования не замедлили выпустить соответствующие средства.

Одной из лучших систем программирования для MS-DOS является Turbo Pascal, разработанная фирмой Borland. Система программирования Delphi продолжила серию Паскаль – ориентированных средств программирования и является одним из наиболее удобных инструментов для Windows-программирования.

Среда Delphi – это сложный механизм, обеспечивающий высокоэффективную работу. Визуально она реализуется несколькими окнами. Главное окно осуществляет основные функции управления проектом создаваемой программы. Окно формы представляет собой проект Windows – окна будущей программы.

Любой размещенный на форме компонент характеризуется некоторым набором параметров. Для изменения этих параметров предназначено окно инспектора объектов. Это окно содержит две страницы – «Свойства» и «События». Страница «Свойства» служит для установки нужных свойств компонента, страница «События» позволяет определить реакцию компонента на то или иное событие. В верхней части окна инспектора объектов располагается раскрывающийся список всех помещенных на форму компонентов.

Окно кода программы предназначено для создания и редактирования текста программы. Этот текст составляется по специальным правилам и описывает алгоритм работы программы.

Таким образом, программирование в Delphi строится на тесном взаимодействии двух процессов: процесса конструирования визуального проявления программы и процесса написания кода, придающего элементам этого окна и программе в целом необходимую функциональность.

Описание алгоритма управляющей программы-модели.

Формирование управляющей программы происходит по следующим этапам:

1) подготовительные операции:

а) фиксирование двигателя путем его остановки (установка в 0);

б) выбор закона управления положением;

в) установка начальных значений переменных, используемых в процессе управления положением;

2) операции непосредственной реализации выбранного закона управления положением:

а) определение значения задания в настоящий момент времени;

б) расчет смоделированного значения пройденного пути (опрос датчика);

в) определение рассогласования между заданием и отработкой положения;

г) определение скорости как функции рассогласования;

д) вывод на экран заданных и смоделированных (реальных) значений.

В начальный момент после запуска программы на экран выдается окно, в центре которого представлен растровый диск датчика BE178A5. В правой части этого окна можно увидеть:

– двенадцатиразрядный код подаваемый на модель двигателя (на ЦАП), который определяет величину скорости вращения вала двигателя.

– трехразрядный код, обратной связи, поступаемый с модели двигателя (с датчика). Первый бит кода информирует о вращении вала двигателя по часовой стрелке (вперед), второй бит – о вращении вала двигателя против часовой стрелки (назад), третий бит соответствует растровому окну начала отсчета.

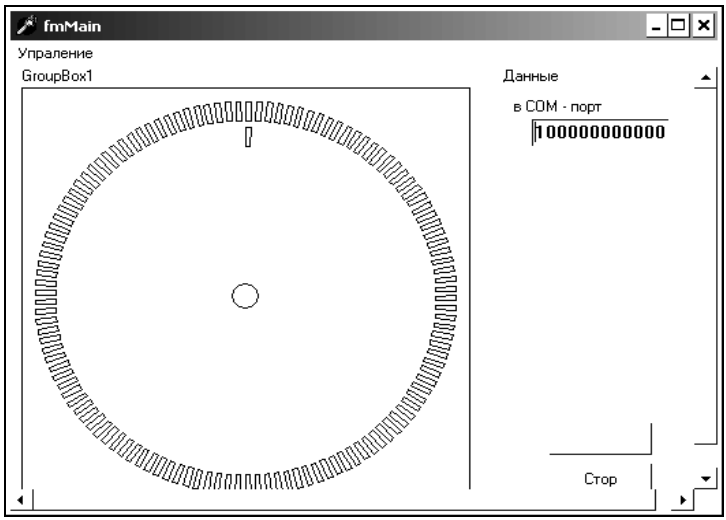


Рис. 1. Программная модель оцифровки датчика положения

При нажатии на кнопку «Пуск» можно увидеть окно динамики перемещения. При нажатии на кнопку «Перезапуск» начинается управляющее воздействие, при этом на диаграмме красным цветом отражается задаваемое воздействие, зеленый цвет соответствует смоделированному значению. Ниже графика выдаются задаваемое, реальное перемещение, относительная погрешность и время управляющего воздействия.

При нажатии на кнопку «Стоп» управляющее воздействие останавливается.

Нажав на пункт меню «Управление», можно либо установить двигатель в 0 либо выбрать закон управления.

В соответствии с выбранным законом управления запрашиваются параметры движения, такие как амплитуда перемещения, период, коэф-

фициент наклона (тангенс угла наклона). Данные параметры используются в дальнейшем, каждый в соответствующем уравнении закона управления для определения значения задания.

Рис. 2. Задание синусоидального закона перемещения

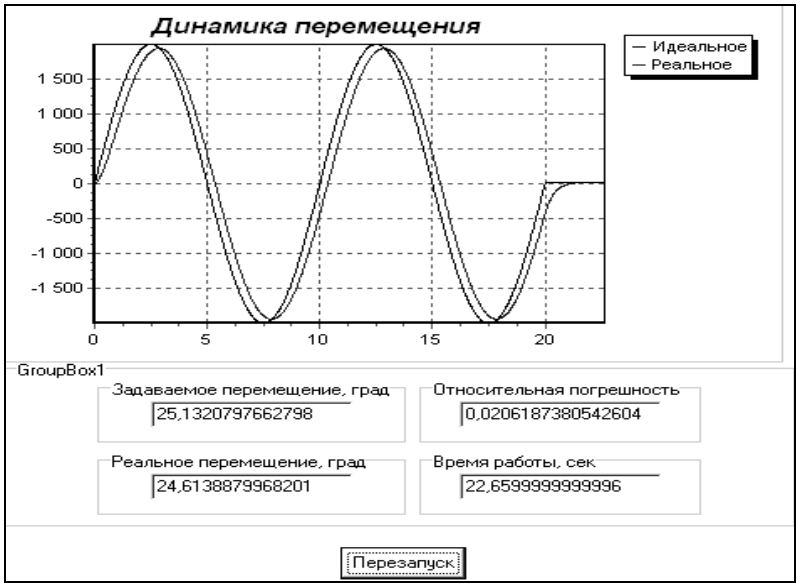


Рис. 3. Динамика перемещения

После этого программа входит в цикл отработки выбранного закона управления положением, а также вывод графиков функций задания и отработки:

$$\varphi_з = f(t), \quad (1)$$

$$\varphi_о = f(t). \quad (2)$$

В этом цикле происходят следующие операции. Сначала сохраняется значение задания в предшествующий момент времени. Далее путем выбора соответствующего уравнения производится вычисление величины задания в настоящий момент времени. На экран выводится линия задания за промежуток времени между предыдущим и настоящим вычислениями.

Величина отработки моделируется программным путем. При моделировании работы двигателя учитывается инерционность системы.

В нашей программе мы можем задать траектории движения электродвигателя. А именно: синусоидальный, пилообразный и трапециевидный.

Литература

1. *Коровин Б.Г.* Системы программного управления ромышленными установками и робототехническими комплексами. Л.: Энергоатомиздат, 1990. 352 с.

2. *Томпкинс У.Т., Уэбстер Д.К.* Сопряжение датчиков и устройств ввода данных с компьютерами IBM PC М.: Мир, 1992. 592 с., ил.

3. *Торгонский Л.А.* Системы питания датчиков положения (Субблоки SB-455, SB-456): Учеб.-метод. пособие. Томск: ТИАСУР, 1987. 34 с.

СИСТЕМА УПРАВЛЕНИЯ АВТОНОМНЫМИ ЭЛЕКТРОСТАНЦИЯМИ

В.Н. Клишин

г. Краснодар, ГОУ ВПО Кубанский государственный технологический университет

В современной промышленности большое значение имеют автономные и резервные источники электроэнергии на основе дизель-генераторных установок. Цели использования дизель-генераторов весьма индивидуальны и учитывают множество параметров.

Зарубежные и отечественные предприятия предлагают широкий модельный ряд дизельных электростанций широкого диапазона установочных мощностей, различных степеней автоматизации и классов применимости.

Такие электростанции поставляются полностью укомплектованными и готовыми к эксплуатации сразу после доставки и подключения. В их состав помимо дизельного двигателя и генератора входят система управления (СУ), устройство автоматического ввода резерва, система дистанционного мониторинга и др.

Системы управления дизельными электростанциями (СУ ДЭС) традиционно строятся на базе специализированных контроллеров – панелей управления, обеспечивающих функционирование агрегата в автоматическом или автоматизированном режиме.

Эксплуатация и техническое обслуживание указанных установок вызывают некоторые трудности:

Во-первых, многие панели управления оказываются попросту неремонтопригодными, так как стоимость приобретения запасных частей (модулей, плат) оказывается соразмерной с покупкой нового устройства.

Во-вторых, попытка самостоятельного ремонта вызывает необходимость применения не оригинальных комплектующих и оборудования, а их аналогов, что не во всех случаях является приемлемым.

В-третьих, при техническом обслуживании панели управления необходимо специализированное сервисное программное обеспечение, поставка которого изготовителем не предусматривается.

Для преодоления перечисленных трудностей эксплуатации систем управления дизель-электрическими станциями необходима разработка аналога российского производства, обеспечивающего замену импортных систем управления дизель-электрическими агрегатами.

Разработку такой системы предпочтительно вести в виде децентрализованной системы управления, построенной по блочно-модульному принципу на отечественной элементной базе.

При этом СУ ДЭС должна обеспечивать автоматизацию дизельных электростанций 3–4-й степени по ГОСТ 14228–80 [1] и по своим техническим характеристикам не уступать зарубежным аналогам.

Для реализации функций управления в соответствии с рекомендациями ГОСТ 10032–80, ГОСТ Р ИСО 8528-4–2005 [2, 3] такая система управления должна включать в себя три основных блока:

1. БКУ – блок контроля и управления дизелем. Микропроцессорное устройство, представляющее собой контроллер электронной системы управления двигателем (ЭСУД) с расширенными функциями системы аварийно-предупредительной сигнализации и отключаемой защиты (СПАСЗО) по ГОСТ 11928–83 [4].

Конструктивно блок управления может быть выполнен в виде отдельного устройства, монтаж которого выполняется на шасси агрегата в непосредственной близости от двигателя.

2. БКС – блок контроля силовых цепей. Представляет собой специализированное микропроцессорное устройство управления автоматическим вводом резерва.

Блок выполняет контроль напряжения, частоты, чередования фаз основного (сеть) и резервного (генератор) вводов. Для обеспечения требуемого режима работы генератора на допустимых перегрузках на линиях генератора производится контроль тока нагрузки.

БКС предназначен для обеспечения работы агрегата в программно выбираемых режимах: автономный, резерв сети, параллельная работа с сетью.

3. МПУ – местный пульт управления. Графическая сенсорная панель оператора либо пульт управления с механическими кнопками и световыми индикаторами (в зависимости от исполнения), предназначенный для осуществления ручного управления дизель-генераторным агрегатом.

МПУ отображает следующую информацию:

– напряжение и частоту резервируемой сети;

– напряжение и частоту генератора;

– напряжение аккумуляторных батарей;

– время наработки дизель-генераторной установки;

– состояние автоматов сети (АвС) и генератора (АвГ);

– состояние дизеля (частота вращения; температура охлаждающей жидкости, масла; давление масла; уровень топлива и т.д.);

– сообщения об авариях.

Конструктивно пульт управления может быть выполнен в виде отдельной панели предназначенной для монтажа, как на агрегате, так и на удалении от него на расстояние до 1000 м.

Перечисленные выше блоки объединены в единую сеть стандарта RS485, что позволяет интегрировать СУ ДЭС в смежные системы.

Примененный подход к построению децентрализованной системы управления автономным источником питания позволяет добиться гибкости, необходимой для адаптации системы управления как к новым, так и к модернизируемым дизель-генераторным агрегатам.

Открытость системы управления в сочетании с применением исключительно отечественной элементной базы позволяет значительно облегчить эксплуатацию и техническое обслуживание автономных дизель-электростанций.

Литература

1. ГОСТ 14228–80 Дизели и газовые двигатели автоматизированные. Классификация по объему автоматизации. М.: Стандартинформ, 2006. 5 с.

2. ГОСТ 10032–80 Дизель-генераторы стационарные, передвижные, судовые вспомогательные. Технические требования к автоматизации. М.: Стандартинформ, 2006. 4 с.

3. ГОСТ Р ИСО 8528-4–2005 Электроагрегаты генераторные переменного тока с приводом от двигателя внутреннего сгорания. Ч. 4. Устройства управления и аппаратура коммутационная. М.: Стандартинформ, 2006. 15 с.

4. ГОСТ 11928–83 Системы аварийно-предупредительной сигнализации и защиты автоматизированных дизелей и газовых двигателей. Общие технические условия. М.: Изд-во стандартов, 2004. 9 с.

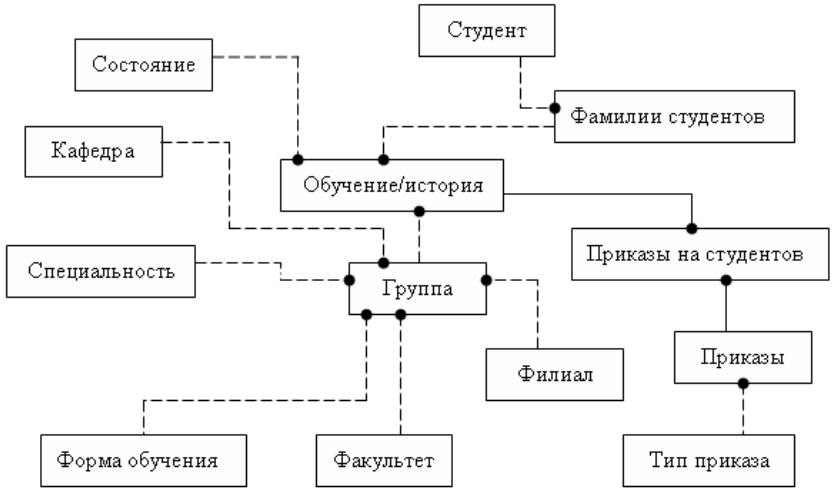
АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ПРИКАЗОВ СТУДЕНТОВ

О.Н. Круподерова, студент 5-го курса ФВС

ТУСУР, г. Томск, Lelechk-a@yandex.ru

Целью данной работы является разработка автоматизированной системы учета приказов на студентов для филиала ТУСУРа в г. Сургут.

Данная система должна обеспечить хранение и управление данными по приказам, группам, по смене фамилии или паспортных данных, факультетам, кафедрам, специальностям и филиалам.



Модель «сущность–связь»

В настоящее время в ТУСУРе уже существует автоматизированная система «Контингент», которая удовлетворяет всем требованиям, но, к

сожалению, нет возможности пользоваться ей в Сургуте. Поэтому часть документов представлена в бумажном виде, часть ведется в EXCEL, которая не дает таких возможностей, как работа по сети, многоуровневый доступ, хранение измененных данных, ведение архивов.

Вся информация в автоматизированной системе организована базой данных. Модель «сущность–связь» приведена на рисунке. База данных находится под управлением СУБД FireBird. Программная часть автоматизированной системы разрабатывается в среде Delphi.

Литература

1. *Ковязин А.Н., Востриков С.М.* Архитектура, администрирование и разработка приложений баз данных в InterBase Firebird Yaffil. Кудиц-Образ. М., 2002. 432 с.

2. *Архангельский А.Я.* Программирование в Delphi 7. М.: ООО «Бином-Пресс», 2003. 1152 с.

КОМПЬЮТЕРНЫЙ ИЗМЕРИТЕЛЬ RLC

М.С. Кузовлев, студент 5-го курса ФВС

ТУСУР, г. Томск, mikael@ms.tusur.ru

Измерительные приборы применяются на многих этапах разработки и эксплуатации радиоэлектронных изделий. Для измерения параметров пассивных элементов, которые используются в аналоговых и цифровых схемах, применяют измерители RLC. Измерители RLC – приборы для измерения сопротивления – R, индуктивности – L, емкости – C.

С развитием цифровой электроники появилась возможность создания малогабаритных и многофункциональных измерителей RLC с удобной формой отображения результата. При цифровой форме представления результатов измерений исключаются вносимые оператором в процессе измерения субъективные ошибки и обеспечивается возможность сопряжения измерительных приборов с вычислительными устройствами [1].

В представляемом докладе представлен вариант измерителя RLC, реализованный на контроллере SDK 1.1 на базе микроЭВМ ADuC842 и персональном компьютере. Структурная схема прибора показана на рисунке.

Структурная схема измерителя RLC

Модуль адаптера предназначен для коммутации исследуемых элементов в схему и выполняет функцию информационного датчика. Стенд SDK 1.1 в своем составе содержит 8 каналов преобразователей непрерывных сигналов АЦП (аналогово-цифровой преобразователь) с точностью 12 разрядов и 2 канала ЦАП (цифро-аналоговый преобразователь). Стенд предназначен для преобразования сигналов, проведения вычислений и передачи результатов измерений в ПК. Персональный компьютер в составе измерителя служит для создания удобного интерфейса представления результата измерений.

Измеритель RLC работает по методу прямого преобразования параметра в напряжение и ток на переменном сигнале [2]. Метод заключается в том, что на исследуемый элемент с ЦАП стенда подается синусоидальный сигнал с известной частотой и амплитудой. На элементе измеряется падение напряжения и ток через него. Результат, обработанный АЦП, заносится в память микроконтроллера. Вычисляются действительная и мнимая часть тока и напряжения, находится активное и реактивное сопротивление исследуемого элемента. В зависимости от тестируемого элемента находятся сопротивление для резисторов, емкость и тангенс угла потерь для конденсаторов, индуктивность и добротность для катушек индуктивности. Для устранения влияния паразитных сопротивлений соединительных проводов и элементов коммутации измерителя применяется пятипроводная схема измерения, по двум проводам подается тестовый сигнал на исследуемый элемент, по двум другим проводам снимается отклик сигнала, один провод является экранирующим.

Результаты вычислений выводятся на встроенный экран стенда в виде числового значения, что позволяет использовать прибор без подключения к ПК, и также передаются в персональный компьютер через разъем RS-232 [3]. В прикладной программе компьютера происходит обработка результатов измерений, их вывод в численном значении, построение графиков зависимости параметров исследуемого элемента от времени, сохранение результатов в базу данных.

Преимущества данного прибора заключаются в том, что он позволяет замерять дополнительные параметры пассивных элементов, такие как тангенс угла потерь для конденсаторов и добротность для катушек. Использование компьютера позволяет выводить зависимость параметров элементов от времени в виде графиков, вести накопление статистики и документирование измерений.

Литература

1. *Тычино К.К., Тычино Н.К.* Многофункциональные цифровые измерительные приборы. М.: Радио и связь, 1981. 128 с.

2. *Эпштейн С.Л., Давидович В.Г. и др.* Цифровые приборы и системы для измерения параметров конденсаторов. М.: Сов. радио, 1978. 192 с.

3. Учебный стенд SDK 1.1 Руководство пользователя. ООО «ЛМТ», 2001.

БЛОК ОБРАБОТКИ ДАННЫХ С МУЛЬТИПЛЕКСИРУЕМЫМИ ШИНАМИ

В.Е. Мацибаров, Ю.Б. Часовникова, студенты ФВС

ТУСУР, КИБЭВС, г. Томск

Блок обработки данных является ядром микропроцессорной системы, входит в состав регистрового АЛУ и предназначен для непосредственного исполнения микроопераций. Блок обработки данных структурно подразделяется на файл регистров РОН (R0-R7), приемники из шины BUS3, передатчики на шину BUS3, арифметико-логического устройства (АЛУ), предназначенного для выполнения 16 операций, регистра результата (RGR), регистра кода операции (PMS) и устройства управления. К устройству управления относятся два регистра адреса и два дешифратора (рис. 1).

Файл РОН подключается к арифметико-логическому устройству через внутренние мультиплексируемые шины BUS 2:A и BUS 2:B.

Шина BUS3 используется для передачи результатов обработки на регистры РОН (0–7) и, возможно, в порт ввода вывода.

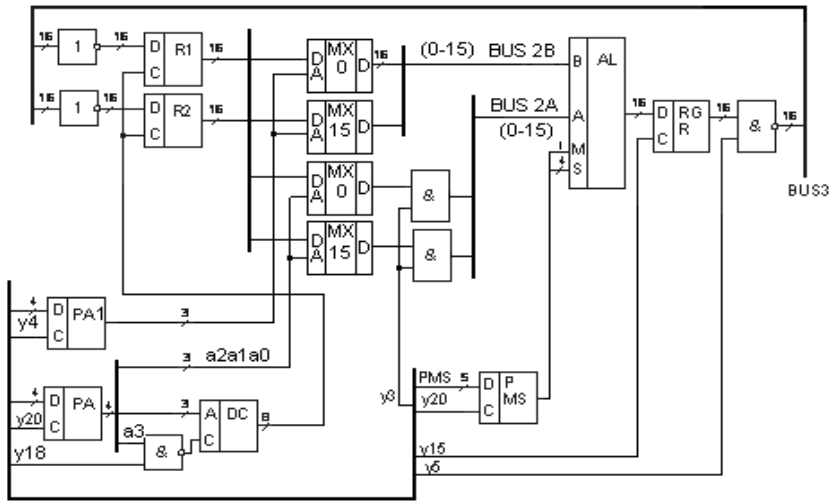
В блок обработки данных включены 8 шестнадцатиразрядных регистров R0-R7, чтение и запись в которые синхронизируются управляющими сигналами y3, y18 соответственно.

Использование схемы мультиплексирования шин подразумевает одновременную передачу операндов на входы АЛУ. На первом шаге интерпретации команды, по управляющему сигналу y4 будут произведены чтение адреса (который записан в поле PMS микрокоманды) второго операнда команды и передача этого операнда на вход неуправляемой шины BUS 2:B.

На втором шаге, по управляющему сигналу y20, будет произведено чтение адреса (который записан в поле PA микрокоманды) первого операнда и передача его на вход АЛУ по управляемой шине BUS 2:A, синхронизируемой y3.

Регистр кода операции PMS сохраняет и передает дешифрованный код операции на вход кода операции АЛУ. Регистр результата RGR сохраняет результат выполнения операции с выходов АЛУ и загружает данными шину BUS3, откуда их можно передать на регистры РОН или рабочие регистры RA или RD1 и далее в канал

Направление информационных потоков в порт ввода вывода и блок обработки данных различают по старшему разряду адреса a_3 a_2 a_1 a_0 в регистр РА Если a_3=1 – это указывает на порт ввода – вывода, если a_3=0 – на блок обработки данных.



Структурная схема блока обработки данных с мультиплексируемыми шинами

Для записи данных на регистры, в регистр РА адреса со стороны порта ввода/вывода подается адрес РОН, в который будет производится запись, и управляющий сигнал y18 на вход синхронизации дешифратора, выходы которого соединены со входами синхронизации РОН.

Последовательность обработки данных БОД покажем на примере выполнения команды ADD R1, R2. Пусть R1 = 0101, R2 = 0011, тогда микропрограмма интерпретации выглядит следующим образом (табл.).

	Линии микрокомандного канала и биты управления		
	21 20 19 18 17 16 15 14 13 12 11 10 9	87654	321
МКК	y21 y20 y19 y18 y17 y16 y15 y14 y13 y3 y4	PMS	0
МК	y5 y6	00001	PA
1	1 0 0 0 0 0 0 0 0 0 1 0 0	00010	000
2	1 1 0 0 0 0 1 0 0 1 0 0 0	00000	0
3	1 0 0 1 0 0 0 0 0 0 0 1 0		001
			0
			001
			0

1. y4) PA1(8-4):=адрес второго операнда (R1) ; R1=0101.

2. y20) PA(4-1):=адрес первого операнда (R2) ; R2=0011.
   и PMS(8-4):=код операции сложения ; PMS=2.
   y3) BUS 2A:= первый операнд.
   и BUS 2:B:= второй операнд.
   y15) RGR:=AУ ; фиксация результата.
3. y5) BUS3:= RGR ; загрузка шины.
   y18) R2:=BUS3.

В результате исполнения микроопераций в регистре R2 будет находиться результат сложения содержимого R1 и R2, т.е. R2=1000.

Литература

1. *Прищепа Л.С.* Проектирование центральных и периферийных устройств ЭВС. Учеб. пособие. Ч. 1. Разд. 2.

2. *Прищепа Л.С.* Компьютерные средства в системах автоматизации и управления: Учеб. пособие. Ч. 1.

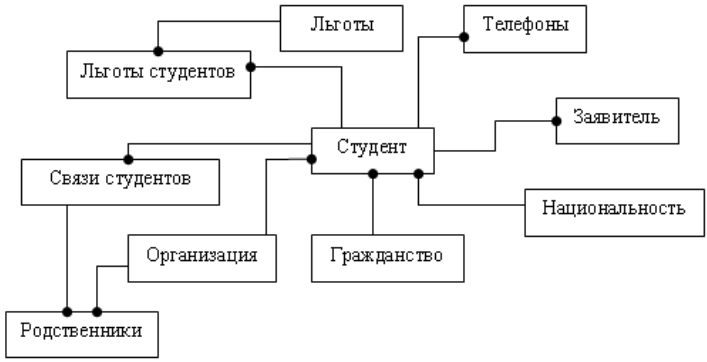
АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА СТУДЕНТОВ

Д.М. Моисеенко, студент 5-го курса ФВС

ТУСУР, г. Томск, Sirius41@yandex.ru

Целью данной работы является разработка автоматизированной системы учета студентов для филиала ТУСУРа в г. Сургут.

Данная система должна обеспечить хранение и управление данными по студентам, заявителям, родственникам и телефонам.



Модель «сущность–связь»

На данный момент в ТУСУРе уже существует автоматизированная система «Контингент», она удовлетворяет всем требованиям, но к сожалению, нет возможности пользоваться ей в Сургуте. Поэтому большое

число документов находится в бумажном виде, также не малое количество хранится, пересылается и ведется в таких продуктах, как Microsoft Word, EXCEL, которая не дает таких возможностей, как работа по сети, многоуровневый доступ, хранение измененных данных, ведение архивов.

Вся информация в автоматизированной системе организована базой данных. Модель «сущность–связь» приведена на рисунке. База данных находится под управлением СУБД FireBird. Программная часть автоматизированной системы разрабатывается в среде Delphi.

Литература

1. *Ковязин А.Н., Востриков С.М.* Архитектура, администрирование и разработка приложений баз данных в InterBase Firebird Yaffil. Кудиц-Образ. М., 2002. 432 с.

2. *Архангельский А.Я.* Программирование в Delphi 7. М.: ООО «Бином-Пресс», 2003. 1152 с.

МЕТОДИКА ВЫБОРА ЭЛЕМЕНТНОЙ БАЗЫ

А.А. Николаев, А.С. Бондаренко,– студенты 5-го и 3-го курсов ФВС

КИБЭВС, ТУСУР, г. Томск, nikol222@sibmail.com

Один из важнейших этапов разработки УВМ – выбор серии ИМС, так как от правильного выбора зависит, будет ли в конечном итоге разрабатываемая машина отвечать всем требованиям, предъявляемым к ней в техническом задании.

Методики выбора серии ИМС, оптимальной для той или иной разрабатываемой машины, в настоящее время не существует, так как связать воедино вопросы технологии, экономики, конструирования, изготовления и эксплуатации машины с тактико-техническими характеристиками ИМС оказалась сложной задачей. Критерии сравнения определяются системой основных параметров логических ИМС: коэффициентом объединения по входу Коб, коэффициентом разветвления по выходу Краз, статической помехоустойчивостью Кп, потребляемой мощностью Рпот и средней задержкой распространения сигнала tзд.р.ср. В ряде случаев, диктуемых специфичностью разрабатываемой машины, к этим критериям сравнения относят вес, габаритные размеры, форму корпуса, степень интеграции логических функций, радиационную стойкость и др. Например, для ЭВМ, предназначенной для массового выпуска, важный критерий сравнения – стоимость серии ИМС.

Методика в случае выбора логических ИМС заключается в следующем. Производится сравнительная оценка по параметрам, отражающим производственные и потребительские качества той или иной серии

ИМС, что дает возможность провести выбор серии ИМС, оптимальной с точки зрения конструктивной, технической, экономической, технологической и эксплуатационной.

По количественному определению сравниваемые параметры делят на две группы.

К первой группе относятся параметры, характеризующие качество серии ИМС и содержащиеся в технической документации на нее: а) средняя задержка на элемент; б) количество типов элементов в серии; в) габариты корпуса; г) стоимость основного элемента; д) устойчивость к климатическим воздействиям; е) устойчивость к механическим воздействиям;

Ко второй группе относятся параметры, определяемые возможностями вычислительных устройств, построенных с применением той или иной серии ИМС: ж) надежность (вероятность безотказной работы); з) потребляемая мощность; и) стоимость изготовления; к) объем; л) вес.

Параметры второй группы определяют из конструкторской документации на устройство (схему). Для сравнительного анализа необходимо выпускать конструкторскую документацию на одно и то же устройство с применением каждого из анализируемых типов серий ИМС.

После установления параметров качества обеих групп для каждой серии ИМС их сводят в матрицу.

Параметры матрицы **X**, имеющие количественное выражение, приводится к такому виду, чтобы большему численному значению параметра соответствовало лучшее качество серии ИМС. Параметры, не удовлетворяющие этому условию, пересчитываются, и получаем матрицу приведенных параметров. Затем производим нормирование параметров матрицы. В результате получаем матрицу нормированных параметров. Для обобщенного анализа систем элементов введем оценочную функцию.

Определив оценочную функцию для каждой из сравниваемых серий ИМС, можно определить серию, наиболее полно удовлетворяющую предъявляемым требованиям к ЭВМ, так как лучшей серии ИМС соответствует меньшее значение величины оценочной функции. Таким образом, процедура сравнительного анализа серий ИМС сводится к следующим этапам:

1. Серии ИМС рассматривают с точки зрения их пригодности по параметрам а, б, в, г, ж, з, и. Если по одному из этих параметров серия не удовлетворяет тактике – техническим требованиям, то ее отбрасывают и не используют.

2. Из параметров отобранных серий составляют матрицу, которую затем при необходимости преобразуют в другую матрицу.

3) Полученную матрицу нормируют и с учетом весовых коэффициентов определяют оценочную функцию для каждой из рассматриваемых серий. Та серия ИМС, у которой величина оценочной функции меньше, признается наиболее оптимальной.

Серии ИМС, обозначенные индексами I, II, III, удовлетворяют по параметрам а, б, в, г, ж, з, и, тактико-техническим требованиям.

Литература

1. *Прищепа Л.С.* Аппаратные средства вычислительной техники. Разд. 5. М.: В-Спектр, 2006. 154 с.

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ДАННЫХ ДЛЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПО ФОРМИРОВАНИЮ НАГРУЗКИ КАФЕДРЫ

А.Ю. Журавлева, студентка; Н.А. Новгородова, ассистент каф. КИБЭВС

ТУСУР, г. Томск, pna@keva.tusur.ru

В Томском государственном университете систем управления и радиоэлектроники (ТУСУР) на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) разрабатывается автоматизированная система для формирования нагрузки кафедры.

Одними из основных документов, моделируемых этой системой, являются рабочий план занятий (РПЗ), извещение о поручениях кафедре и распределение нагрузки между преподавателями.

Деканат на основе учебного плана на специальность составляет рабочие планы занятий на группы, обучающиеся по соответствующей специальности. Также деканат на основе РПЗ и приказов ректора, в которых указано количество необходимого времени на соответствующий вид отчетности по дисциплине, составляет извещение о поручениях кафедре по определенной специальности. Кафедра, в свою очередь, распределяет нагрузку между преподавателями, согласовываясь с бюро расписаний.

Разработанная концептуальная модель данных для автоматизированной системы по формированию нагрузки кафедры приведена на рисунке.

Процесс составления РПЗ имеет следующие особенности:

– данный документ составляется сроком на один семестр;

– заполняется для каждой группы отдельно по ее учебному плану;

– группы, имеющие даже разные учебные планы, могут изучать некоторые дисциплины совместно (потоком);

– в данном документе учитываются только аудиторные виды обучения.

Концептуальная модель данных

Извещение о поручениях кафедре имеет следующие особенности:

– данный документ составляется сроком на один семестр;

– формируется на одну специальность одной формы обучения на основе нескольких РПЗ для одной кафедры – преподавателя;

– в извещение о поручениях кафедре включаются как аудиторные, так и неаудиторные виды занятий для каждой дисциплины, согласно учебному плану;

– расчет итоговой нагрузки осуществляется по специальным формулам.

Процесс распределения нагрузки на кафедре имеет следующие особенности:

– данный документ заполняется на основе извещений о поручениях кафедре;

– документ составляется два раза в год сроком на один семестр;

– при расчете нагрузки преподавателей наряду с аудиторными занятиями учитывается и внеаудиторная работа, такая как ведение практик, ведение дипломников, руководство аспирантами, учебная НИР, проверка дипломных проектов, проведение консультаций и т. п.;

– один и тот же предмет, формы занятий в одной группе могут вести разные преподаватели;

– преподавание предмета может производиться одновременно в нескольких группах (потоке);

– расчет нагрузки преподавателя ведется на основе количества студентов в группе и количества подгрупп;

– после завершения этапа распределения нагрузки необходимо рассчитать общую нагрузку по кафедре и сравнить с нагрузкой, указанной в извещении о поручениях кафедре.

Литература

1. *Давыдова Е.М., Новгородова Н.А.* Базы данных: Учеб. пособие. Томск: ТУСУР, 2005. 127 с.

2. *Коннолли Томас, Бегг Карелии*. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. 3-е изд.: Пер. с англ. М.: Изд. дом «Вильяме», 2003. 1440 с.: ил.

3. *Кузнецов С.Д.* Информационно-аналитические материалы. http://www.citmgu.ru/

ТИПОВЫЕ ЗАДАЧИ КОНСТРУКТОРСКОГО ПРОЕКТИРОВАНИЯ РЭС И АЛГОРИТМЫ ИХ РЕШЕНИЯ

А.С. Новожилов, студент 5-го курса ФВС

ТУСУР, г. Томск

При конструкторском проектировании РЭА (радиоэлектронной аппаратуры) решаются задачи, связанные с поиском наилучшего варианта конструкции, удовлетворяющего требованиям технического задания и максимально учитывающего возможности технологической базы производства. Тесная взаимосвязанность задач и большая размерность каждой из них обычно не позволяют предложить метод поиска оптимального конструктивного решения в едином цикле в связи с трудностями создания общей математической модели, комплексно учитывающей особенности конструкторско-технологической базы производства.

Поэтому разработка и реализация алгоритмов и методов решения отдельных задач этапа конструкторского проектирования: компоновки,

размещения и трассировки – до сих пор остаются актуальными проблемами, решение которых неотъемлемо связано с развитием систем автоматизации проектирования.

При проектировании РЭС задача компоновки решается на различных иерархических уровнях. В зависимости от принятых критериев существуют три варианта постановки задачи компоновки:

– типизация – разбиения ФС (или ПЭС) на части по критерию минимума числа разнотипных узлов (минимум номенклатуры узлов);

– покрытие – преобразование ФС в ПЭС, т.е. в схему соединения конструктивных модулей, номенклатура которых заранее известна;

– разрезание – разбиение ФС (или ПЭС) на части, соответствующие модулям более высокого уровня, с минимизацией числа связей между этими частями, причем число частей может задаваться или определяться в процессе решения.

Исходной информацией при решении задач размещения являются: данные о конфигурации и размерах коммутационного пространства, определяемые требованиями установки и крепления данной сборочной единицы в аппаратуре; количество и геометрические размеры конструктивных элементов, подлежащих размещению; схема соединений, а также ряд ограничений на взаимное расположение отдельных элементов, учитывающих особенности разрабатываемой конструкции.

Поэтому все применяемые в настоящее время алгоритмы размещения используют промежуточные критерии, которые лишь качественно способствуют решению основной задачи: получению оптимальной трассировки соединений. К таким критериям относятся: 1) минимум суммарной взвешенной длины соединений; 2) минимум числа соединений, длина которых больше заданной; 3) минимум числа пересечение проводников; 4) максимальное число соединений между элементами, находящимися в соседних позициях либо в позициях, указанных разработчиком; 5) максимум числа цепей простой конфигурации.

Трассировка соединений является, как правило, заключительным этапом конструкторского проектирования РЭС и состоит в определении линий, соединяющих эквипотенциальные контакты элементов, и компонентов, составляющих проектируемое устройство.

Основная задача трассировки формулируется следующим образом: по заданной схеме соединений проложить необходимые проводники на плоскости (плате, кристалле и т.д.), чтобы реализовать заданные технические соединения с учетом заранее заданных ограничений. Основными являются ограничения на ширину проводников и минимальные расстояния между ними.

Известные алгоритмы трассировки печатных плат можно условно разбить на три большие группы:

1. Волновые алгоритмы, основанные на идеях Ли и разработанные Ю.Л. Зиманом и Г.Г. Рябовым. Данные алгоритмы получили широкое распространение в существующих САПР, поскольку они позволяют легко учитывать технологическую специфику печатного монтажа со своей совокупностью конструктивных ограничений. Эти алгоритмы всегда гарантируют построение трассы, если путь для нее существует.

2. Ортогональные алгоритмы, обладающие большим быстродействием, чем алгоритмы первой группы. Реализация их на ЭВМ требует в 75–100 раз меньше вычислений по сравнению с волновыми алгоритмами. Такие алгоритмы применяют при проектировании печатных плат со сквозными металлизированными отверстиями. Недостатки этой группы алгоритмов связаны с получением большого числа переходов со слоя на слой, отсутствием 100%-й гарантии проведения трасс, большим числом параллельно идущих проводников.

3. Алгоритмы эвристического типа. Эти алгоритмы частично основаны на эвристическом приеме поиска пути в лабиринте. При этом каждое соединение проводится по кратчайшему пути, обходя встречающиеся на пути препятствия.

Литература

1. *Деньдобренко Б.Н., Малика А.С.* Автоматизация конструирования РЭА. М.: Высш. шк., 1980.

2. *Курейчик В.М.* Математическое обеспечение конструкторского и технологического проектирования с применением САПР. М.: Радио и связь, 1990.

3. *Морозов К.К., Одиноков В.Г., Курейчик В.М.* Автоматизированное проектирование конструкций радиоэлектронной аппаратуры. М.: Радио и связь, 1983.

4. *В.Н. Ильин, В.Т. Фролкин, А.И. Бутко и др.* Автоматизация схемотехнического проектирования: Учеб. пособие для вузов. М.: Радио и связь, 1987.

5. *Алексеев О.В., Головков А.А., Пивоваров И.Ю., Чавка Г.Г.* Автоматизация проектирования радиоэлектронных средств. М.: Высш. шк., 2000.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПОИСКА, АНАЛИЗА И ПРИНЯТИЯ РЕШЕНИЯ «ПУАРО»

К.В. Пинчин, студент 5-го курса ФВС

ТУСУР, г. Томск, e-mail: ronin@kemerovocity.ru

В современных условиях в бизнесе существенное значение приобретает анализ возможных ситуаций, определение их тенденций, оценка возможных рисков при принятии решений. Уже недостаточно владеть информацией в виде маркетинговых исследований или бизнес, справок о

предприятиях потенциальных партнеров и конкурентов. Необходимо правильно ответить на вопросы: кто или что является причиной возникновения событий; откуда исходит или может исходить угроза и как ее избежать или уменьшить? Важность решения этих задач стала причиной возникновения деловой разведки – важнейшего инструмента информационно-аналитической поддержки принятия решений.

Деловая разведка в Интернете является в настоящее время равноправной составляющей успешного бизнеса любой современной коммерческой фирмы. Сбор информации о конкурентных производствах, технологиях и производителях с последующей обработкой и аналитикой для принятия правильных и продуманных решений. Хочется отметить, что это не промышленный шпионаж, так как действует в рамках существующих законов и 80% оперативной и стратегической информации получают через Internet. Открытыми доступным информационным источниками относятся:

– электронные СМИ;

– официальные сайты организаций и корпоративные блоги;

– электронные справочники и энциклопедии;

– профессиональный базы данных;

– и т.д.

Для реализации системы была создана проектная группа ГПО в составе студентов 4-го курса: А.И. Михайловского, Д.А. Истомина, М.А. Рыпакова, Е.А. Басова и руководителя группы – студента 5-го курса К.В. Пинчина.

Системы «ПУАРО» позволит создать предпосылки для принятия стратегически важных решений пользователем системы. В настоящее время отсутствие развитых средств деловой разведки в Интернет существенно сдерживает развитие крупных и средних компаний и фирм, поскольку приводит к принятию неоптимальных решений без учета тенденций развития конкурентов.

Реализация и детальная проработка вопросов стратегического развития бизнеса компаний позволит не только реально продавать систему «ПУАРО», но и включать ее в качестве компонента в проведении исследований рынка специализированными фирмами.

Прежде чем создать что-то новое, нужно хорошо изучить уже имеющиеся системы, их плюсы и минусы. Первым этапом работ было рассмотрение систем для деловой разведки представленные на российском рынке.

Произведен анализ программных продуктов для того, чтобы воплотить в системе «ПУАРО» все востребованные функции и возможности. Были выявлены источники угроз и рисков. Также были проанализирова-

ны методы снижения появления риска. Риски, требующие вмешательства, были рассмотрены отдельно, а также были составлены рекомендации для уменьшения воздействия данных рисков.

Далее были сформулированы требования к системе в целом, отраженные в техническом задании. Система будет состоять из следующих подсистем:

1. Подсистема поиска, которая включает в себя веб-паука и индексатор. Веб-паук предназначен для скачивания веб-страниц из Интернета. А индексатор осуществляет анализа скаченных веб-страниц, их разбиение на составляющие и занесение данных в базу данных.

2. Подсистема хранения, состоит из базы данных и вспомогательных программа для манипулирования данных. База данных состоит из двух частей: словаря и индексной базы данных. Словарь содержит все найденные в Интернете слова, причем при занесении слов в словарь часто отсекаются окончания и суффиксы для более эффективного хранения информации. Индексная база данных включает:

– таблицу документов (содержит список всех известных поисковой машине адресов страниц вместе с дополнительной информацией);

– обратный индекс (который хранит информацию о том, в каких документах и в каких конкретно позициях каждого из документов можно найти каждое из слов);

– прямой индекс (хранит «препарированный» текст и некоторые элементы форматирования для каждого известного поисковой машине документа);

– ссылочный индекс (содержит «препарированный» текст с учетом текстов гиперссылок).

3. Подсистема анализа предназначена для поиска информации по базе данных по запросу пользователя и ее предварительному анализу.

4. Подсистема принятия решения осуществляет анализ выбранной информации из базы данных и вывод результатов в удобной для восприятия форме.

В ходе планирования системы были выделены два направления в реализации системы:

– локальный вариант – все части системы установлены у клиента;

– клиент-серверная версия – система установленная у клиента посылает запросы к базе данных установленной у разработчика.

Первый вариант установки предполагает полную установку системы у клиента и возможность ее настройки под нужды клиента. В отличие от первого варианта второй вариант предполагает установку у клиента только подсистем анализа и принятия решения. А подсистемы поиска и хранения будут размещены на серверах разработчика системы.

Такой вариант позволит значительно снизить затраты по установке и эксплуатированию системы. Так как клиентская программа будет обращаться только за необходимыми ей данными на сервер разработчиков системы. В свою очередь вся нагрузка по созданию полных информационных баз данных ляжет на разработчиков системы. Второй вариант установки предполагает более универсальный вариант системы и содержимое информационных баз данных.

На данный момент нами реализованы подсистемы поиска и хранения. Подсистема хранения реализована на свободно распространяемом СУБД PostgreSQL.

Литература

1. *Баяндин Н.И.* Основы деловой разведка: Учеб. пособие // Под ред. Л.М. Кунбутаева М.: МЭИ, 2005. 244 с.

2. http://www.it2b.ru

3. *Деревицкий А.Н.* Коммерческая разведка: Курс агентуры для тех, кто продает и управляет продажами. СПб.: Питер, 2005. 208 с.

ВСТРАИВАНИЕ ЦВЗ С ПОМОЩЬЮ АЛГОРИТМОВ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Ю.М. Филимонов, доц. каф. КИБЭВС; Л.А. Побызаков, студент

ТУСУР, г. Томск, lunh@sibmail.com

Развитие информационных технологий привело к широкому использованию цифровых фотографий, dvd-фильмов, музыки в формате mp3. Наряду с этим возник практический смысл защиты информации. Так возникла стеганография как направление в IT. Стеганография – это метод организации связи, который собственно скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания. Слово «стеганография» в переводе с греческого буквально означает «тайнопись» (steganos – секрет, тайна; graphy – запись). К ней относится огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные каналы и средства связи на плавающих частотах и т.д. Стеганография занимает свою нишу в обеспечении безопасности: она не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к

тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты. В настоящее время в связи с бурным развитием вычислительной техники и новых каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т.п. Это дает нам возможность говорить о становлении нового направления – компьютерной стеганографии. Из цифровой стеганографии вышло наиболее востребованное легальное направление – встраивание цифровых водяных знаков, являющееся основой для систем защиты авторских прав. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера (атакам). В результате необходимо встраивать информацию не только незаметно, но и так, чтобы она была устойчива к различным видам атак.

В настоящее время большинство хранящихся на компьютерах изображений с непрерывным цветовым тоном кодируются с помощью алгоритма JPEG. Однако при значительном сжатии, изменении внешнего вида рисунка. ЦВЗ становятся едва различимыми или совсем пропадают. Новый стандарт JPEG 2000, основанный на использовании алгоритма вейвлет-преобразования, позволяет сжимать изображения в 200 раз без заметной для глаза человека потери качества.

Вейвлет-преобразования имеют очень хорошую частотно-пространственную локализацию и по этому показателю превосходят традиционные косинус-преобразования и другие преобразования Фурье. Таким образом, становится возможным применять более сильное квантование, улучшая свойства последовательности для последующего сжатия без потерь. Алгоритмы сжатия изображений, основанные на этом преобразовании, при той же степени сжатия показывают лучшие результаты по сохранению качества изображения.

На этапе предварительной обработки изображение разбивается на несколько равных блоков. Затем в каждом блоке происходит смещение постоянной составляющей: из значений цветности для каждого пикселя вычитается среднее значение, после чего смещенные значения цветности преобразуются в систему яркость/цветность. После применения вейвлет-преобразования полученные матрицы числовых коэффициентов подвергаются квантованию. Следующий этап сжатия изображения – энтропийное кодирование – предполагает применение адаптивного арифметического кодера, а не кодирования по методу Хаффмана, как в алгоритме JPEG, за счет чего увеличивается скорость сжатия. Затем сжатый поток данных разбивается на пакеты. Именно благодаря гибкой и продуманной структуре пакетов возможно достижение целей разработки этого метода сжатия.

Одной из основных преследуемых целей является тщательное исследование способов внедрения ЦВЗ или любой другой информации в стеганографии на основе вейвлетов. При исследовании будут рассмотрены текущие алгоритмы сжатия изображений, произведется детальный анализ робастности и ошибкоустойчивости этой техники по отношению к искажению изображения. На основе полученных результатов будут выдвинуты рекомендации по модификации алгоритмов для конкретного случая.

Литература

1. *Грибунин В.Г.* Цифровая стеганография. М.: СОЛОН-Пресс, 2002.
2. http://www.intuit.ru- описание форматов jpeg и jpeg2000.

БЛОК ОБРАБОТКИ ДАННЫХ С УПРАВЛЯЕМОЙ ШИНОЙ «МОНТАЖНОЕ ИЛИ» И ДОПОЛНИТЕЛЬНЫМ РЕГИСТРОМ

А.А. Шилов, Ю.Б. Часовникова, студенты ФВС
ТУСУР, г. Томск, КИБЭВС

Блок обработки данных (БОД) включен в ядро микропроцессора системы и входит в состав регистрового АЛУ, БОД предназначен для непосредственного исполнения микроопераций. Блок обработки данных структурно подразделяется на файл регистров общего назначения (РОН R0-R7), приемники из шины BUS3, передатчики шины BUS3, дополнительный регистр для хранения первого операнда команды, арифметико-логического устройства (АЛУ), предназначенного для выполнения 16 операций, регистра результата (RGR), регистра кода операции (PMS) и устройства управления. К устройству управления относятся регистр адреса PA и два дешифратора (рис. 1).

Файл РОН подключается к арифметико-логическому устройству по входу и выходу через управляемые внутренние общие шины (BUS) с использованием логики «Монтажное ИЛИ».

В блок обработки данных включены 8 шестнадцатиразрядных регистров R0-R7, чтение и запись в которые синхронизируется управляющими сигналами y3, y18 соответственно.

Шина BUS2 используется для чтения данных с регистров и передачи их на обработку. Шина BUS3 – для записи данных на регистры.

Дополнительный регистр в схеме включения АЛУ подразумевает временное мультиплексирование при подаче операндов на входы АЛУ. В первом цикле интерпретации команды будет произведено чтение второго операнда команды (если команда содержит два операнда) в допол-

нительный регистр, а во втором цикле подача первого операнда будет произведена непосредственно на вход АЛУ.

Таким образом, использование дополнительного регистра позволяет обойтись применением одного регистра адреса, который адресует в один момент времени один регистр РОН.

Регистр кода операции PMS сохраняет и передает дешифрованный код операции на вход кода операции АЛУ. Регистр результата RGR сохраняет результат выполнения операции с выходов АЛУ и загружает данными шину BUS3, откуда их можно передать на регистры РОН или рабочие регистры РА или RD1 и далее в канал.

Направление информационных потоков в порт ввода вывода и блок обработки данных различают по старшему разряду адреса a_3 a_2 a_1 a_0 в регистре РА. Если в a_3=1 единица указывает на порт ввода – вывода, a_3=0 – соответственно на блок обработки данных.

В соответствии с теорией алгоритмов процесс интерпретации команды состоит в передаче, приеме, хранении и обработке набора данных. В формате команд имеются ссылки на регистры общего назначения (РОН) из списка R(0-7) как ресурс процессора и адреса (данные) памяти комплекса. При этом операционный автомат (регистровое арифметико-логическое устройство – РАЛУ) процессора имеет аппаратные средства чтения содержимого регистров и записи на регистр, а также обработки данных этих регистров (например, команда ADD).

Запись или чтение при работе с регистрами, а также пересылки данных синхронизованы управляющими сигналами, которые представлены битами формата микрокоманды на каждом шаге интерпретации команды программы пользователя.

Для записи данных на регистры, в регистр адреса со стороны порта ввода/вывода подается адрес регистра РОН, в который будет производится запись, и управляющий сигнал y18 на вход синхронизации дешифратора, выходы которого соединены с входами синхронизации регистров РОН.

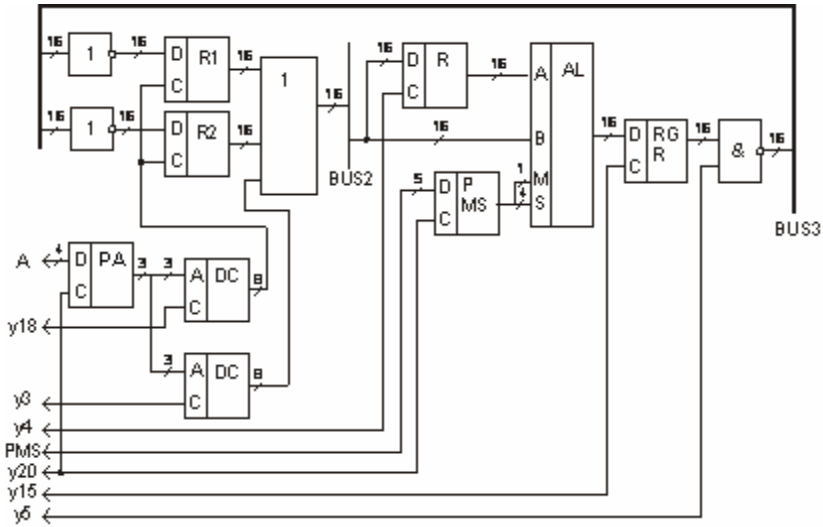
Для чтения данных с регистров на регистр адреса также подаются адрес регистра РОН и сигнал синхронизации y3 на вход дешифратора, выходы которого соединены с передатчиками на шину BUS2.

Рассмотрим пример интерпретации команды ADD R1,R2 блоком обработки данных. Перед началом интерпретации данные должны содержаться в регистрах R1 и R2.

Интерпретация команды ADD R1,R2 разделена для выполнения трех микроопераций блока обработки данных:

1. Чтение адреса регистра R1 в регистр адреса, одновременно подача синхронизующего сигнала y3 на вход дешифратора и сигнала синхро-

низации на вход дополнительного регистра y4, для записи второго операнда команды.



Структурная схема блока обработки данных с управляемой шиной «Монтажное ИЛИ» и дополнительным регистром

2. Чтение адреса регистра R2 в регистр адреса, синхронизация чтения по сигналу y3 и прием регистром PMS кода операции (ADD) также синхронизуемый своим управляющим сигналом y20. Исполнение арифметико-логическим устройством операции над двумя операндами (второй операнд в дополнительном регистре, первый операнд непосредственно подается на вход АЛУ). Запись результата в регистр результата (RGR) по сигналу синхронизации y15.

3. Передача данных с регистра результата RGR в регистр–приемник R2. Для этого в регистр адреса сохраняется адрес регистра R2, а на вход дешифратора подается сигнал синхронизации y18, что разрешает запись в регистр R2. Чтение по шине BUS3 в регистр R2 с регистра результата RGR синхронизируется сигналом y5.

В результате исполнения микроопераций в регистре R2 будет находиться результат сложения содержимого R1 и R2.

Литература

1. *Прищепа Л.С.* Проектирование центральных и периферийных устройств ЭВС: Учеб. пособие. Ч. 1. Разд. 2.

2. *Прищепа Л.С.* Компьютерные средства в системах автоматизации и управления: Учеб. пособие. Ч. 1.

КОМПЬЮТЕРНЫЙ ОСЦИЛЛОГРАФ НА БАЗЕ ЛАБОРАТОРНОГО СТЕНДА SDK 1.1

В.Н. Сидоренко, студент 5-го курса ФВС
ТУСУР, г. Томск, vitekbatek@gmail.com

В последние годы в связи с «всеобщей компьютеризацией» значительно возрос интерес к так называемым виртуальным приборам – измерительной аппаратуре, выполненной на базе плат ЦАП–АЦП и использующей в качестве устройства управления и отображения обычный персональный компьютер (ПК). И это не просто дань моде, такие приборы обладают рядом достоинств по сравнению с аналоговыми предшественниками. Они предоставляют возможность создания компактной, мобильной, гибкой и недорогой измерительной системы, пригодной для решения широкого круга задач в самых различных областях.

В частности, осциллограф АСК–3105, занимая всего отсек «5,25» дисковода, позволяет наблюдать форму сигнала с использованием двух независимых каналов в полосе частот от 0 до 100 МГц, имеет аппаратный буфер памяти на 65535 выборок для каждого канала и позволяет проводить спектральный анализ выделенного участка сигнала [3].

В предлагаемой статье рассматривается компьютерный осциллограф построенный на базе лабораторного стенда SDK 1.1, разработанный согласно требованиям задания.

Обобщенная структурная схема цифровых осциллографов приведена на рис. 1.

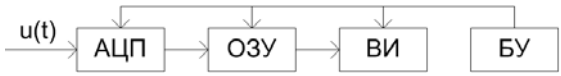


Рис. 1. Обобщенная структурная схема цифровых осциллографов.

Блок управления (БУ) отвечает за взаимодействие всех структурных единиц схемы. Аналого-цифровой преобразователь (АЦП) служит для преобразования непрерывного сигнала в цифрую форму. Оперативное запоминающее устройство (ОЗУ) позволяет запомнить весь массив значений U(t), поступающих в виде кодов с АЦП, а также необходимую служебную информацию. Визуальный индикатор (ВИ) служит для визуального представления результата [2].

Анализ технических средств лаборатории показал возможность создания такого цифрового осциллографа на базе учебно-лабораторного стенда SDK 1.1. Стенд реализован на микроконтроллере ADuC 842 и содержит необходимые структурные единицы: АЦП и ОЗУ размером 128 кБ. Характеристики АЦП приведены в таблице. Наличие оптически развязанного приемопередатчик инструментального канала RS232 позволяет передавать данные с SDK 1.1 на ПК по средствам COM-порта [1].

Характеристики АЦП стенда SDK 1.1

Кол-во разрядов	12
Диапазон входных напряжений	0…Vref
Входной ток	±1мкА
Входная емкость	32пФ
Кол-во выборок	400К/с

Структурная схема разрабатываемого комплекса представлена на рис. 2.

Рис. 2. Структурная схема комплекса

Так как данный АЦП позволяет работать только с однополярным сигналом, был разработан адаптер, позволяющий производить измерения сигнала разной полярности в диапазоне от ±1 до ±500 вольт. Наряду с этим, адаптер обеспечивает защиту входа АЦП от высокого напряжения и короткого замыкания.

На SDK 1.1 возложены следующие функции: выполнение аналого-цифрового преобразования, сохранение результатов в ОЗУ, передача результата через последовательный интерфейс RS232 в ПК. Преобразования могут быть как однократными, так и многократными с определенным числом выборки. Максимально возможное количество определено размером ОЗУ стенда и составляет 65535.

Персональный компьютер предназначен для установки настроек преобразований, и отображения результата в графической форме.

Литература

1. Учебный стенд SDK 1.1: Руководство пользователя. 2001. 99 с.
2. *Довгяло Д.А.* Лекции по метрологии. 2008. 91 с.
3. http://www.eliks.ru/product/vi/virpr.htm

СОЗДАНИЕ СИСТЕМЫ СТАБИЛИЗАЦИИ НЕУСТОЙЧИВОГО ОБЪЕКТА

А.В. Вельганюк, В.В. Курганкин, магистранты 5-го курса;
С.В. Замятин, к.т.н.; В.И. Гончаров, д.т.н., профессор
ТПУ, г. Томск, outcold@sibmail.com

Введение. Проблема управления неустойчивым объектом затрагивает широкий спектр задач – наблюдаемость, достижимость, устойчивость, аналитический синтез регуляторов и т.д. К системе и закону

управления неустойчивым объектом предъявляются более высокие требования, чем для объекта устойчивого. В данной работе рассматривается проблема по созданию установки, позволяющей демонстрировать особенности управления неустойчивым объектом. В качестве такого объекта принят шар, находящийся в верхней части профилированного колеса (рис. 1). Незначительные отклонения шара от положения равновесия приводят к его движению с ускорением вниз по желобу колеса. Для противодействия силам гравитации и сохранения положения шара в окрестности заданной точки имеется электромеханический привод, который позволяет вращать колесо в направлении, обеспечивающем стабилизацию положения шара. Для рассматриваемой установки были проведены кинематические и конструктивные расчеты [1], моделирование системы управления, созданной на базе двигателя постоянного тока [2]. В настоящей работе продолжается рассмотрение вопросов, связанных с согласованием различных компонентов системы друг с другом, их взаимное сопряжение, синтез и реализация регуляторов, написание программ обработки сигнала измерительного органа, изготовление установки.

1. Задача системы управления. Механическая часть объекта представляет собой систему твердых тел, движение которых определяется связями между ними. Назначение системы управления – удержание шара в верхней точке колеса путем приложения к последнему вращающего момента.

2. Состав и назначение отдельных элементов системы. Для реализации системы управления был разработан стенд, представленный на рис. 2.

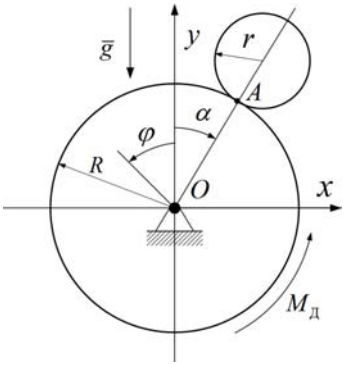


Рис. 1. Геометрические иллюстрации

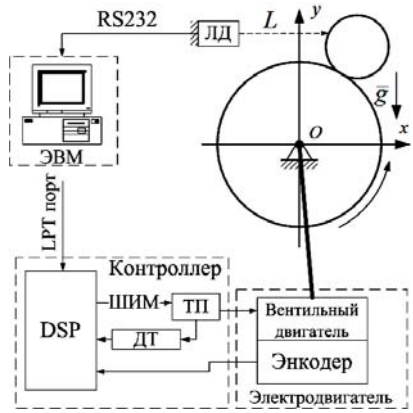


Рис. 2. Схема установки

При аппаратной реализации системы были использованы следующие элементы:

– лазерный датчик серии РФ603 фирмы Рифтэк (Республика Беларусь);

– вентильный двигательный со встроенным энкодером EzM-56L (Корея);

– контроллер Ezi-Servo EzS-PD-56M, имеющий транзисторный преобразователь, датчик тока и сигнальный процессор (Республика Корея):

ТП – транзисторный преобразователь; ШИМ – широтно-импульсная модуляция; DSP – цифровой процессор (digital signal processor);

– персональный компьютер с программным обеспечением на базе Windows XP;

– в качестве объекта управления был выбран резиновый мяч радиусом 80 мм и колесо радиусом 185 мм, изготовленное из материала, обеспечивающего малый момент инерции.

3. Задачи сопряжения отдельных узлов системы. Одной из основных задач, рассматриваемых в данной работе, является сопряжение сигнала лазерного дальномера и контроллера управления двигателем. Выходным сигналом лазерного дальномера, характеризующим расстояние до объекта, является бинарное число, передаваемое по последовательному COM порту. Сигналом для управления двигателем является последовательность импульсов, количество которых соответствует углу поворота вала. Причем контроллер воспринимает информацию в виде последовательности импульсов, которые подаются по двум каналам. Разность импульсов с первого канала и второго позволяет контроллеру определить текущее положение мяча.

Для сопряжения этих сигналов были разработаны алгоритмы, программно реализованные в среде разработки приложений Delphi.

4. Система управления. Система управления на базе контроллера Ezi-Servo EzS-PD-56M реализована в виде двухконтурной системы подчиненного регулирования. Упрощенная структурная схема системы представлена на рис. 3.

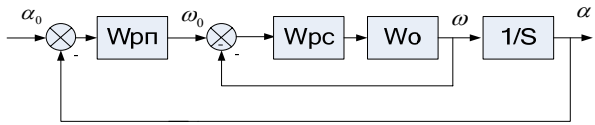


Рис. 3. Упрощенная структурная схема: Wрп – передаточная функция регулятора положения; $W_{рс}$ – передаточная функция регулятора скорости; $W_{дв}$ – передаточная функция двигателя; $W_{оу}$ – передаточная функции объекта управления

Передаточная функция регулятора положения и регулятора скорости представляют собой П и ПИД регуляторы соответственно.

На основе разработанной модели объекта были рассчитаны параметры регуляторов. В процессе экспериментальной настройки системы расчетные коэффициенты были уточнены.

Заключение. В работе рассмотрено создание системы управления неустойчивым объектом типа «мяч на колесе». Основными сложностями, возникшими при реализации данной системы, являются задачи сопряжения устройств и синтеза регуляторов системы управления. Так же рассматриваемый объект управления, в отличие от устойчивых объектов, требует значительно более точной настройки параметров регуляторов.

Литература

1. *Гладышев К.Н.* Разработка системы управления неустойчивым объектом. Томск: ТПУ, 2005.

2. *Курганкин В.В.* Разработка системы управления скоростью двигателя BG60. Томск: ТПУ. 2007.

МОДЕЛЬ КОНТРОЛЯ ЗНАНИЙ НА ОСНОВЕ СЕМАНТИЧЕСКОЙ СЕТИ

Л.Н. Жеребцова, студентка 5-го курса ФВС

ТУСУР, г. Томск, fashion_women@mail.ru

Вступление человечества в XXI в. требует перехода к новой стратегии развития общества на основе знаний и высокоэффективных технологий. Соответственно обеспечение эффективности системы образования – одна из важнейших задач. Внедрение компьютерных технологий в процесс обучения позволяет:

– полностью провести весь курс обучения по определенной дисциплине на компьютере (включая лекции, практические занятия и контроль усвоения материала);

– избавить студента от процедуры поиска и покупки книг;

– оперативно редактировать лекционный материал с учетом новых данных, которые появляются в конкретной предметной области, в том числе и через вычислительные сети;

– совершенствовать методы изложения материала на основе анализа результатов периодического тестирования студентов по каждой теме;

– предоставлять студентам возможности изучать лекционный материал и выполнение практических заданий в домашних условиях.

При разработке обучающей программы очень важно использовать весь арсенал технологических средств, предоставляемых современными информационными технологиями. Обучающая программа особенно эффективна в тех случаях, когда она:

– обеспечивает практически мгновенную обратную связь, т.е. является интерактивной;

– помогает быстро найти необходимую информацию;

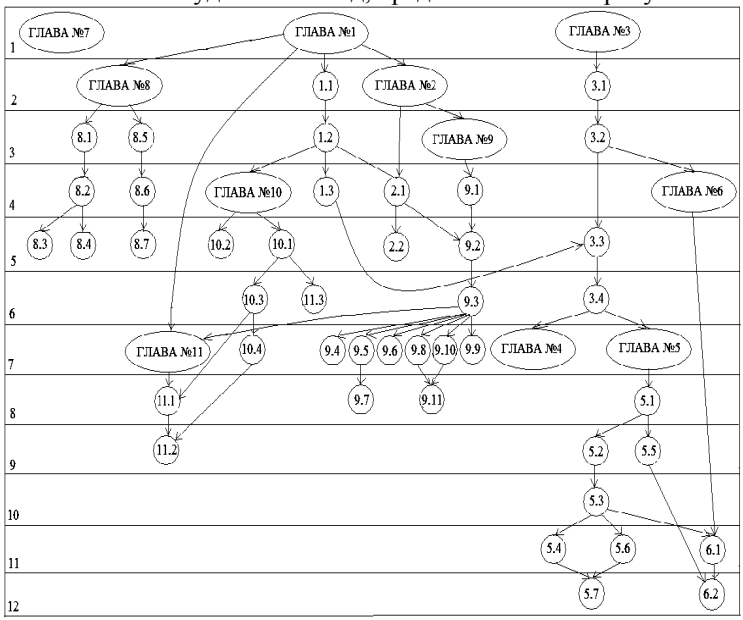
– существенно экономит время при многократном обращении к гипертекстовым объяснениям;

– не просто выводит текст на экран, но и рассказывает, показывает, моделирует и т.д. – именно здесь проявляются возможности и преимущества мультимедийных технологий;

– позволяет быстро, но в темпе, наиболее подходящем для конкретного индивидуума, проверить знания по определенному разделу.

Существует много различных методов построения обучающих программ. В данной работе рассматривается построение обучающих программ на основе семантической сети.

На основании определений семантической сети и понятийной структуры, составим для дисциплины «Дискретная математика» семантическую сеть, основываясь на системе понятий, и представим ее в виде графа. В качестве узлов семантической сети возьмем разделы дисциплины «Дискретная математика» (главы, пункты, подпункты). Определим отношение между узлами: изучение раздела А зависит от изучения раздела В или для изучения раздела В необходимо знание раздела А, тогда семантическая сеть будет иметь вид, представленный на рисунке.



Семантическая сеть для дисциплины «Дискретная математика»

Из рисунка видно, что для полноценного изучения главы №2 дисциплины, необходимо изучить основные понятия главы №1 и т.д. Семантическая сеть расположена по уровням. Обозначим узлы, изучение которых не зависит от других узлов, как «открытые». Открытыми узлами, также будем называть узлы, изучение которых зависит от других узлов, но они уже были изучены студентом. Например, глава №6 будет открытой для изучения, если изучены подпункты 3.1, 3.2, и глава №3. Обозначим узлы, изучение которых зависит от других узлов, как «закрытые». Например, изучение главы №9 зависит от изучения глав №1, №2. Значит, глава №9 является закрытой для изучения, до тех пор, пока студент не изучит предыдущие главы и подпункты. Так как любой узел соответствует теме, то понятия открытых и закрытых тем относятся также и к ним.

Первый уровень представим как открытые темы для изучения студентами, то есть те темы, которые студент может изучить на базе тех знаний, которые он в процессе обучения. Далее уровни будем размещать по мере открытости тем для рассмотрения студентами. Если студент не изучил открытую тему на первом уровне, он не может приступить к изучению следующей темы из-за недостатка знаний, которые мог получить открытую тему. Следовательно, получаем семантическую сеть, представленную в виде графа, каждый подпункт которой связан с предыдущим и последующим.

Для представления структуры данных семантической сети используем структуру данных типа матрицы R_{mxn} (1, если изучение *i* темы зависит от *j* столбца; 0, в противном случае).

На основании данных семантической сети, изображенной на рисунке 1, формируем матрицу соответствия. Если 1 в столбце матрицы соответствия, то этот раздел входит или необходим для изучения раздела *N*, который указан в строке. На время обучения создается дубликат таблицы, а в векторе обнуляются столбцы, соответствующие разделы которых были изучены. Тогда, проводя анализ строки символов, можно найти неизученные темы, если код равен 1. Каждому студенту ставится в соответствие вектор обученности, в котором 0 – кодируется изученная тема, 1 – неизученная тема. На время обучения для студента формируется дубликат матрицы $\mathbf{R}_{mxn}$, в котором нулем отмечены все изученные темы.

Преподаватель имеет возможность просмотреть их качество и сделать выводы относительно корректировки курса или индивидуальных занятий с отстающими. Система хранит информацию в течение всего периода обучения для проведения анализа динамики знаний учащихся. В идеальном варианте эти данные хранятся на протяжении всего времени, в течение которого читается курс, и служат основой для оценки и возможной корректировки курса.

Литература

1. *Башмаков И.А., Рабинович П.Д.* К вопросу о концепции информатизации учебного процесса.

2. *Соболева Т.С., Чечкин А.В.* Дискретная математика: Учебник для студ. ВУЗов. М.: Академия, 2006. 256 с.

3. *Давыдова Е.М., Леденева Т.М., Мещеряков Р.В., Подвальный С.Л.* Дискретная математика: Учебник. 2-е изд., перераб. и доп. Томск: В-Спектр, 2006. 288 с.

ОБУЧАЮЩИЕ СИСТЕМЫ ПО ДИСЦИПЛИНЕ «ДИСКРЕТНАЯ МАТЕМАТИКА»

Л.Н. Жеребцова, студентка 5-го курса ФВС

ТУСУР, г. Томск, fashion_women@mail.ru

При переходе к новой стратегии развития общества на основе знаний и высокоэффективных технологий, одной из важнейших задач, является обеспечение эффективности системы образования.

Студенты должны знать и уметь использовать конечные функциональные преобразователи (в частности, владеть булевой алгеброй, теорией исчисления высказываний и предикатов), основы теории кодирования и математических методов сжатия информации, а также основы криптографии.

Одним из важных структурных элементов каждого занятия и всего процесса обучения в целом является проверка знаний и умений учащихся. Она всегда находится в зоне пристального внимания преподавателя, свидетельствует о результатах обучения. Преподаватель добивается от студентов полного понимания пройденного материала. В помощь преподавателям и студентам пишутся обучающие программы с системой контроля знаний учащихся.

Для оптимальной и удобной работы программы по дисциплине «Дискретная математика» необходимо выявить критерии, позволяющие исследования построить таким образом, чтобы в результате работы была построена модель, удобная в применении не только для студента, но и для преподавателя.

В первую очередь, в разрабатываемой программе должны быть представлены все основные разделы и темы по дискретной математике, такие как:

– теория множеств,
– отношения,
– нечеткие множества,
– логика высказываний,
– булевы функции,
– комбинаторика,
– кодирование,
– графы.

Причем в программе эти темы будут представлены в виде тем или лекций. Обязательным материалом должны быть: теоретическая часть, примеры решения задач, рисунки, показывающие наглядно выполнение поставленной задачи; после каждой пройденной студентами темы им будет предложено выполнить тестовые задания для закрепления материала.

К настоящему времени уже хорошо известны компьютерные дидактические программы следующих типов:

– контролирующие программы – предъявляют задания в учебной среде (возможно игровой), в которой обучаемый должен достигнуть заданных целей путем планирования и выполнения некоторых действий;

– обучающие программы – предъявляют обучаемому учебный материал и вопросы, на которые он должен дать ответы;

– моделирующие программы – требуют от обучаемого воспроизведения последовательности рассуждений или «сборки» правильного результата на основе знаний, предоставленных системой (интеллектуальные системы поддержки рассуждений учащихся), например, программы для построения рисунков на экране компьютера;

– программы тренажеры – служат для отработки и закрепления технических навыков решения задач. Они должны обеспечивать получение информации по теории и приемам решения задач, тренировку на различных уровнях самостоятельности, контроль и самоконтроль;

– дидактические игры – выдают ответы обучаемому на формируемые им вопросы, используя игровой процесс;

– гипертекстовые системы – в основном представляют собой мультимедийные справочники, в которых хорошо реализована система навигации и поиска информации.

Контроль знаний в обучающей системе строится следующим образом:

– регистрация (ввести пароль и выбрать тему для изучения);

– так как структура вопроса строится в форме теста, то студент должен либо выбрать правильный ответ, либо ввести его;

– студент может вернуться к предыдущему вопросу, а также перейти к следующему, либо может выйти из режима контроля;

– после того как студент выполнил все задания, ему автоматически выставляется оценка, либо выдается процент количества правильных и неправильных ответов;

– программа построена таким образом, что студент сначала изучает необходимый материал для решения задач и только потом ему предлагается проверить свои знания и умения в решении задач. Программа строится на основе семантической сети.

Тест в разрабатываемой программе будет представлять собой совокупность вопросов по пройденной теме данной дисциплины. Вопросы будут как в форме теста, но на некоторые вопросы необходимо будет вписать правильный ответ. Обучающая программа будет показывать

студенту, на сколько вопросов ему еще надо ответить, и на сколько он уже ответил, причем количество правильных и неправильных ответов студент будет видеть на экране. Студенту предоставляется возможность при решении задач использовать материал, необходимый для решения. После проведения тестового опроса студенту выставляется автоматически оценка, на которую он освоил данный материал. Время для проверки знаний студента тоже будет ограничено, будет показываться, сколько времени прошло и сколько осталось на выполнение задания.

Обучающие программы очень удобны и практичны, потому что студент сначала наглядно может посмотреть решение задач на примерах уже прорешенных и сам по аналогии сможет потренироваться, а впоследствии напишет тест. Эта система контроля знаний достаточно удобна и для преподавателя, и для студента. Преподаватель может на основании результатов тестов смело сказать, какую тему студент разобрал, а с какой еще нужно поработать. Таким образом, на основе этой программы можно выявить статистику успеваемости студентов по данной дисциплине.

Литература

1. *Губарев В.В.* Информатика в рисунках и таблицах (фрагменты системного путеводителя по концептуальным основам): Учеб. пособие. Новосибирск: Изд-во НГТУ, 2003. 198 с.

2. *Аванесов В.С.* Теория и методика педагогических измерений.

3. *Давыдова Е.М., Мещеряков Р.В.* Дискретная математика: Учеб. пособие. Томск: ТУСУР, 2004. 181 с.

ИССЛЕДОВАНИЕ РОБАСТНОСТИ ДВУСВЯЗНЫХ СИСТЕМ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ

О.В. Злобина, А.А. Антропов

Томский политехнический университет, e-mail: goodok20@ya.ru

В работе приводятся результаты исследования робастности двусвязной системы автоматического управления (ДСАУ) в отношении перерегулирования и взаимовлияния каналов, а также поиск путей улучшения этих характеристик.

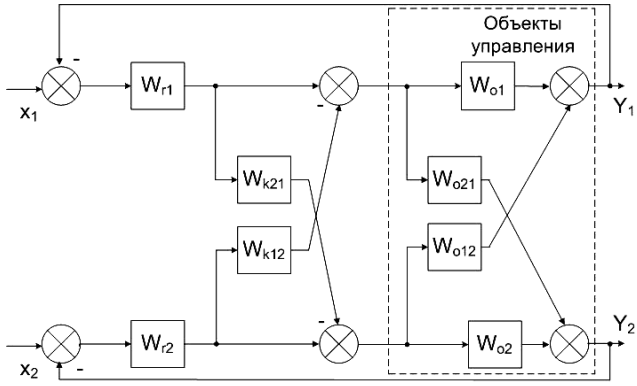
Постановка задачи

Рассматривается система управления двухконтурным турбореактивным двигателем [1], структурная схема которой представлена на рисунке.

Обозначения и передаточные функции (ПФ) элементов:

$W_{o1}(s)=\frac{3{,}4(0{,}4s+1)}{0{,}38s^2+1{,}1s+1}$, $W_{o2}(s)=\frac{0{,}9(1{,}1s+1)}{0{,}38s^2+1{,}1s+1}$ – ПФ прямых канналов

объекта управления (ОУ), $W_{o21}(s)=\dfrac{0{,}18(1{,}13s+1)}{0{,}38s^2+1{,}1s+1}$, $W_{o12}(s)=\dfrac{6{,}8(0{,}55s+1)}{0{,}38s^2+1{,}1s+1}$ – ПФ перекрестных связей ОУ, $W_{r1}(s), W_{r2}(s)$ – ПФ регуляторов, $W_{k12}(s), W_{k21}(s)$ – ПФ компенсаторов.



Структурная схема ДСАУ

Регуляторы и компенсаторы ДСАУ были синтезированы в [2] на основе ВИМ [3] и принципа автономности контуров [4]: $W_{k12}(s)=\dfrac{1{,}1s+2}{0{,}4s+1}$, $W_{k21}(s)=\dfrac{0{,}226s+0{,}2}{1{,}1s+1}$, $W_{r1}(s)=\dfrac{0{,}23s^2+0{,}69s+0{,}64}{0{,}27s^2+s}$,

$W_{r2}(s)=\dfrac{1{,}09s^2+2{,}74s+2{,}4}{1{,}01s^2+s}$.

Синтезированная ДСАУ отвечает заданным требованиям: перерегулирование σ отсутствует, время регулирования t_p не превышает 2 с, взаимовлияние каналов не превышает 5%. Оценивание последнего из параметров проводилось по формуле, которая, к примеру, в случае определения влияния второго канала на первый имеет вид: $\mu_{21}=\max\limits_t|h_1(t)|$, где $h_1(t)$ – переходная характеристика первого канала при отсутствии сигнала на его входе $x_1(t)\equiv 0$ и единичном ступенчатом воздействии на входе второго канала $x_2(t)\equiv 1(t)$.

Задача настоящей работы состоит в поиске таких регуляторов, которые бы обеспечивали, во-первых, робастность системы по перерегулированию в условиях изменения КУ ОУ в пределах ±10% и, во-вторых, в рассмотрении мер, обеспечивающих снижение взаимовлияния каналов.

Исследование робастности ДСАУ

Для решения поставленной задачи были проведены исследования зависимостей перерегулирования и влияния каналов друг на друга при изменении КУ прямых каналов ОУ.

Проведенные исследования показали, что:

– значительная чувствительность системы проявляется лишь в первом канале,

– величины перерегулирования σ и влияния μ_2 возрастают до недопустимого уровня при изменении КУ ОУ,

– рассматриваемая ДСАУ является робастной в очень узком диапазоне изменения параметров ОУ.

Предыдущий опыт синтеза систем [3] показал, что робастность в сильной мере зависит от желаемого времени регулирования. Для проверки возможности использования этих знаний в данной задаче были проведены эксперименты для следующих сочетаний изменения параметров, увеличение или уменьшение которых отражается стрелкой, направленной соответственно вверх или вниз: 1) $t_{p1} = 2$ с, $t_{p2}\downarrow$, 2) $t_{p1}\downarrow$, $t_{p2} = 2$ с, 3) $t_{p1}\downarrow$, $t_{p2}\downarrow$.

Результаты эксперимента сведены в таблицу.

Изменение величин σ и μ_{21} в зависимости от изменения t_{p1} и t_{p2}

	Изменение величины σ	Изменение величины μ_{21}
1. $t_{p1} = 2$ с, $t_{p2}\downarrow$	$\sigma\downarrow$	$\mu_{21}\uparrow$
2. $t_{p1}\downarrow$, $t_{p2} = 2$ с	$\sigma\uparrow$	$\mu_{21}\downarrow$
3. $t_{p1}\downarrow$, $t_{p2}\downarrow$	$\sigma\downarrow$, но меньше, чем в случае сочетания 1	$\mu_{21}\downarrow$, но меньше, чем в случае сочетания 2

Полученные результаты показывают, что в рассматриваемой системе можно добиваться повышения уровня робастности за счет изменения желаемого быстродействия. Однако эти возможности весьма ограничены для рассматриваемой структуры ДСАУ. Поэтому нужно искать другие варианты повышения робастности, вероятнее всего, они будут основаны на иных структурных решениях.

Заключение. В работе приведены результаты поиска путей придания автономной ДСАУ наибольшего запаса робастных свойств. Однако указанный способ не всегда реализуем. Возможные варианты поиска эффективных решений связаны с исследованиями ДСАУ на основе иных вариантов наложения компенсационных связей для расширения границ робастности.

Литература

1. *Методы* классической и современной теории автоматического управления: Учебник: 5 т.; Т. 3: Синтез регуляторов систем автоматического управления

/ Под ред. К.А. Пупкова, и Н.Д. Егупова. М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. 616 с.

2. *Злобина О.В., Антропов А.А., Гончаров В.И.* Синтез двусвязных систем автоматического управления на основе принципа автономности с применением вещественного интерполяционного метода / Труды VI Всерос. науч.-практ. конф. «Молодежь и современные информационные технологии». 2008. (в печати).

3. *Гончаров В.И.* Синтез электромеханических исполнительных систем промышленных роботов: Учеб. пособие. Томск: Изд. ТПУ, 2002. 100 с.

4. *Морозовский В.Т.* Многосвязные системы автоматического регулирования. М.: Энергия, 1970. 288 с.

СИГНАЛИЗИРУЮЩАЯ ПОДСИСТЕМА ПОДАЧИ ДАВЛЕНИЯ

А.А. Лазичев, к.т.н., доцент каф. ПМИ ТУСУР;
Ю.А. Самулеева, студентка 5-го курса ФВС ТУСУР
ТУСУР, г. Томск, lazan@mail.ru.

Для увеличения конкурентоспособности манометрической продукции в условиях современного рынка требуется одновременно решать сразу две задачи: повышать качество манометров и снижать их себестоимость [1]. Достигнуть таких результатов можно в том числе и за счет внедрения автоматизированного комплекса, ускоряющего выпуск продукции и снижающего участие человека в производственном процессе. Примером этого комплекса может служить проектируемая система автоматизированной настройки манометров при помощи нанесения шкал.

Работу автоматизированной системы настройки манометров при помощи нанесения шкал можно представить следующим образом (см. рисунок). Тестируемые манометры устанавливаются в специальные держатели – цапфы для подачи давления. Напротив каждого тестируемого манометра устанавливается видеокамера, связанная через устройство ввода видеоданных с персональным компьютером. Камеры передают изображения положения стрелки в заданные моменты времени. Видеопоток в компьютер передается непрерывно с некоторой частотой кадров, однако для анализа нужны не все кадры, а только отвечающие определенным моментам времени, т.е. соответствующие некоторым определенным значениям давления. Вычислительные алгоритмы, предназначенные для предварительной (подготовительной) обработки видеоданных и определения угла поворота стрелки, формируют массивы данных, по которым сначала в памяти компьютера формируется образ манометрической шкалы, а затем он, при помощи принтера, выводится на металл. Таким образом, в автоматизированной системе настройки манометров при помощи нанесения шкал выделяются четыре подсистемы:

1. Сигнализирующая подсистема подачи давления.
2. Подсистема ввода видеоданных.

3. Алгоритмы преобразования и определения положения стрелки тестируемых манометров.

4. Подсистема нанесения шкал.

1 – Клапан сброса давления в системе
2 – Клапан подачи давления в систему
3 – Система подачи давления к тестируемым манометрам
4 – Датчик текущего давления в системе
5 – Тестируемые манометры
6 – Видеокамеры
7 – Плата ввода видеоданных с камер в ПК
8 – Универсальный принтер для печати шкал
УСУЗ – Устройство сопряжения и управления задвижками клапанов
ПО СП – Программное обеспечение сигнализирующей подсистемы

Подсистема подачи давления является, пожалуй, одним из наиболее важных элементов рассмотренной системы автоматизации, обеспечивающей ее работоспособность. Поэтому в данной работе рассматривается создание именно этой системы.

Сигнализирующая подсистема подачи давления для автоматизации сборки и настройки манометров предназначена для непрерывного контроля давления, подаваемого на тестируемые манометры. Исходную подсистему можно разделить на две части:

1. Непосредственно блок подачи/сброса давления.
2. Блок контроля текущего давления и сигнализации.

Блок подачи/сброса давления состоит из насосной станции, трубопровода и двух клапанов, один из которых работает на подачу, а другой – на сброс давления. Система сбора и обработки информации контролирует давление, подаваемое непосредственно на манометры, и выдается управляющее воздействие на вентиль сброса и подачи при избытке и недостатке давления соответственно. Идея функционирования автоматической подсистемы подачи давления основывается на управлении положением вентилей подачи/сброса давления. Управляющий сигнал с ПК поступает на двигатель, задающий положение вентилей. Подаваемое/сбрасываемое давление напрямую зависит от угла поворота («открытия») вентиля: чем меньше угол, тем медленнее подается давление. Управление углом поворота вентилей осуществляется при помощи шагового двигателя через шестерни или редуктор. Рассмотрим следующую часть подсистемы подачи/сброса давления – блок сбора и обработки информации, принцип функционирования которой заключается в следую-

щем: датчик фиксирует текущее значение давления в системе и передает его значение через устройство сопряжения в ПК. При достижении заданного значения программа подает управляющий сигнал в подсистему ввода видеоданных.

Сформулируем требования к датчику, который используется в блоке сбора и обработки информации:

1. Наличие индикации текущего давления.
2. Наличие цифрового интерфейса.
3. Быстродействие.
4. Верхний предел показаний датчика должен быть не менее верхнего предела измерений манометров.
5. Предел допускаемой основной погрешности датчика должен быть не более 0,25 предела допускаемой основной погрешности манометра.

Исходя из вышеперечисленных требований, наиболее целесообразным видится использование цифрового прецизионного манометра ДМ5002.

Следует отметить, что в разрабатываемой подсистеме подачи давления управление клапанами будет осуществляться автоматически, в отличие от уже существующих систем. Для выбора электродвигателя необходимо определить крутящий момент, который нужно приложить к регулировочному крану для его открытия (закрытия), что соответствует подаче (сбросу) давления. Воспользовавшись динамометром и рычагом, подсчитаем, что крутящий момент равен 35 [кгс·см] или 3,5 [Нм]. Относительная погрешность определения момента при этом равна 3,601%, что составляет 1,26 [кгс·см] или 0,126 [Нм]. При обзоре существующих на рынке видов двигателей делаем вывод, что для нашей системы наиболее пригодными являются шаговые двигатели. Для снижения стоимости системы необходимо использовать двигатель с меньшим крутящим моментом по сравнению с измеренным. Следовательно, нужно рассчитать параметры редуктора, который обеспечит увеличение крутящего момента в десять раз. В итоге получаем, что количество зубьев ведущей шестерни $z_1 = 9$, а ведомой шестерни соответственно равно $z_2 = 90$. Диаметр ведущей шестерни $d_1 = 7{,}2$мм, диаметр ведомой шестерни $d_2 = 72$мм [2].

Следовательно, наиболее подходящим двигателем является FL42STH38 из-за его небольшой цены, малой погрешности и по соответствию его крутящего момента и момента, необходимого нам для управления регулировочным краном. Управление будет осуществляться программно при помощи блока управления шаговым двигателем с ПК.

Литература

1. *Кузнецов А.А.* Автоматизированный измерительно-технологический комплекс для автоматизированной настройки манометров: Дис. … канд. техн. наук: / Том. гос. ун-т систем управления и радиоэлектроники. Томск, 2004. 149 с.

2. *Кудрявцев В.Н., Державец Ю.А., Глухарев Е.Г.* Конструкции и расчет зубчатых редукторов. Л.: Машиностроение. Ленингр. отд-ние, 1971. 328 с.

СЕКЦИЯ 12

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель – **А.А. Шелупанов,** зав. каф. КИБЭВС, д.т.н., проф.*
*зам. председателя – **Р.В. Мещеряков,** к.т.н., доц. каф. КИБЭВС*

СТРУКТУРА КВАДРАТА НАТУРАЛЬНОГО ЧИСЛА. СВОЙСТВА. СЛЕДСТВИЯ

М.С. Афанасьева, студентка РТФ; А.Н. Колесов, к.т.н., доц.
каф. СРС, ТУСУР, г. Томск, mrc@main.tusur .ru

1. Исходные предпосылки и соглашения

Ниже, если не оговорено другое, под числом понимается натуральное число, под корнем – корень квадратный из натурального числа, под степенью числа – вторая степень числа (квадрат числа) и под цифрой – цифра десятичной системы счисления.

Известная формула квадрата суммы N слагаемых [1] в применении к числу (основанию) B из N цифр b_i, записанная в виде

$$B^2 = \left(\sum_{i=1}^{N} b_i \cdot 10^{i-1}\right)^2 = \sum_{i=1}^{N}\left(b_i \cdot 10^{i-1}\right)^2 + \sum_{i,j=1}^{N} (2\cdot(b_i \cdot 10^{i-1})\cdot(b_j \cdot 10^{j-1})) \ , \ i \neq j \ , \quad (1)$$

представляет конечный результат возведения B в степень, но не позволяет увидеть структуру квадрата числа B из-за громоздкости записи, а также из-за неподходящей организации входящей в нее информации. В статье цифра нулевого разряда имеет номер первый.

2. Соображения по организации анализа образования квадрата и некоторые его результаты, важные для последующих выводов

Обучение извлечению корня из чисел ограниченной величины осуществлялось в школах вплоть до середины 20-го века на базе свойств квадрата двучлена. Расширение границ вычислений – потребность новых задач. Этим объясняется нынешней интерес к теме.

Анализ процесса образования квадрата в ходе наращивания цифры старшего разряда от начала формирования квадрата до завершающей

цифры старшего разряда основания позволил увидеть некоторые закономерности в структуре квадрата, представляющие интерес при стремлении уменьшить объем вычислительной работы при обработке чисел, в том числе и больших для используемого мат. пакета.

В [2, 3] предпринимались попытки анализа окончаний произвольных чисел с целью исключения чисел, подлежащих извлечению корня, но заведомо не являющихся квадратами. Материалы статей [2, 3] и продолжение работы в направлении содержания [2, 3] привели к осознанию определенной структуры квадрата, представленной на рисунке, где объединенные ячейки в «индивидуальных» строках (инд. стр.) указывают возможные расположения цифр этих строк.

Требования на допустимый объем статьи не позволяют продемонстрировать «рождение» структурной схемы. По этой причине ограничиваемся представлением схемы, части ее свойств и применений.

Разряды основ	5		4		3		2		1	
Цифры основан	b_5		b_4		b_3		b_2		b_1	
Номера пар разрядов квадратов	5		4		3		2		1	
Разряды цифр	10	9	8	7	6	5	4	3	2	1
Квадраты цифр основания («общая» строка)	b_5^2		b_4^2		b_3^2		b_2^2		b_1^2 Инд.стр.№1	
Инд. стр. №2							$2\cdot b_2 * (b_1)$			
Инд. стр. №3					$2\cdot b_3 * (b_2 \cdot b_1)$					
Инд. стр. №4			$2\cdot b_4 * (b_3 \cdot b_2 \cdot b_1)$							
Инд. стр. №5	$2\cdot b_5 * (b_4 \cdot b_3 \cdot b_2 \cdot b_1)$									
и. т.д.										

Структура квадрата натурального числа (символы соответствуют формуле (1)). (инд. стр. №1 совпадает с «общей» строкой, так как содержит только квадрат первой цифры основания)

3. Некоторые свойства структуры, отображенной на рисунке

1) Анализ структуры показал**:** число, изображаемое двумя старшими цифрами «индивидуальной» строки, связанной с цифрой b_i основания, не может превзойти величины $(2\cdot b_i)$; число, изображаемое двумя цифрами, предшествующими только что упомянутой паре цифр, не может превысить величины 18; младшая цифра этой строки равна младшей цифре произведения $(2\cdot b_i \cdot b_1)$.

2) По структуре на рисунке отметим следующее: квадрат числа формируется из суммируемых поразрядно «индивидуальных» и «общей» строк; «общая» строка является строкой квадратов цифр основания, располагающихся в парах смежных разрядов этой строки, идущих в порядке следования цифр в основании.

3) «Индивидуальные» строки представляют собой удвоенные произведения предшествующего основания и очередной его старшей цифры. Начала этих строк (соответствующие младшей цифре произведения $(2 \cdot b_i \cdot b_1)$ и начинающиеся с разряда i) при наращивании цифр в основании сдвигаются каждый раз на один разряд в сторону больших разрядов и могут достигать разряда с номером $(2 \cdot i)$.

4) Длины строк прогрессивно нарастают с ростом номера *i* разряда старшей цифры основания. Добавление очередной цифры в старший разряд основания влечет появление новой «индивидуальной» строки.

Таким образом, в старших двух разрядах полного (окончательного) квадрата всегда максимально возможный целочисленный корень является цифрой старшего разряда основания!

При нечетном числе разрядов в исследуемом квадрате пара разрядов, соответствующая старшей цифре основания, образуется посредством приписывания нуля перед старшей цифрой квадрата.

4. Следствия анализа структуры квадрата числа и ее свойств

1) Из предыдущих пунктов вытекает простой способ демонстрации верности изложенного выше на конкретном примере**:** если иметь в своем распоряжении квадраты двух чисел *произвольной разрядности*, полученных для оснований, разнящихся только старшей цифрой, то определение основания чисел не составляет труда и может быть выполнено практически моментально, без привлечения каких-либо средств вычисления, кроме «карандаша и бумаги». Вычитание упомянутых выше квадратов «вычленяет» последнюю «индивидуальную» строку, деление которой на удвоенную разность старших цифр оснований сразу дает все цифры основания, предшествующие старшей цифре.

2) Вычитание из полного квадрата квадрата старшей цифры основания (с учетом расположения цифр на разрядной шкале) приводит к сумме последней индивидуальной строки с квадратом предшествующего основания. Механизм справедлив и для других цифр основания.

3) Поскольку вклад двух старших цифр основания в величину квадрата всегда превосходит «по удельному весу» вклад остальных цифр основания, то, вычитая квадраты этих цифр (с учетом положения в структурной схеме) из анализируемого числа, можно «вручную» определить приближенную величину квадратного корня из любого числа (с тем

большей точностью, чем ближе это число к ближайшему меньшему квадрату). Ошибка максимальна, когда структура числа имеет вид: $(a^2+2\cdot a)$, где a – ближайший меньший целочисленный корень испытуемого произвольного целого числа, и уменьшается с ростом a.

4) Данные по структуре квадрата с привлечением формулы квадрата двучлена дают возможность с минимумом проб «вручную» точно определить две головных цифры основания. Удаление квадратов старших цифр предположительного основания из обследуемого числа (с учетом разрядности) и последующее деление найденной разности на удвоенное значение старшей цифры основания дает завышенное (см. п. 4.2) приблизительное значение корня. Далее «двигаясь» в сторону понижения разрядности можно реализовать определение всей целочисленной части корня с минимумом проб при сравнении соответствующих цифр обследуемого числа и цифр, подбираемых при ориентировании на вычисленное указанным здесь способом приблизительное значение корня. Момент прекращение подбора цифр устанавливается заранее по номеру младшего разряда последней «индивидуальной» строки обследуемого числа (предположительно квадрата). При количестве разрядов в числе $(2\cdot n)$ (см. п. 3.3), номер младшего разряда последней «индивидуальной строки» равен $(n-1)$.

5. Заключение

В процессе исследования структуры корня получено следующее:

– Выявлена структура квадрата целого числа из формулы (1)).

– Уточнены действия по нахождению квадратных корней «вручную».

– Предложен путь приближенного определения квадратного корня из произвольного числа при отсутствии или минимальном использовании простейших средств выполнения вычислений.

– Сформулированы условия определения значения целочисленной части корня произвольного числа и указан путь такого определения, позволяющий реализовать алгоритм вычисления на ЭВМ.

– Конкретизированы задачи на продолжение исследований в плане облегчения, ускорения вычислений и повышения точности вычислений, в том числе и с числами произвольных размерностей (к сожалению, не раскрытые здесь из-за ограничений на объем статьи).

Литература

1. *Курош А.Г.* Курс высшей алгебры. М.: Гос. Изд-во физ.-мат. лит., 1963. 431 с.

2. *Афанасьева М.С., Колесов А.Н.* Научная сессия ТУСУР-2007: Материалы докл. Всерос. техн. конф. студентов, аспирантов и молодых ученых. Ч. 2. Томск: В-Спектр. С. 106–108.

3 *Афанасьева М.С., Колесов А.Н.* Студенческих сборник статей ТУСУР-2007. Первый ежегодный сборник статей по результатам научно-исследовательской деятельности студентов. Ч. 2. Томск: В-Спектр, 2007. С. 6–11.

ЗАЩИЩЕННЫЙ ПОЧТОВЫЙ КЛИЕНТ ОРГАНИЗАЦИОННАЯ ЧАСТЬ

В.В. Алехин, студент 5-го курса КИБЭВС
ТУСУР, г. Томск, avv@ms.tomsk.ru

Жизнь современного общества во многом зависит от надежности систем передачи информации. Особенно это касается тех систем, где обмен сообщениями электронным способом является частью общего документооборота (банк, государственные и военные учреждения) и где на первом месте стоит не доставка их в реальном времени, а конфиденциальность передаваемых сведений и гарантированность доставки, что обязательно при передаче сведений конфиденциального характера.

Так, например, электронная почта прочно вошла во все направления деятельности мира информационных технологий и для многих стала явлением обыденным и повседневным.

Анализ российского рынка систем защищенной электронной почты показывает, что он не так велик, как может показаться на первый взгляд. В основном такое положение складывается из-за ограниченного выбора СКЗИ, соответствующих требованиям российских стандартов и государственных органов надзора и контроля. В соответствии с требованиями контролирующих органов в отечественные системы защищенного электронного документооборота должны встраиваться только сертифицированные средства криптографической защиты информации, реализующие алгоритмы шифрования по ГОСТ 28147-89, ЭЦП – ГОСТ Р 34.10-94 (в настоящее время ГОСТ Р 34.10-01) и хэш-функции – ГОСТ Р 34.11-94. Это значит, что, например, системы электронной почты на основе стандарта PGP/MIME (OpenPGP) [1] для российского пользователя при использовании в обмене электронными документами с государственными структурами недоступны [2].

Как правило, системы защищенного электронного документооборота, основанные на принципах электронной почты, используемые на территории Российской Федерации, жестко привязаны к определенному типу криптопровайдера [4].

Отличительным свойством разрабатываемой системы является ее масштабируемость. Интерфейс системы строится таким образом, что при необходимости можно подключать различные криптопровайдеры (на начальном этапе планируется поддержка четырех сертифицированных: Крипто-Про CSP, Верба OW, Сигнал-Ком CSP и Домен-К) и транспортные протоколы (изначально планируется поддержка стандартных почтовых протоколов SMTP/POP3). Транспортный и криптографический модули оформляются в отдельные подключаемые динамические библиотеки, что и дает эффект мультиплатформенности системы. На российском рынке на данный момент не представлено ни одной разработки, обладающей подобными характеристиками.

При проектировании подобной системы необходимо четко представлять себе все составляющие системы защищенного электронного документооборота: юридическую сторону вопроса, криптографическую аспекты и транспортную подсистему. Нельзя спроектировать клиентскую часть без определенного фундамента. Фундаментом в данном случае является анализ российского рынка систем защищенного электронного документооборота, а также угроз безопасности субъектам системы. На основании произведенного анализа сформированы и выдвинуты требования, на основании которых и ведется разработка. Кроме того, следует учитывать, что существует законодательство, регламентирующее все разработки в данной области [3].

Система проектируется в соответствии с нормативными документами, для того чтобы не исключать в дальнейшем возможности ее последующей сертификации.

Литература

1. Стандарты RFC 2459, 3280.

2. Закон РФ от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

3. Закон РФ от 08.08.2001 №128-ФЗ «О лицензировании отдельных видов деятельности».

4. Мир связи. Connect! Информационный ресурс [В Интернете] http://www.connect.ru

ИСПОЛЬЗОВАНИЕ СЕТЕВЫХ СКАНЕРОВ

Р.Х. Айзатулин, студент ФВС 5-го курса

ТУСУР, г. Томск, Ayzatulin_rh@mail.ru

Nmap

Программа Nmap предназначена для сканирования сетей с любым количеством объектов, определения состояния объектов сканируемой

сети а также портов и соответствующих им служб. Программа реализована для многих операционных систем, в том числе и для Windows. Благодаря своей популярности она включена во многие дистрибутивы Linux.

Сканер позволяет сканировать TCP- и UDP-порты и использует различные способы сканирования – как обычные методы сканирования, так и незаметные. Отдельно можно выделить технологию сканирования IdleScan, при которой пакеты посылаются не сканирующей, а посторонней машиной, при этом сканирующая система абсолютно невидима.

По мере развития в программе добавились новые возможности: определение операционной системы по отпечатку TCP/IP, определение версий сервисов удаленного узла. Благодаря возможности любого пользователя пополнять базу знаний новыми данными, система распознает множество различных сетевых устройств.

XSpider

XSpider в автоматическом режиме проверяет компьютеры в сети на уязвимости. Основным достоинством сканера является большая и регулярно пополняемая база известных уязвимостей многих программных продуктов. Сканирование состоит из нескольких этапов: сканирование портов, идентификация сервисов, определение уязвимостей. Для обнаружения уязвимостей сканер перебирает множество различных комбинаций запросов. К плюсам сканера можно отнести его автоматизированность – возможность генерации отчетов, сканирование по расписанию. Однако при этом нельзя выбрать какой-то конкретный метод сканирования.

Необходимость сканирования

Рассмотренные сетевые сканеры предназначены для разных целей. Для эффективной работы со сканером Nmap предполагается знание протоколов и понимания методов сканирования.

Также при помощи дополнительных программ (например, Hping – сканер, позволяющий отправлять произвольные пакеты) можно более подробно просканировать исследуемую систему. После анализа системы при помощи Nmap, можно изменить политику безопасности, так как методики сканирования подробно расписаны на официальном сайте. Зная, что использование данной методики дало положительный результат, можно менять соответствующие настройки, как пример – параметры IP пакета TTL, DF которые имеют разные значения для различных операционных систем.

При использовании XSpider можно протестировать сетевые сервисы, как на программные ошибки, так и на ошибки политики безопасности (ограничение доступа, недостаточная длина пароля), также возможен анализ скриптов Web-сайтов, структуры HTTP-серверов.

В итоге использование сканеров в политике безопасности необходимо, однако сам по себе сканер не так эффективен, как при интеграции в систему безопасности, например интеграция с межсетевым экраном, для блокирования доступа к узлу при обнаружении уязвимости.

Как пример, компания, выпускающая сканер Xspider, заменяет его на более комплексное решение – Maxpatrol, в котором реализуется контроль соответствия политикам безопасности, поддержка основных стандартов безопасности, таких как ISO 17799, комплексный анализ сложных систем на базе различных платформ и сетевого оборудования.

Реагирование на попытки сканирования

Так как сканеры могут использоваться не только для анализа защищенности сети, но и как этап, предшествующий атаке, то администратор должен реагировать на попытки сканирования. Однако на все попытки сканирования реагировать невозможно, поэтому учитывается характер сканирования. Если сканирования носят постоянный характер и при этом нарушается работа сети, следует заблокировать доступ с этого адреса, или обратиться в техническую службу провайдера.

Литература

1. Документация по сканеру Nmap. http://insecure.org
2. Документация по сканеру XSpider. http://www.ptsecurity.ru
3. Статьи «Будущее сканеров безопасности», «Сканирование портов: за и против». http://www.securitylab.ru

СКАНИРОВАНИЕ СЕТИ НА УЯЗВИМОСТЬ

Э.Э. Бахарчиев, 5-го курс КИБЭВС
ТУСУР, г. Томск, e-mail: David_777@sibmail.com

Сканирование сети имеет своей целью выявление подключенных к сети компьютеров и определение работающих на них сетевых сервисов (открытых портов TCP или UDP). Первая задача выполняется посылкой ICMP-сообщений Echo с помощью программы ping с последовательным перебором адресов узлов в сети. Стоит попробовать отправить Echo-сообщение по широковещательному адресу – на него ответят все компьютеры, поддерживающие обработку таких сообщений.

Для незаконного подключения к сети злоумышленник, разумеется, должен иметь физическую возможность такого подключения. В крупных корпоративных и особенно университетских сетях такая возможность часто имеется. Следующим шагом для злоумышленника является конфигурирование параметров стека TCP/IP его компьютера.

Прослушивание сети (сегмента сети) даст злоумышленнику много полезной информации. В частности, он может определить, какие IP-адреса имеют узлы сети, и с помощью ICMP Echo-запросов (программа ping) определить, какие адреса не используются (или компьютеры выключены). После этого злоумышленник может присвоить себе неиспользуемый адрес.

Администратор сети может обнаружить попытки сканирования путем анализа трафика в сети и отслеживания Echo-сообщений, за короткий промежуток времени посылаемых последовательно по всем адресам сети. Для большей скрытности злоумышленник может существенно растянуть процесс во времени («медленное сканирование») – это же касается и сканирования портов TCP/UDP. Также злоумышленник может применить «обратное сканирование» (inverse mapping): в этом случае на тестируемые адреса посылаются не сообщения ICMP Echo, а другие сообщения, например RST-сегменты TCP, ответы на несуществующие DNS-запросы и т.п. Если тестируемый узел не существует (выключен), злоумышленник получит в ответ ICMP-сообщение Destination Unreachable: Host Unreachable.

Следовательно, если сообщение не было получено, то соответствующий узел подключен к сети и работает.

Программа traceroute поможет в определении топологии сети и обнаружении маршрутизаторов.

Для определения того, какие UDP- или TCP-приложения запущены на обнаруженных компьютерах, используются программы-сканеры, например программа nmap. Поскольку номера портов всех основных сервисов Интернета стандартизованы, то, определив, например, что порт 25/TCP открыт, можно сделать вывод о том, что данный хост является сервером электронной почты, и т. д. Полученную информацию злоумышленник может использовать для развертывания атаки на уровне приложения.

Сканирование TCP-портов хоста производится несколькими способами. Наиболее простой способ – установление TCP-соединения с тестируемым портом с помощью функции *connect*. Если соединение удалось установить, значит, порт открыт и к нему подсоединено серверное приложение. Достоинством этого способа является возможность выполнения сканирования любым пользователем, и даже без специального программного обеспечения: стандартная программа telnet позволяет указать произвольный номер порта для установления соединения. Существенный недостаток – возможность отслеживания и регистрации такого сканирования: при анализе системного журнала сканируемого хоста будут обнаружены многочисленные открытые и сразу же прерванные соединения, в результате чего могут быть приняты меры по повышению уровня безопасности.

Сканирование в режиме половинного открытия (half-open scanning) не имеет описанного недостатка, но требует от злоумышленника возможности формировать одиночные TCP-сегменты в обход стандартного модуля TCP (или, при использовании уже написанных программ, как минимум – прав суперпользователя). В этом режиме злоумышленник направляет на сканируемый порт SYN-сегмент и ожидает ответа. Получение ответного сегмента с битами SYN и ACK означает, что порт открыт; получение сегмента с битом RST означает, что порт закрыт. Получив SYN+ACK, злоумышленник немедленно отправляет на обнаруженный порт сегмент с битом RST, таким образом ликвидируя попытку соединения. Поскольку соединение так и не было открыто (ACK от злоумышленника не был получен), то зарегистрировать такое сканирование гораздо сложнее.

Третий способ – сканирование с помощью FIN-сегментов. В этом случае на сканируемый порт посылается сегмент с установленным битом FIN. Хост должен ответить RST-сегментом, если FIN-сегмент адресован закрытому порту. FIN-сегменты, направленные на порт, находящийся в состоянии LISTEN, многими реализациями TCP/IP игнорируются (стандарт требует в состоянии LISTEN посылать RST-сегменты в ответ на сегменты, имеющие неприемлемый ACK SN; про сегменты, имеющие только флаг FIN, ничего не говорится). Таким образом, отсутствие отклика говорит о том, что порт открыт. Варианты этого способа сканирования – посылка сегментов с флагами FIN, PSH, URG («Xmas scan») или вообще без всяких флагов («Null scan»).

Конечно, сканирование SYN-сегментами дает более надежные результаты, однако, к счастью, многие брандмауэры могут не пропускать SYN-сегменты без флага ACK из Интернета во внутреннюю сеть (так, запрещаются соединения хостов Интернета с внутренними хостами, инициируемые из Интернета, но разрешаются соединения, инициируемые изнутри).

Программа tcplogd может зарегистрировать попытки сканирования в различных режимах.

Для определения открытых портов UDP злоумышленник может отправить на тестируемый порт UDP-сообщение. Получение в ответ ICMP-сообщения Port Unreachable (тип 3, код 3) говорит о том, что порт закрыт.

Программа-сканер может также определить операционную систему сканируемого узла по тому, как узел реагирует на специальным образом сконструированные, нестандартные пакеты: например, TCP-сегменты с бессмысленными сочетаниями флагов или ICMP-сообщения некоторых типов, и по другим признакам.

В марте 2001 г. в списке рассылки Bugtraq шла оживленная дискуссия об опции TCP Timestamp (Временной штамп) [McDanel]. У многих

систем часы модуля TCP, чьи показания помещаются в опцию Timestamp, связаны с системными часами, что позволяет по значению опции определить uptime – время, прошедшее с момента загрузки компьютера. Эта информация может представлять потенциальную угрозу для безопасности компьютера в следующих аспектах.

Некоторые реализации могут использовать uptime для инициализации генератора псевдослучайных чисел, который используется различными приложениями для создания серийных номеров, имен временных файлов и т.п., а также для назначения номеров ISN для TCP-соединений. Зная uptime и имея аналогичный генератор, злоумышленник может предсказать результаты его работы.

Зная тип системы и время последней перезагрузки, можно сделать вывод, что заплаты (patches), касающиеся безопасности и вышедшие позже момента загрузки, в системе не установлены (если их установка требует перезагрузки).

Наблюдая за системой продолжительное время, можно составить график ее регулярных перезагрузок и произвести имперсонацию хоста в тот момент, когда он перегружается и не способен работать с сетью.

Однако возможность выполнения реальных атак с использованием значения uptime пока остается под вопросом.

Для определения адресов работающих в сети компьютеров и запущенных на них UDP- или TCP-сервисов злоумышленник, непосредственно подключенный к сегменту сети, может использовать простое прослушивание. Такая форма сканирования сети является более скрытой, чем рассылка тестирующих датаграмм.

Приведем пример описания сканирования одного компьютера, находящегося в корпоративной сети, и отметим его уязвимости и способ решения.

В заключение следует отметить, что администратор сети должен знать и использовать методы и инструменты злоумышленника и проводить превентивное сканирование сети организации для обнаружения слабых мест в безопасности до того, как это сделает злоумышленник. Для этой цели имеется также специальное программное обеспечение – сканеры безопасности, network security scanners, типа Nessus.

Литература

1. Б*еловин С.М.* Проблема безопасности в TCP/IP Protocol Suite. С. 32–48. 1989.

2. http://www.void.ru/

3. http://www.hackzone.ru/

4. http://www.security.nnov.ru/

5. http://www.xakep.ru/

ВЫБОР АЛГОРИТМА ШИФРОВАНИЯ ДЛЯ ТРАНСПОРТНОЙ СИСТЕМЫ ЗАЩИЩЕННОГО ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

В.Б. Бажинов, С.В. Голубев, А.Л. Навойников, А.В. Хоменко,
студенты 4-го курса ФВС
ТУСУР, г. Томск, кафедра КИБЭВС AlexRemote@sibmail.com

Целью создания транспортной системы защищенного обмена электронными документами является передача электронных документов, обеспечение целостности, сохранности и конфиденциальности документов в процессе их транспортировки и хранения. Испытанный метод защиты информации – шифрование. На данный момент существует множество криптографических алгоритмов.

С учетом некоторой специфичности задачи (требованиям к скорости зашифрования/расшифрования) будем рассматривать только симметричные криптографические алгоритмы (табл. 1):

DES (Data Encryption Standard). Федеральный стандарт шифрования США.

Blowfish.

IDEA (International Decryption-Encryption Algorithm).

ГОСТ 28147-89. Стандарт Российской Федерации на шифрование и имитозащиту данных.

Таблица 1

Сравнительные скоростные характеристики алгоритмов блочного шифрования, используя рекомендуемый авторами алгоритма минимальный остаточный размер ключа (размер блока 64 бит), на Intel Pentium x86

Алгоритм шифрования	Число циклов на раунд	Число раундов	Число циклов на зашифрованный байт (скорость шифрования)	Размер ключа
IDEA	50	8	50	128
Blowfish	9	16	18	448
ГОСТ 28147-89	32	32	256	256

Криптостойкость рассмотренных алгоритмов

Блок подстановок в DES допускает аппроксимацию аффинными преобразованиями. Многие булевы функции, используемые в подстановках, отличаются от аффинных функций лишь для двух из шестнадцати возможных наборов аргументов, т.е. нелинейность подстановки DES

равна двум. Кроме того, DES облагает свойством дополнения. При подборе ключа это позволяет нарушителю вдвое сократить объем перебора, т.е. ключ можно искать с точностью до инверсии.

Алгоритм IDEA благодаря использованию операции умножения по модулю $2^{16}+1$, обладающей сильным перемешивающим эффектом, представляется достаточно стойким по отношению к линейному криптоанализу. Стойкость этого алгоритма по отношению к дифференциальному методу криптоанализа не очевидна. IDEA ориентирован на программную или аппаратную реализацию с использованием встроенного аппаратного умножителя. Однако даже в этом случае умножение по модулю $2^{16}+1$ выполняется программно заметно медленнее, чем сложение, что обусловлено необходимостью выполнения дополнительных операций, кроме собственно умножения 16-битных чисел. Количество машинных тактов для шифрования IDEA в программной реализации при отсутствии специальных мер зависит от вида ключа и шифруемого текста. Поэтому точное измерение длительности шифрования каждого блока позволяет извлечь дополнительную информацию о ключе. Очевидно, это обстоятельство может заметно снизить стойкость IDEA. Кроме того, для этого алгоритма существует класс слабых ключей.

Исследования Blowfish показали, что для этого алгоритма существуют слабые ключи (S-блоки, в которых есть одинаковые слова). При использовании таких ключей дифференциальный криптоанализ позволяет восстановить массив подключей для 8 циклов с помощью 2^{23} выбранных открытых текстов, а для 16 циклов – с помощью $3*2^{51}$ выбранных открытых текстов. Если слабые ключи не используются, то для 8 циклов восстановить массив подключей можно с помощью 2^{48} выбранных открытых текстов. В 1998 г. алгоритм Blowfish представлен в качестве кандидата на стандарт шифрования США.

В алгоритме шифрования ГОСТ 28147-89 блок подстановки не фиксирован и является секретным параметром. Ключ – 256 бит, что делает невозможной атаку перебором. Для повышения стойкости к дифференциальному и линейному методам криптоанализа желательно выбирать экстремальные подстановки с нелинейностью 4 и рассеиванием 1. Кроме того, наиболее вероятная разность двух выходов подстановки при фиксированной разности входов должна иметь малую вероятность (разности определяются суммой по модулю 2). Однако нахождение таких подстановок сопряжено со значительными трудностями. Число циклов в ГОСТ 28147-89 по сравнению с DES увеличено вдвое. Криптоанализ усеченного 24-циклового ГОСТ 28147-89 без последних восьми циклов показал, что стойкость его превышает 2^{54} для случайного блока подстановки.

Международные юридические аспекты использования алгоритмов шифрования.

Следует отметить, что современное Российское патентное законодательство никаким образом не поддерживает права на *алгоритм*, соответственно не выдаются патенты на алгоритмы шифрования. Таким образом, на территории Российской Федерации допустимо использование любых рассмотренных алгоритмов шифрования, а вот в случае продвижения программы на международный рынок, использование некоторых алгоритмов либо полностью запрещено, либо требует обязательного лицензирования у патентообладателя (табл. 2).

Таблица 2

Юридические аспекты использования алгоритмов шифрования

Алгоритм шифрования	Ограничения
IDEA	Запатентован Ascom-Tech, при коммерческом использовании требует обязательного лицензирования
Blowfish	Не запатентован, свободно распространяемый
ГОСТ 28147-89	Не запатентован, при использовании в России требуется сертификат ФАПСИ

Обобщая существенные при разработке транспортной системы свойства алгоритмов шифрования (скорость шифрации и криптостойкость), наиболее предпочтительным для использования является ГОСТ 28147-89 (при условии наличия полной документации по стандарту, в том числе и специальных криптографических подстановок, от которых существенно зависит криптостойкость алгоритма).

Литература

1. *Новосельский А.* Алгоритмы шифрования http://www.codenet.ru/progr/alg/enc/

2. Counterpane Labs. «The Blowfish encryption algorithm» http://www.counterpane.com/

3. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии: Учеб. пособие, 2-е изд., испр. и доп. М.: Гелиос АРВ, 2002. 480 с.

КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К.С. Беляк, студент 5-го курса каф. КСУП

ФВС, ТУСУР, г. Томск, Kseniyabelyak@mail.ru

Информационные технологии значительно расширили возможности бизнеса, однако новые возможности всегда сопряжены с новыми риска-

ми. Чем сложнее информационная система, тем выше риск осуществления по отношению к ней различных угроз: например, проникновения в систему извне или несанкционированный доступ изнутри предприятия с целью финансового мошенничества или хищения коммерческой информации.

Анализ рисков – это то, с чего должно начинаться построение любой системы информационной безопасности, а также устранение ее возможных недостатков. Он включает в себя мероприятия по обследованию безопасности предприятия. Результатом анализа информационных рисков является определение того, какие ресурсы и от каких угроз надо защищать, а также в какой степени ресурсы нуждаются в защите. Определение набора адекватных контрмер осуществляется в ходе управления рисками.

При разработке алгоритма оценки информационных рисков, основанного на анализе угроз и уязвимостей информационной системы, были рассмотрены и проанализированы различные существующие классификации угроз информационной безопасности. При попытке использования данных классификаций для описания по возможности большего количества угроз показали, что во многих случаях реальные угрозы либо не подходили ни под один из классификационных признаков, либо, наоборот, удовлетворяли нескольким.

По характеру угрозы информационной безопасности можно разделить на технологические и организационные. Соответственно, получен верхний уровень классификации:

1. Угрозы технологического характера.

2. Угрозы организационного характера.

Технологические угрозы информационной безопасности делятся на:

1.1. Физические.

1.2. Программные (логические).

Следующая ступень классификации – источник угрозы. Источниками физических угроз могут быть:

1.1.1. Действия нарушителя (человека).

1.1.2. Форс-мажорные обстоятельства.

1.1.3. Отказ оборудования и внутренних систем жизнеобеспечения.

Независимо от источника физические угрозы воздействуют:

1.1.1.1. На ресурс.

1.1.1.2. На канал связи.

Источниками программных угроз могут быть:

1.2.1. Локальный нарушитель.

1.2.2. Удаленный нарушитель.

Объектом локального нарушителя может быть только ресурс.

При этом на ресурсе локальный нарушитель может реализовать угрозы, направленные:

1.2.1.1.1. На операционную систему.

1.2.1.1.2. На прикладное программное обеспечение.

1.2.1.1.3. На информацию.

Угрозы, исходящие от удаленного нарушителя, могут воздействовать:

1.2.2.1. На ресурс.

1.2.2.2. На канал связи.

При доступе к ресурсу удаленный нарушитель может воздействовать:

1.2.2.1.1. На операционную систему.

1.2.2.1.2. На сетевые службы.

1.2.2.1.3. На информацию.

При воздействии на канал связи удаленный нарушитель может реализовать угрозы, направленные:

1.2.2.2.1. На сетевое оборудование.

1.2.2.2.2. На протоколы связи.

Организационные угрозы по источнику воздействия подразделяются на:

2.1. Воздействие на персонал.

2.2. Действия персонала.

Воздействие на персонал может быть:

2.1.1. Физическим.

2.1.2. Психологическим.

Как физическое, так и психологическое воздействие на персонал направлено на сотрудников компании с целью:

2.1.1.1. Получения информации.

2.1.1.2. Нарушения непрерывности ведения бизнеса.

Причинами действий персонала, способных вызвать угрозы информационной безопасности, могут быть:

2.2.1. Умышленные действия.

2.2.2. Неумышленные действия.

Угрозы, вызванные умышленными действиями персонала, могут быть направлены:

2.2.1.1. На информацию.

2.2.1.2. На непрерывность ведения бизнеса.

Угрозы, вызванные неумышленными действиями персонала, могут быть направлены:

2.2.2.1. На информацию.

2.2.2.2. На непрерывность ведения бизнеса.

В результате классификация угроз информационной безопасности разделяется по характеру угрозы, виду воздействия, источнику и объекту угрозы.

Таким образом, основная цель создания классификации угроз – наиболее полная, детальная классификация, которая описывает все существующие угрозы информационной безопасности, по которой каждая из угроз попадает только под один классификационный признак, и которая, таким образом, наиболее применима для анализа рисков реальных информационных систем.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СБЕРБАНКЕ РФ

А.Ю. Бердников, студент 5-го курса кафедры КИБЭВС
ТУСУР, г. Томск, AlexMracdu@yandex.ru

В наше время нельзя представить работу банка без средства вычислительной техники, так как объемы обрабатываемой и хранимой информации давно переросли рамки восприятия человеческого разума.

Развитие информационных технологий в управлении бизнес-процессами привело управленцев «Сбербанка РФ» к осознанию, необходимости создания эффективной технологии обслуживания клиентов и постоянной работе над развитием и внедрением таких технологий. Одним из направлений таких технологий является Дистанционное банковское обслуживание корпоративных клиентов и индивидуальных предпринимателей с использованием защищенного электронного документооборота.

Применение электронного документооборота в отношениях с Банком позволяет:

a) обеспечить высокую скорость проведения расчетов;

b) иметь оперативную информацию о состоянии банковских счетов;

c) минимизировать банковские комиссии, возникающие при обслуживании банковских счетов;

d) организовать взаимодействие между головной и дочерними компаниями по координации платежных потоков;

e) заключать сделки по привлечению и размещению денежных средств;

f) направлять списки на пополнение счетов сотрудников организации;

g) вести официальную переписку с банком по любым вопросам;

Система Банк-Клиент

Электронный документооборот между Банком и Клиентом может быть организован независимо от местонахождения Клиента, используя

вседоступную телефонную линию связи и технологию VPN (виртуальная частная сеть).

«Сбербанк РФ» стремится к созданию полноценной и безопасной системы дистанционного банковского обслуживания, охватывающей все аспекты взаимоотношений Клиента и Банка при предоставлении банковских услуг.

Для реализации безопасного электронного документооборота Банк использует программные продукты, выполненные на базе сертифицированного средства криптографической защиты информации (Данные о производителе и ПО имеют гриф «Коммерческая тайна» и не подлежат разглашению).

«Сбербанк РФ» имеет все необходимые права на распространение средств криптографической защиты информации, используемых в рамках системы электронного документооборота.

Система электронного документооборота реализована в версии: Система «Банк-Клиент».

Функциональные возможности

Неограниченный список возможных типов документов

Система электронного документооборота позволяет формировать и направлять в Банк следующие типы документов:

– Платежное поручение в рублях.

– Заявление об отзыве ранее направленного в Банк расчетного документа.

– Запрос на получение платежного поручения с факсимильным штампом Банка.

– Заявление на перевод иностранной валюты.

– Поручение на покупку иностранной валюты.

– Поручение на продажу иностранной валюты.

– Поручение на списание средств с транзитного валютного счета.

– Заявление об акцепте/отказе от акцепта платежного требования.

– Заявка на предоставление кредита в рамках открытой кредитной линии.

– Списки для пополнения карт счетов.

– Сообщения/письма свободного формата с возможностью вложения файлов.

– Список формализованных типов документов, возможных для электронного обмена, пополняется по мере развития банковских услуг и/или возникновения новых потребностей и ничем не ограничивается.

Уведомление о поступлении претензий к счету

При поступлении к банковскому счету Клиента претензий в виде решений о приостановлении операций по счетам налогоплательщика,

платежных требований, инкассовых поручений по системе электронного документооборота направляется соответствующее уведомление. Это позволяет Клиентам оперативно предпринять действия по урегулированию данной претензии и лучше спланировать свои финансовые потоки.

Шаблоны документов

С целью облегчения создания новых документов по часто повторяющимся платежам имеется возможность создания неограниченного количества Шаблонов.

Создаваемым шаблонам можно присваивать наименования исходя из сущности операции, что впоследствии облегчит выбор нужного шаблона.

Предоставление выписок по банковскому счету

Выписка по счету Клиента может быть запрошена из Банка. Для этого создается документ «Запрос на выписку» и отправляется в Банк.

Также выписка может быть сформирована непосредственно на рабочем месте Клиента на основании документов операций, полученных из Банка ранее.

Выписка может быть подготовлена за период времени или за один день по выбору Клиента (в том числе по текущему операционному дню).

Предоставление документов операций, проведенных по банковскому счету

Все операции, проведенные Банком по счету Клиента и полученные Клиентом при очередном сеансе обмена, консолидируются в специальном представлении.

В любой момент по своему желанию Клиент может получить по ним соответствующие распечатки с отметкой Банка о дате проведения операции по счету.

В случае отмены Банком какой-либо операции она выделяется специальным шрифтом.

Минимизация рисков ошибок

В программе предусмотрен контроль вводимых реквизитов документов на предмет соблюдения формата вводимых значений и соответствия справочникам системы. В случае наличия ошибок или отклонения от правил выдается протокол ошибок и производится цветовая подсветка проблемных полей документа.

Процедура подготовки документов к отправке в Банк организована таким образом, чтобы максимально снять риски ошибок. Перед отправкой документов в Банк у Клиента всегда имеется возможность убедиться в корректности отправляемого пакета, проверив его по сумме и количеству документов.

Контроль исполнения документов

Документы, направленные Клиентом в Банк, по мере прохождения по технологической цепочке принимают различные состояния, которые передаются Клиенту во время очередного сеанса обмена с Банком. Контроль состояний документов позволяет оперативно выявить ситуации возврата документов без исполнения.

В случае невозможности исполнения какого-либо распоряжения Клиента Банком направляется уведомление об этом с указанием причин.

Гибкое распределение Сбербанка РФ прав пользователей Клиента

В зависимости от потребностей Клиента, сотрудникам организации, работающим в системе электронного документооборота, может быть предоставлен индивидуальный набор прав. Например, только на просмотр выписок и операций по банковскому счету Клиента, или на просмотр/создание документов только определенного типа.

Это позволяет организациям повысить степень защиты электронного документооборота от несанкционированных действий пользователей.

Литература

1. Инструкция по системе «Банк-Клиент» Сбербанка РФ.

2. Положения о работе с документацией составляющей коммерческую тайну Сбербанка РФ.

3. *Демин В.С.* Автоматизированные банковские системы. М.: Менатеп-Информ, 1997 г.

ХЭШ-ФУНКЦИЯ НА БАЗЕ КЛЕТОЧНЫХ АВТОМАТОВ

С.И. Боровков, студент 5-го курса КИБЭВС

ТУСУР, г. Томск, AstroN-28@sibmail.com

Цель работы – разработка и реализация хэш-функции на базе клеточных автоматов.

Хэш-функции – это функции, предназначенные для «сжатия» произвольного сообщения или набора данных в некоторую битовую комбинацию фиксированной длины, называемую сверткой. Хэш-функции имеют разнообразные применения при проведении статистических экспериментов, при тестировании логических устройств, при построении алгоритмов быстрого поиска и проверки целостности записей в базах данных. В криптографии хэш-функции применяются для решения следующих задач:

− построение систем контроля целостности данных при их передаче или хранении;

− аутентификация источника данных.

Для достижения различных целей применяются соответствующие хэш-функции.

С широким распространением автоматизированных систем и ужесточением требований безопасности возникла потребность в надежных хэш-функциях, применяемых для осуществления аутентификации пользователей в информационной системе. Для достижения этих целей были разработаны бесключевые функции хэширования.

Обычно требуется, чтобы бесключевые хэш-функции обладали следующими свойствами:

1. однонаправленность;
2. устойчивость к коллизиям;
3. устойчивость к нахождению второго прообраза, –

означающими соответственно высокую сложность нахождения сообщения с заданным значением свертки; пары сообщений с одинаковыми значениями свертки; второго сообщения с тем же значением свертки для заданного сообщения с известным значением свертки.

Суть применения состоит в следующем. Пользователь информационной системы, проходя процедуру авторизации, вводит пароль произвольной длины (в установленном диапазоне). Из него вычисляется хэш-значение, представляющее собой последовательность символов фиксированной длины. Благодаря свойству однонаправленности из хэш-значения невозможно получить исходную последовательность символов, т.е. пароль пользователя. При следующей авторизации введенный пароль снова хэшируется и полученное значение сравнивается с сохраненным хэш-значением. Таким образом, происходит аутентификация пользователей в системе.

Но уязвимость хэш-функций состоит в существовании коллизий, т.е. в возможности найти другую исходную последовательность, хэш-значение которой будет совпадать с хэш-значением заданной последовательности. Поэтому существует потребность в разработке новых, более надежных хэш-функций.

Благодаря уникальным свойствам клеточных автоматов на их основе можно разработать не только стойкий криптографический алгоритм, но и принципиально иную надежную хэш-функцию.

Клеточные автоматы являются дискретными динамическими системами, поведение которых полностью определяется в терминах локальных зависимостей. Пространство представлено равномерной сеткой, каждая ячейка которой, или клетка, содержит несколько битов данных;

время дискретно, а законы мира выражаются единственным набором правил, например, небольшой справочной таблицей, по которой любая клетка на каждом шаге вычисляет свое новое состояние по состояниям ее близких соседей.

Благодаря опыту, полученному при разработке криптосистемы клеточных автоматов, была создана хэш-функция, основные моменты которой описаны ниже.

В исходной последовательности (пароле) символы заменяются на соответствующие им ASCII-коды, которые затем переписываются в двоичном виде и побитно заносятся в трехмерный массив определенных размеров. Затем из заполненного трехмерного массива в определенном порядке берутся биты для формирования ключа преобразования. Если массив заполнился не весь, оставшиеся ячейки заполняются значениями уже заполненных ячеек, но берутся они в ином порядке, нежели в порядке заполнения данного трехмерного массива. Благодаря трехмерности поля, биты могут браться из кодов разных символов исходной последовательности, что практически равноценно заполнению оставшихся ячеек случайными битами. Но все эти биты, которыми заполнили оставшиеся ячейки, формируют коды некоторых символов. Следовательно, существует строка, полностью заполняющая массив, который будет иметь идентичное содержание. Возникает возможность коллизии. Чтобы исключить такую возможность, к сформированной ключевой последовательности добавляются биты самой исходной последовательности. В результате чего ключи будут отличаться, что устранит возможность коллизии в данном случае.

Если исходная последовательность не поместилась в трехмерный массив, то происходит аналогичное заполнение дополнительного трехмерного массива тех же размеров. Если после этого остались не вошедшие в массивы биты, они заносятся в ячейки первого массива, которые «обволакивают» данный трехмерный массив, тем самым создавая соседние ячейки для ячеек, находящихся на границах массива.

Каждые 6 бит сформированного ключа будут являться одним правилом преобразования, так как у каждой ячейки массива есть 6 общих сторон с другими ячейками (6 соседей). Перебирая правила, на каждом шаге будет вычисляться новое значение для каждой ячейки трехмерного массива в зависимости от ее пространственных соседей, а также в зависимости от ее значения в массиве прошлого состояния, роль которого исполняет упомянутый выше дополнительный массив, и характер этой зависимости будет определять текущие 6 бит ключа. Наличие массива прошлого состояния, значения которого учитываются при вычислении новых значений ячеек основного массива, а также вычисление ключа из

исходной последовательности обеспечивают надежное выполнение требования однонаправленности.

Изменяемая зависимость каждого бита исходного текста от своих пространственных соседей в совокупности с трехмерностью массива, наличием массива предыдущих состояний и уникальным алгоритмом дополнения введенной последовательности без использования констант обеспечивают практическую невозможность выявления каких-либо зависимостей между исходной последовательностью (паролем) и его хэш-значением.

Изменение хотя бы одного бита в исходной последовательности приводит к непредсказуемым, кардинальным изменениям в результирующем хэш-значении.

Литература

1. *Тоффоли Т., Марголус Н.* Машины клеточных автоматов. М.: Мир, 1991. 280 с.

2. *Алферов А.П., Зубов А.Ю., Кузьмин А.В., Черемушкин А В.* Основы криптографии: Учеб. пособие. 3-е изд., испр. и доп. М.: Гелиос АРВ, 2005. 480 с.

3. *Шнайер Б.* Прикладная криптография. 2-е изд.. Протоколы, алгоритмы и исходные тексты на языке С. М.: Триумф, 2002. 610 с.

КРИПТОСИСТЕМА КЛЕТОЧНЫХ АВТОМАТОВ С ОКРЕСТНОСТЬЮ МУРА

С.И. Боровков, студент 5-го курса КИБЭВС

ТУСУР, г. Томск, AstroN-28@sibmail.com

В связи с бурным развитием информационных технологий и растущими темпами автоматизации процессов управления данными все больше времени и средств уделяется вопросам безопасности информации. Одним из важнейших способов защиты информации является ее шифрование с помощью стойких и надежных криптографических алгоритмов. Криптоанализ не стоит на месте, если разработанный алгоритм считается стойким, то это не значит, что никогда не будут найдены методы его взлома. Естественно, необходимо учитывать и быстрые темпы роста вычислительных мощностей современных компьютеров. Даже в самых стойких криптографических алгоритмах со временем могут найти уязвимость. Особенно учитывая то, что современные шифры, которые считаются самыми стойкими на сегодняшний день, относятся к классу предположительно стойких алгоритмов. Поэтому всегда существует необходимость в разработке новых, более стойких алгоритмов шифрования.

Идея построения шифров на базе клеточных автоматов уже не нова, но весьма перспективна. В результате анализа современных требований к криптосистемам и свойств клеточных автоматов была разработана криптосистема клеточных автоматов с окрестностью Мура. Для проверки работоспособности и исследования стойкости алгоритма написана его программная реализация «CellCrypt». В рамках этой работы разработано и реализовано несколько модификаций алгоритма, обладающих различными характеристиками и свойствами. Структура алгоритма имеет кардинальные отличия от разработанных раннее. Обладание свойствами клеточных автоматов наделяет его многими преимуществами в плане криптостойкости.

Разработанный алгоритм удовлетворяет всем требованиям к современным криптосистемам. Возможность использования ключа длиной 256 бит и более обеспечивает достаточную стойкость от атак методом последовательного перебора. Длина ключа не фиксирована, что также является преимуществом. Кроме того, размеры исходного поля клеточного автомата также являются не фиксированными и могут быть использованы в качестве дополнительных ключевых данных.

Алгоритм является блочным, как и большинство современных используемых алгоритмов. Но здесь могут применяться блоки очень больших размеров, что затруднит криптоанализ. Использование блоков больших размеров порождает уязвимость, заключающуюся в необходимости добавления дополнительных символов в последний, не до конца заполненный блок. Но уникальные возможности клеточных автоматов позволили доработать алгоритм таким образом, что необходимость добавления дополнительных символов была устранена. Данное обстоятельство означает, что стойкость последнего шифруемого блока к криптоанализу не снижается по сравнению с остальными блоками, но даже в значительной степени повышается.

Одной из самых значительных особенностей разработанной криптосистемы является изменяемая зависимость каждого бита сообщения от соседних бит. Изменение хотя бы одного бита в сообщении приведет к непредсказуемому изменению всего шифротекста. На каждом раунде шифрования состояние каждой клетки зависит от состояний ее нескольких соседей, но заранее не известно, каких именно. Это определяется ключом. Такие зависимости очень сложно проследить, так как после преобразования очередной ячейки следующая ячейка будет учитывать только что измененное состояние своего соседа. А на каждом раунде правило, определяющее зависимость клеток друг от друга, меняется. Данный алгоритм делает невозможным дешифрование части блока, его можно расшифровать только полностью.

Очень важным свойством представленной криптосистемы является косвенное участие ключа в преобразовании сообщения. Это означает, что ключ никаким образом не взаимодействует с шифруемым сообщением. Он не участвует ни в каких операциях преобразования с битами сообщения. Подобное свойство является уникальным для криптографического алгоритма. Именно благодаря взаимодействию ключа и шифруемого сообщения в других шифрах существует один из самых успешных методов криптоанализа – линейный криптоанализ. В описываемом криптографическом алгоритме ключ не участвует в операциях преобразования с битами шифруемого сообщения, а только определяет характер зависимости битов друг от друга, вследствие чего линейный криптоанализ к данному шифру просто не применим.

В алгоритме не используются фиксированные блоки для подстановок. Такие блоки применяются при проведении дифференциального анализа. Для осуществления взлома данной криптосистемы, возможно, понадобится разработка иных методов криптоанализа.

При практическом тестировании было выявлено, что данные, зашифрованные криптосистемой «CellCrypt», не содержат избыточной информации, которая может быть использована при криптоанализе. Кроме того, они успешно прошли тесты на равномерное распределение.

Криптосистема не уступает в скорости шифрования данных другим наиболее стойким на сегодняшний день криптографическим алгоритмам. Однако это относится к режиму побайтного шифрования. В режиме побитного шифрования (в системе «CellCrypt» реализованы оба режима) наблюдается заметное отставание в скорости. Но дальнейшая оптимизация программы, возможно, позволит исправить данный недостаток.

Разработка криптографических алгоритмов на базе клеточных автоматов может стать новым направлением в развитии криптографии.

Литература

1. *Тоффоли Т., Марголус Н.* Машины клеточных автоматов. М.: Мир, 1991. 280 с.

ПРОЦЕССНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

В.В. Деркач, студент 5-го курса каф. КИБЭВС
ТУСУР, г. Томск, G-Man@sibmail.com

При построении системы управления информационной безопасности (СУИБ) мы используем стандарты и на их основе строим процессную модель СУИБ компании-заказчика, содержащую три уровня процессов.

– Процессы стратегического уровня – управление рисками, управление непрерывностью ведения бизнеса, разработка и развитие политики ИБ верхнего уровня.

– Тактические процессы – разработка и развитие процедур ИБ, технической архитектуры системы ИБ, классификация ИТ-ресурсов, мониторинг и управление инцидентами и другие.

– Процессы операционного уровня – управление доступом, управление сетевой безопасностью, проверка соответствия и др.

Определяются взаимосвязи процессов. В результате мы получаем трехуровневую процессно-сервисную модель системы управления ИБ, соответствующую требованиям стандарта ISO 27001, на которую накладывается ролевая модель.

Управление информационной безопасности (ИБ) заключается в четком выполнении всех процедур по управлению ИБ и по обеспечению ИБ, координация и регулирование процедур, контроль их правильного, а также эффективного выполнения.

Стандарт декларирует два основных принципа управления:

1. Процессный подход к управлению безопасностью. Процессный подход рассматривает управление как процесс – набор взаимосвязанных непрерывных действий. Процессный подход акцентирует внимание на достижении поставленных целей, а также на ресурсах, затраченных для достижения целей.

2. Применение PDCA-модели как основа для всех процедур управления ИБ. PDCA-модель (или модель Шухарта-Деминга) определяет четыре этапа, которые последовательно должны выполняться для каждого процесса.

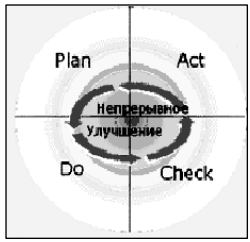


Рис. 1. PDCA-модель: Plan – планируй;
Do – выполняй; Check – проверяй; Acr – действуй

Название этапа	Описание этапа
Планируй (создание СУИБ)	Определение Политики управления ИБ, целей, процессов и процедур, мер и способов обеспечения ИБ.
Выполняй (внедрение и функционирование СУИБ)	Внедрение и функционирование Политики управления ИБ, требований, процессов и процедур.
Проверяй (мониторинг и проверка СУИБ)	Оценка и (при необходимости) анализ функционирования процессов в соответствии с требованиями документов системы управления ИБ, а также предоставление отчетов о результатах проведения проверок руководству компании.
Действуй (поддержание и улучшение СУИБ)	Выполнение корректирующих и превентивных действий.

Рис. 2. Описание этапов PDCA-модели

В системе управления рисками ИБ на этапе «**Планированируй»** определяются политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков.

На этапе «**Выполняй»** производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации. Руководством организации принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, либо минимизировать. После этого разрабатывается и внедряется план обработки рисков.

На этапе «**Проверяй»** отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

На этапе **«Действуй»** по результатам непрерывного мониторинга и проводимых проверок выполняются необходимые корректирующие действия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

Внедрение системы управления ИБ, как правило, заключается в информировании соответствующих сотрудников о правилах и сроках выполнения процедуры, регулярный контроль выполнения процедуры, а также оценка ее эффективности, внесение корректирующих и превентивных действий. То есть, по сути, внедрение всего цикла PDCA-модели для каждой процедуры.

Как правило, консультанты по разработке и внедрению системы управления ИБ разрабатывают «План внедрения системы управления», в котором описывают четкую последовательность действий при внедрении процедур, методы контроля и осуществления проверок выполнения процедуры.

Систему управления ИБ можно считать внедренной и эффективно функционирующей на практике тогда, когда все ее процедуры хотя бы один раз пройдут этапы модели PDCA, когда будут найдены и решены проблемы, возникающие при внедрении процедур.

ИБ – достаточно трудоемкий процесс. Однако если к задаче обеспечения безопасности подойти комплексно и своевременно, а также выполнять все рекомендации международных стандартов в области управления ИБ – ISO/IEC 27001:2005 и ISO/IEC 17799:2005, то процесс обеспечения ИБ, а также управления безопасностью станет прозрачным, а защита от угроз безопасности эффективной.

Литература

1. *Куканова Н.* Современные методы и средства анализа и управления рисками информационных систем компаний //www.dsec.ru

2. *Астахов А.* Как построить и сертифицировать систему управления информационной безопасностью? // shop.globaltrust.ru

3. *Астахов А.* BS 7799 – прародитель международных стандартов. // www.cnews.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКЕ

С.Ю. Дьяченко, студент 5-го курса кафедры КИБЭВС

ТУСУР, г. Томск, cobb@yandex.ru

Банки – одни из самых благодарных клиентов фирм, занимающихся информационной безопасностью!

Почему?

Потому что им есть что защищать и есть чем за это платить. Бюджеты банков на безопасность всегда были большими. Но вот всегда ли они используются эффективно? И что значит «эффективно» в данном случае?

Эффективным можно считать такое расходование средств на безопасность, при котором риски по всем возможным угрозам уравновешены и приведены к приемлемому для ведения бизнеса уровню. Одной из неприятных особенностей угроз является их постоянное изменение. Прошло то время когда грабеж банка ассоциировался с вооруженным ограблением, это стало практически не осуществимо и не применимо на практике из-за большой сложности и риска быть пойманным.

Капиталы теперь представляют собой биты и байты, хранящиеся не в сейфах. Таким образом, хоть физической безопасности никто не отменял, все большую актуальность приобретает защита информации. Но, к сожалению, в отличие от золота в слитках или денежные купюры, информацию нельзя запереть в сейф. Она должна быть доступна. Причем зачастую не только сотрудникам, но и клиентам. Администраторам безопасности приходится своими руками открывать доступ к тому, что они обязаны защищать.

Сейчас на рынке услуг предлагается большое количество продуктов, решающих те или иные задачи в области защиты информации. Даже – слишком большое количество. И тогда решения начинают носить спонтанный характер. Но, к примеру, никому не нужен сейф без дверцы, так и частичная информационная защита тоже бесполезна и даже опасна, так как создает иллюзию безопасности.

Что же нужно?

Нужна система, которая:

– учитывает все места хранения информации;

– учитывает все каналы передачи информации;

– учитывает все возможные точки доступа к информации;

– позволяет предоставлять доступ к информации уполномоченным сотрудникам и клиентам, доступ в нужном месте и в нужном виде;

– позволяет блокировать доступ к информации тем, кому он не разрешен;

– позволяет контролировать текущую ситуацию;

– позволяет управлять всеми своими элементами;

– обладает достаточной гибкостью и масштабностью.

Нет ни одного производителя, который бы предлагал продукты на все случаи жизни. Необходимо объединение в одну систему продуктов многих поставщиков.

Выделим основные типовые элементы информационной защиты банковских учреждений:

– защита периметра информационных систем;

– обеспечение внутренней безопасности;

– защита выделенных внутренних серверных ресурсов;

– защита филиалов и удаленных офисов;

– организация безопасной передачи данных по открытым сетям;

– централизованное управление и мониторинг.

Перед построением системы безопасности информации требуется выявить информационные ресурсы и информационные потоки, имеющуюся организационную структуру и типологию, список используемого программного и аппаратного оборудования, а также уже имеющиеся системы защиты. Иными словами – требуется аудит. Только в этом случае можно получить реальную картину. Также можно для правдивости и реальности проведенного аудита прибегать к услугам независимой компании. Это позволит дополнительно выявить недостатки.

В последнее время среди производителей отчетливо наблюдается тенденция построения решений типа «все в одном». У специалистов это называется UTM (Unified Threat Management – унифицированная защита от угроз). Благодаря этому подходу теперь можно построить комплексную защиту, используя продукты 3–4 производителей, хотя раньше для этого требовалось связать вместе изделия 10–15 компаний.

Защита периметра

Первыми средствами обеспечения безопасности корпоративных сетей были межсетевые экраны (МСЭ). Эти программные или аппаратно-

программные комплексы ставятся на границе между корпоративной сетью и Интернетом.

Как правило, такие экраны обеспечивают выполнение целого ряда задач. Все их перечислить довольно сложно. Выделим основные задачи, решаемые МСЭ:

Контроль доступа определяет, кто, откуда и к каким приложениям и ресурсам должен иметь доступ. Причем это касается как входящих соединений (доступ внешних пользователей к ресурсам банка), так и исходящих (обращение сотрудников к внешним ресурсам).

Защита от атак на всех уровнях. Существует довольно много технологий некорректного использования легальных сервисов. Соответственно, системы защиты должны выявлять во всем объеме трафика подобные попытки и блокировать их.

Аутентификация пользователей позволяет персонифицировать доступ к тем или иным ресурсам, что особенно важно в финансовых учреждениях, где существуют строгие градации уровней доступа для различных категорий сотрудников и клиентов.

Трансляция адресов позволяет использовать внутри корпоративных систем приватное адресное пространство, что значительно упрощает управление сетями и в определенных случаях повышает их безопасность.

Обеспечение непрерывности бизнеса на периметре подразумевает резервирование как самих МСЭ, так и каналов доступа, что позволяет банкам быть застрахованными даже от проблем с провайдерами.

Обеспечение внутренней безопасности

Как бы хорошо ни была организована защита периметра, этого недостаточно. Потребность в обеспечении внутренней безопасности обусловлена двумя причинами.

Наличие богатого набора интерфейсов (например, приводы дисководов, компакт-дисков или порты USB) делает практически каждый компьютер частью периметра информационной системы.

Для обеспечения высокого уровня безопасности, особенно в финансовых учреждениях, необходимо обеспечивать защиту и от внутренних пользователей, которые, иногда по незнанию, а иногда и целенаправленно, могут нанести ущерб.

Решать вопросы внутренней безопасности можно на двух уровнях: на уровне межсетевых устройств и непосредственно на самих рабочих станциях. Лучше всего, когда охвачены оба уровня.

Для защиты на самих рабочих станциях используется набор функций, которые обладают большими возможностями. Перечислим некоторые из них:

– персональный экран, защищающий как сам компьютер, так и остальную сеть от действий пользователя;

– контроль доступа к конкретным приложениям и данным;

– проверка системы на наличие вредоносных программ;

– проверка программного обеспечения системы на наличие обновлений;

– контроль работы антивирусного программного обеспечения и актуальности его баз;

– возможность детального контроля сервисов персональных сообщений, таких, как ICQ, MSN Messenger и др.;

– возможность как централизованного, так и локального управления. В случае необходимости локальное управление может быть заблокировано.

Литература

1. *Левен И.* Информационная безопасность в банке, статья опубликована в журнале «CIO» №4 от 28 апреля 2007 г.

2. *Демин В.С.* Автоматизированные банковские системы. М.: Менатеп-Информ, 1997.

РАЗРАБОТКА СИСТЕМЫ НОРМАТИВНО-СПРАВОЧНОЙ ИНФОРМАЦИИ (НСИ). ПОЛИТИКА БЕЗОПАСНОСТИ СИСТЕМЫ НСИ

В.Н. Елисеев, студент 5-го курса каф. КИБЭВС

ТУСУР, г. Томск, freelvlan@sibmail.com

В современном мире, мире крупных компаний, корпораций и холдингов существует актуальная задача внутренней консолидации информации, мониторинга и оптимального планирования. Зачастую в различных филиалах или подразделениях одного предприятия имеются свои правила именования материалов, товаров и прочего. Одно подразделение может использовать один тип ресурсов, а другое использует некое комплексное решение. Помимо ресурсов в различных филиалах одного предприятия стандарты, требования, правила, положения и пр. управляющая информация могут различаться. При этом собрать со всех подразделений однородную информацию, например о затратах на один вид ресурсов, становится нелегкой задачей. Однако даже при создании единого информационного пространства свести все справочники к единому знаменателю оказывается нелегко.

Для решения именно такого рода задач предназначена предлагаемая система НСИ: поддержание корпоративных данных в актуальном со-

стоянии, обеспечение полноты, устранение ошибок и избыточности, контроль целостности и непротиворечивости данных.

Внутреннее представление данны*х.* Разрабатываемая система НСИ предполагает разделение всей системы предприятия на 3 уровня: верхний, нижний, пользовательский. Верхним уровнем является управляющий офис предприятия, нижний – филиалы и подразделения, под пользовательским уровнем понимается работа с системой пользователей, не относящихся к данному предприятию или не имеющих достаточно привилегий для работы на верхнем и нижнем уровнях системы. Все справочники в системе представлены в виде дерева.

Принцип работы. Для получения данных о справочниках предприятия используется клиентская часть системы с единым графическим интерфейсом. Все справочники, учетные записи пользователей и изменения хранятся в базе данных под управлением СУБД Oracle 10g. Запросы и ответы имеют единый XML-формат и обрабатываются движком системы на сервере. Для получения нужной информации пользователю необходимо сформировать запрос на клиентской части системы и отправить на сервер. После обработки запроса сервер, исходя из данных запроса и информацией в базе данных, пришлет ответ с требуемой информацией.

Модель политики безопасности. Для защиты реализуемой системы НСИ от несанкционированного доступа (НСД) каждый пользователь после регистрации получит свой уникальный идентификатор (ID), будет отнесен к определенной группе пользователей, а также наделен необходимым количеством привилегий для работы с системой в зависимости от того, на каком уровне системы он находится. Перед началом работы с системой каждый пользователь должен пройти процесс идентификации и аутентификации. Только после этого он будет допущен в систему.

Часто в зависимости от деятельности или специфики предприятия требуется разработка сложной индивидуальной системы НСИ, в которой проработаны и оговорены все нюансы ее функционала. Данная система НСИ предлагается для использования как универсальное средство для оптимизации и безопасности внутреннего документооборота предприятий и благодаря модульной организации может расширять свой функционал по мере необходимости.

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ В ОБЛАСТИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ИСТОРИЯ СОЗДАНИЯ, ТЕКУЩЕЕ СОСТОЯНИЕ И ПРОБЛЕМЫ

С.С. Ерохин, инженер; С.В. Голубев, студент 4-го курса ФВС
ТУСУР, г. Томск, кафедра КИБЭВС, cmisas@sibmail.com

В 1990 г. под эгидой Международной организации по стандартизации (ИСО) и при содействии в дальнейшем государственных организаций США, Канады, Великобритании, Франции, Германии и Нидерландов были развернуты работы по созданию международного стандарта (исторически сложившееся название – Общие критерии) в области оценки безопасности информационных технологий (ИТ). Разработка этого стандарта преследовала следующие основные цели:

- унификация национальных стандартов в области оценки безопасности ИТ;
- повышение уровня доверия к оценке безопасности ИТ;
- сокращение затрат на оценку безопасности ИТ на основе взаимного признания сертификатов.

В 1996 г. появилась версия 1.0 «Общих критериев», которая, помимо публикации в Internet для всеобщего свободного доступа, была одобрена ISO и обнародована в качестве Проекта Комитета.

Широкое открытое обсуждение документа и «опытная эксплуатация» привели к его существенной переработке и выходу версии 2.0 ОК в мае 1998 г. В версии 2.1 ОК 34-[36], принятой в августе 1999 г, были учтены мнения экспертов. Соответствующий международный стандарт ISO/IEC 15408-1999 53-[55] введен в действие с 1 декабря 1999 г. Таким образом, фактически стандарт ISO/IEC 15408-1999 и версия 2.1 ОК совпадают, а если пренебречь описываемыми ниже нюансами, их названия могут считаться взаимозаменяемыми.

В 1998 г. правительственными организациями Канады, Франции, Германии, Великобритании и США было подписано соглашение о взаимном признании оценок (The International Mutual Recognition Arrangement – MRA), полученных на основе Общих критериев. В соответствии с этим Соглашением стороны намеревались признавать сертификаты на продукты и системы ИТ, полученные в странах, присоединившихся к Соглашению, если они получены на основе применения Общих критериев и выданы организациями, удовлетворяющими требованиям Соглашения. Установленные в MRA правила позволяли присоединиться к Соглашению как в виде участника, только признающего сертификаты, выданные в соответствии с ОК, так и в виде участника, выдающего эти сертификаты.

В середине 90-х гг. Британский институт стандартов (BSI) при участии коммерческих организаций, таких как Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks&Spencer, Logica и др., занялся разработкой стандарта управления информационной безопасностью. И в 1995 г. был принят национальный британский стандарт BS 7799 управления информационной безопасностью организации вне зависимости от сферы ее деятельности. Первая часть стандарта носила рекомендательный характер. Вторая часть была предназначена для сертификации и содержала часть обязательных требований, не входивших в первую часть. Как и любой национальный стандарт BS 7799 в период 1995–2000 гг. пользовался, скажем, так, умеренной популярностью только в рамках стран британского содружества.

Что же касается официальной сертификации по ISO 17799, то она изначально не была предусмотрена (полная аналогия с BS 7799). Была предусмотрена только сертификация по BS 7799:2, который представлял собой ряд обязательных требований (не вошедших в первую часть BS 7799/ISO 17799) и в приложении перечень условно обязательных (на усмотрение сертификатора) наиболее важных требований BS7799:1/ISO 17799. Процедура сертификации по ISO должна была появиться только после выхода в рамках ISO стандарта аналога BS 7799:2 (отметим, что это случилось только в конце 2005 г. с выходом сертификационного стандарта ISO 27001). В 2005 г. вышла новая значительно расширенная по сравнению с 2000 г. редакция стандарта ISO 17799:2005.

В 2005 г. в рамках ISO появился сертификационный стандарт ISO 27001, пришедший на смену BS 7799:2, и теперь сертификация проводится уже по ISO 27001.

В 2006 г. международный комитет по разработке стандартов информационной безопасности (ISO/IEC JTC 1/SC 27/WG 1) принял решение объединить стандарты в области управления информационной безопасностью под одним серийным номером в 27000 серию.

ISO27000	Определения и основные принципы. Планируется унификация со стандартами COBIT и ITIL. Проект стандарта находится в разработке.
ISO27001	ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Выпущен в июле 2005 г.
ISO27002	ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.
ISO27003	Руководство по внедрению системы управления информационной безопасностью. Выпуск запланирован на 2008 г.

ISO27004	Измерение эффективности системы управления информационной безопасностью. Дата выхода неизвестна.
ISO27005	Управление рисками информационной безопасности (на основе BS 7799-3:2006). Выпуск запланирован на 2008 г.
ISO27006	ISO/IEC 27006:2007 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью
ISO27007	Руководство для аудитора СУИБ (в разработке).
ISO27011	Руководство по управлению информационной безопасностью для телекоммуникаций (в разработке).

Основными проблемами в области международной стандартизации ИБ являются:

- недостаточное развитие законодательной базы;
- противоречия международных и национальных стандартов;
- слабо проработанная терминологическая база;
- малый объем судебной практики по спорным вопросам ИБ;
- отсутствие готовых правил, решений, методик;
- слабая проработка отдельных направлений;
- сложность стандартизации новых, быстроменяющихся технологий;
- отсутствие социальной ориентации на требования сотрудников;
- недоступность практических наработок, вызванная необходимостью сохранения коммерческой тайны предприятия.

Литература

1. *Кобзарь М., Сидак А.* Методология оценки безопасности информационных технологий по общим критериям. http://www.jetinfo.ru/2004/6/1/article1.6.2004.html

2. *Медведовский И.* ISO 17799: Эволюция стандарта в период 2002–2007. http://dsec.ru/about/articles/iso17799_evolution/

3. *Цирлов В., Марков А.* Управление рисками – нормативный вакуум информационной безопасности. http://www.osp.ru/os/2007/08/4492873/

РАСЧЕТ АКУСТИЧЕСКИХ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ

А.А. Филиппов, А.В. Седунов, студенты 5-го курса КИБЭВС

ТУСУР, г. Томск, anton1@sibmail.com, al_sed@sibmail.com

Акустический канал утечки информации состоит из трех составляющих: источника опасного сигнала, физической среды его распро-

странения (воздух, вода, земля, строительные и другие конструкции) и технического средства его приема, определяющих физический путь, по которому злоумышленник обеспечивает несанкционированное получение информации. Следует отметить, что средством перехвата акустической информации является человеческое ухо, возможности которого можно существенно улучшить за счет различных технических средств и решений.

Виброакустический канал утечки информации обеспечивает возможность прослушивания помещений с помощью электронных стетоскопов или радиостетоскопов. После усиления и простейшей обработки этот сигнал может быть прослушан, записан на магнитофон или передан по радиоканалу. Информация может сниматься со стен, перекрытий, дверей, оконных рам и стекол, труб отопления и водоснабжения, различных коробов и т.д.

Для обнаружения возможных акустических и виброакустических каналов утечки информации необходимо произвести измерения акустических показателей, рассчитать показатели акустической защищенности и сравнить с нормативными значениями.

В данной работе измерения проводились с помощью программно-аппаратного комплекса «ГРИФ-АЭ1001», предназначенного для проведения проверок выполнения норм эффективности защиты речевой информации от утечки по акустическому, виброакустическому каналам и по каналу низкочастотных наводок на линиях коммуникаций.

Для измерения акустических и виброакустических показателей использовались элементы блока, такие как направленный микрофон и акустическая колонка АКМ-01 с уровнем сигнала 70 дБ.

В соответствии с методикой проведения специальных исследований технических средств по измерению акустических и виброакустических показателей необходимо было провести следующие операции:

1. При помощи микрофона и акустической колонки АКМ-01 измерить излучаемый уровень тест-сигнала для каждой октавной полосы частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц.

2. При помощи микрофона измерить уровень шума в контрольной точке для каждой октавной полосы частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц.

3. При помощи микрофона и акустической колонки измерить отношение «сигнал/шум» в контрольной точке для каждой октавной полосы частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц.

После проведения измерений применялся инструментально-расчетный метод оценки разборчивости речи.

Для оценки защищенности каналов утечки информации используются два критерия – энергетический и смысловой.

Энергетическим показателем является распределение отношений «сигнал/шум», дБ, в октавных полосах частот в контрольных точках для нормированного энергетического спектра речевого сигнала.

Смысловым критерием является словесная разборчивость речи W – относительное или процентное количество принятых специально тренированными слушателями (артикулянтами) слов из общего количества переданных по тракту.

Так как программно аппаратный комплекс «ГРИФ-АЭ1001» не имеет собственной расчетной программы, то была разработана программа для вычисления интегрального индекса артикуляции речи R и зависимости словесной разборчивости от интегрального индекса артикуляции речи W. Все вычисления в данной программе производятся по следующим формулам:

$$\Delta A(f_{\text{ср}i}) = \begin{cases} \dfrac{200}{f^{0,43}} - 0,37, & \text{если } f \le 1000 \text{ Гц}; \\ 1,37 - \dfrac{1000}{f^{0,69}}, & \text{если } f > 1000 \text{ Гц}; \end{cases} \quad (1)$$

$$k(f) = \begin{cases} 2,57 \cdot 10^{-8} f^{1,18}, & \text{если } 100 < f < 400 \text{ Гц}; \\ 1 - 1,047 \exp(-10^{-4} \cdot f^{1,18}), & \text{если } 400 < f < 10000 \text{ Гц}; \end{cases} \quad (2)$$

$$p_i = \begin{cases} \dfrac{0,78 + 5,46 \exp[4,3 \cdot 10^{-3} (27,3 - |O_i|)^2]}{1 + 10^{0,1|O_i|}}, & \text{если } q_i \le A_i; \\ 1 - \dfrac{0,78 + 5,46 \exp[4,3 \cdot 10^{-3} (27,3 - |O_i|)^2]}{1 + 10^{0,1|O_i|}}, & \text{если } q_i > A_i; \end{cases} \quad (3)$$

$$R = \sum_i p_i k_i, \quad (4)$$

$$W = \begin{cases} 1,54 R^{0,25} [1 - \exp(-11R)], & \text{если } R < 0,15; \\ 1 - \exp(-\dfrac{11R}{1 + 0,7R}), & \text{если } R \ge 0,15; \end{cases} \quad (5)$$

где $\Delta A(f_{\text{ср}i})$ – формантный параметр, характеризующий энергетическую избыточность дискретной составляющей речевого сигнала; $k(f)$ – весовой коэффициент; R – интегральная артикуляция речи; p_i – коэффициент

восприятия формант слуховым аппаратом человека, представляющий собой вероятное относительное количество формантных составляющих речи, которые будут иметь уровни интенсивности выше порогового значения;

$$O_i = q_i - \Delta A_i, \qquad (6)$$

O_i – относительный уровень интенсивности формат; q_i – отношение «уровень речевого сигнала/уровень шума», дБ.

Также данная программа позволяет рассчитать октавные уровни звукоизоляции и виброизоляции по формуле

$$Q_i = L_{ci} - L_{\text{ш}i},$$

где Q_i – уровень звукоизоляции.

В результате исследования были получены следующие данные при $R = 0{,}56$; $W = 0{,}78$.

Октавные полосы	$L_{\text{ш}i}$, дБ	$L_{(\text{с+ш})i}$, дБ	L_{ti}, дБ	Q_i, дБ
250	67,195	77,483	108,543	41,348
500	68,550	77,666	112,827	44,277
1000	71,263	77,213	113,825	42,562
2000	74,450	78,804	115,433	40,983
4000	77,287	77,957	113,687	36,4

Вывод. По результатам измерений, звукоизоляция данного помещения не соответствует нормативным требованиям, что говорит о незащищенности помещения.

Литература

1. *Зайцев А.П., Шелупанов А.А.* Технические средства и методы защиты информации. Ч. 1. Учеб. пособие. Томск: Изд-во Том. гос. ун-та систем управления и радиоэлектроники, 2005.

2. *Хорев А.А., Железняк В.К., Макаров Ю.К.* Некоторые методические подходы к оценке эффективности защиты речевой информации.

ЗАЩИТА БАНКОВСКОЙ ТАЙНЫ ОТДЕЛЕНИЯ СБЕРБАНКА

С.Н. Филькин, студент 5-го курса; К.Н. Филькин, аспирант;
Г.А. Праскурин, ассистент кафедры КИБЭВС
ТУСУР, г. Томск

Сбербанк РФ занимает отдельное положение среди банков, так как только он имеет свои отделения и филиалы по всей стране, образующие единую распределенную иерархическую структуру. В силу этого Сбербанк России имеет свой стандарт по информационной безопасности и

свои внутренние нормативные документы, регламентирующие порядок и содержание действий, направленных на обеспечение информационной безопасности.

Цель системы обеспечения ИБ Политика информационной безопасности Сберегательного банка определяет следующим образом: создание и постоянное соблюдение в Банке условий, при которых риски, связанные с нарушением безопасности информационных активов банка, постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска.

Нормативные документы Сберегательного банка по обеспечению информационной безопасности выделяют множество сведений, составляющих банковскую тайну и подлежащих защите. Однако отделения Банка работают лишь с несколькими из них. В табл. 1 приведены основные из сведений, подлежащих защите.

Перечень сведений, составляющих КТ

Сведения	Срок отнесения к коммерческой тайне
1. Содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности. Принадлежность к КТ определяется в каждом конкретном случае	не менее 5 лет
2. Условия заключаемых и заключенных в рамках кредитных сделок договоров (кредитных договоров, договоров поручительства, договоров залога и т.п.)	В течение 5 лет после истечения срока действия кредитного договора
3. Материалы о невозвратности кредитов	Определяется в каждом конкретном случае
4. Сведения о технической укрепленности и оборудовании Банка средствами сигнализации, системами контроля доступа	В течение всего срока применения
5. Информация о месторасположении и размерах помещений, в которых осуществляются операции с денежной наличностью и другими ценностями	Постоянно
6. Базы данных автоматизированных систем по реально проведенным операциям, процедуры доступа к информационным ресурсам	В течение всего срока применения

Самыми критичными для безопасности банковской тайны являются базы данных автоматизированных систем, процедуры доступа к информационным ресурсам.

С точки зрения безопасности любое лицо, имеющее логический или физический доступ к информационным активам и компонентам соответствующих информационных технологий может являться потенциальным злоумышленником. При этом предполагается возможность сговора сотрудника Банка с внешним злоумышленником, но не сговор двух и более сотрудников Банка.

Для обеспечения информационной безопасности и противодействию угрозам информационных активов в Сбербанке РФ используются следующие принципы:

1) осведомленность сотрудников о риске информационной безопасности;

2) персональная ответственность за нарушения требований информационной безопасности;

3) минимальность полномочий – доступ к информационным активам предоставляется только в объеме, необходимом для выполнения служебных обязанностей;

4) разделение полномочий – выполнение критичных банковских операций двумя сотрудниками;

5) контроль лимитов и ограничений – ограничение по сумме, времени и другим показателям проведения критичных банковских операций;

6) комплексность защиты – меры по обеспечению безопасности информационных активов принимаются по всем видам угроз с учетом оценки рисков;

7) адекватность защиты – принимаемые меры должны быть адекватны имеющим место рискам информационной безопасности;

8) непрерывность процессов контроля – должен осуществляться постоянный мониторинг и аудит системы обеспечения информационной безопасности;

9) пассивность контроля – средства информационной безопасности не предоставляют доступ сотрудникам, ответственным за их эксплуатацию, непосредственно к критичной банковской информации.

Специфическими для Сбербанка являются принципы разделения полномочий и контроля лимитов и ограничений. Эти принципы обеспечивают корректность выполнения банковских операций и доступа к базам данных.

Литература

1. Нормативные документы по информационной безопасности Сбербанка РФ.

2. *Соколов А.В., Степанюк О.М.* Защита от компьютерного терроризма: Справ. пособие. СПб.: БХВ-Петербург Арлит, 2002. 498 с.

МЕТОДЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

С.В. Голубев, студент 4-го курса КИБЭВС
ТУСУР, г. Томск, кафедра КИБЭВС, cmisas@sibmail.com

Процесс регистрации пользователя в системе состоит из трех взаимосвязанных, выполняемых процедур: идентификация, аутентификация и авторизация

Идентификация – это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

В общем случае **идентификатор пользователя –** некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей. Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Аутентификация – это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Современные методы аутентификации основываются на множественных факторах (существует и широко применяется двухфакторная аутентификация, известны примеры трехфакторной аутентификации).

Многофакторная аутентификация – аутентификация, в процессе которой используется аутентификационные факторы нескольких типов.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

- индивидуального объекта заданного типа;
- знаний некоторой известной только ему и проверяющей стороне информации;
- индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие печать, удостоверения, пропуска, магнитные карты, аппаратные токены и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники. Уникальность каждого из перечисленных предметов определяется информацией, которую он содержит. В простейшем случае эта информация представляет собой идентификатор и пароль пользователя, которые просто считываются с носителя и передаются модулю аутентификации. Более сложный случай – носитель содержит криптографический

ключ, который используется в каком-либо из протоколов удаленной аутентификации.

Уникальный предмет используется сам по себе довольно редко: чаще всего это один из элементов двухфакторной аутентификации.

Аутентификация обладает и рядом недостатков:

- предмет может быть похищен или отнят у пользователя;
- в большинстве случаев требуется специальное оборудование для работы с предметами;
- теоретически возможно изготовление копии или эмулятора предмета.

Во вторую группу входят методы аутентификации, использующие пароли. При некомпьютерном использовании это может быть произносимый голосом пароль или запоминающаяся комбинация для замка. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты. Запоминаемое секретное слово может быть наиболее удобным средством с точки зрения перемещающихся пользователей, т.е. для организации удаленного доступа. К недостаткам парольной аутентификации относятся:

- выбор пользователем простого, легко угадываемого пароля;
- возможность подсмотреть или перехватить пароль при вводе;
- получение пароля путем применения насилия к его владельцу;
- использование методов социальной инженерии.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя. В настоящее время существует множество методов биометрической аутентификации, которые делятся на две группы: статические и динамические. Статические методы биометрической аутентификации основываются на физиологической (статической) характеристике человека, т.е. уникальной характеристике, данной ему от рождения и неотъемлемой от него, к ним относится:

- по отпечатку пальца;
- по форме ладони;
- по расположению вен на лицевой стороне ладони;
- по сетчатке глаза (по рисунку кровеносных сосудов глазного дна);
- по радужной оболочке глаза;
- по форме лица;
- по термограмме лица;

- по ДНК;
- другие методы.

Динамические методы биометрической аутентификации основываются на поведенческой (динамической) характеристике человека, т.е. построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия, к ним относятся:

- по рукописному почерку;
- по клавиатурному почерку;
- по голосу;
- другие методы.

Общей характеристикой, используемой для сравнения различных методов и способов биометрической идентификации – являются статистические показатели – ошибка первого рода (не пустить в систему «своего») и ошибка второго рода (пустить в систему «чужого»). Сортировать и сравнивать описанные выше биометрические методы по показаниям ошибок первого рода очень сложно, так как они сильно разнятся для одних и тех же методов из-за сильной зависимости от оборудования, на котором они реализованы.

По показателям ошибок второго рода статические методы идентификации существенно лучше динамических.

Недостатки биометрической аутентификации:

- необходимость в оборудовании для считывания биометрических характеристик;
- сложность смены аутентификационной информации при компрометации;
- влияние условий окружающей среды;
- религиозные и культурный фактор.

Литература

1. *Мещеряков Р.В., Праскурин Г.А.*Теоретические основы информационной безопасности автоматизированных систем: В 2-х разд. Томск: Том. Межвуз. центр дистанционного образования, 2005. Разд. 1. 147 с.

2. *Лакин Г.Ф.* Биометрия. М.: Высш. шк., 1990. 352 с.

3. *Ричард Э. Смит* Аутентификация: от паролей до открытых ключей. М.: Вильямс, 2002. С. 432.

СТРАХОВАНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ СПЕЦИАЛИЗИРОВАННОГО ОПЕРАТОРА СВЯЗИ

О.С. Горшков, студент 5-го курса каф. КИБЭВС
ТУСУР, г. Томск, leshij@sibmail.com

Существующая система сдачи налоговой и бухгалтерской отчетности на бумажных носителях далека от идеала. Но жизнь не стоит на месте, и электронные возможности пришли и в эту сферу. У компаний теперь есть законный выбор: они могут представлять отчетные документы в электронном виде. А для некоторых предприятий с недавних пор это стало обязанностью. Многое зависит от партнера – специализированного оператора связи.

Специализированный оператор связи – организация, предоставляющая услуги по обмену открытой и конфиденциальной информацией между налоговыми органами и налогоплательщиками в рамках системы представления налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи.

Преимущества электронного способа сдачи отчетности для компаний очевидны. Во-первых, программа контролирует соответствие заполнения документов, высылаемых фирмой в адрес проверяющих, формату ФНС. Во-вторых, вся информация между организацией и инспекцией передается в зашифрованном виде, что обеспечивает ее полную безопасность и конфиденциальность. Кроме того, формы отчетности и реквизиты инспекций и счетов, необходимые для налоговых выплат, обновляются своевременно. Да и выгоды для налоговых органов налицо – присланные отчитывающейся компанией сведения автоматически разносятся на лицевые счета, что избавляет от необходимости перенабирать данные, как следствие, исчезают связанные с этим опечатки. Представленная информация обрабатывается быстрее, что делает процесс выверки платежей более оперативным.

В любом случае, какие бы методы защиты не проводились вероятность наступления риска все-таки существует. Как ответ на возникающие новые угрозы в области информационных технологий Ингосстрахом разработана Программа страхования информационных рисков, в основе которой лежит принципиально новый вид страхования: Страхование информационных систем.

На сегодняшний день это единственная в России программа страхования информационных рисков, предоставляющая полноценную защиту от компьютерных атак, несанкционированного доступа к компьютерным системам, компьютерных вирусов, преступных действий сотрудников, а также убытков от перерыва в коммерческой деятельности и дополнительных расходов, возникающих вследствие утраты информации.

Страхование реализуется в виде последовательного выполнения 5 обязательных шагов:

1) переговоры, определяющие условия страхования;
2) разработка и согласование предложений по страхованию;
3) проведение экспертизы страхователя;
4) выполнение рекомендаций, полученных в результате экспертизы;
5) подписание договора о страховании.

Прежде чем страховая компания примет на себя риски страхователя, она должна убедиться, что сеть страхуемой компании не является незащищенной, и первая же атака не приведет к наступлению страхового случая. Другими словами, непременным условием страхования информационных рисков является проведение специальной экспертизы по анализу рисков страхового объекта. Эта экспертиза называется – «сюрвей» (от английского «survey» – «осмотр»), проводится экспертами в области информационной безопасности, которые и выносят свой вердикт об уровне защищенности страхуемой компании.

В случае выполнения всех пунктов между страховой и страхуемой компаниями заключается полис. В рамках полиса могут быть застрахованы любые программные и программно-аппаратные информационные системы, предназначенные для сбора, передачи, хранения и обработки информации, в том числе системы управления производством, ERP-системы, системы электронного документооборота, внутрикорпоративные центры сертификации (удостоверяющие центры), биллинговые системы, веб-серверы, локальные вычислительные сети компаний и т.п.

В качестве объектов страхования по полису выступают:

Информационные ресурсы

– информация в любом виде – базы данных, библиотеки, архивы в электронной форме на технических носителях любого рода;

– программные средства и комплексы, находящиеся в разработке или эксплуатации.

Финансовые активы

– денежные средства в электронной форме в виде записей на счетах (системы клиент-банк);

– ценные бумаги в электронном (бездокументарном) виде.

Кроме страхования информационных ресурсов, страховые компании предлагают страховать и электронное оборудование.

Данное страхование особенно актуально при наличии у страхователя:

– разветвленных вычислительных, информационных систем, LAN/WAN сетей;

– телекоммуникационных систем, систем связи и телефонии, систем АТС;

– систем хранения информации;

– систем бесперебойного питания;

– систем управления доступом и систем технической безопасности;

– подобного дорогостоящего оборудования, принадлежащего страхователю или арендуемого страхователем.

Также предлагается страхование гражданской ответственности.

Могут быть застрахованы следующие виды гражданской ответственности:

– ответственность, связанная с эксплуатацией зданий и помещений;

– ответственность перед работниками компании;

– ответственность за нанесение ущерба своим клиентам при предоставлении различных услуг в области информационных технологий;

– ответственность удостоверяющего центра ЭЦП;

– ответственность регистратора доменных имен.

Плюсов у страхования много, причем для всех участников этого процесса. Самый главный плюс получает страхователь, который сможет возместить свои потери в результате любых воздействий на информационные ресурсы. Экспертной компании, проводящей сюрвей, страхование предоставляет новых клиентов. При этом экспертная компания в выигрыше в любом случае, так как ее услуги оплачиваются независимо от заключения договора страхования. Страховая компания также получает не малую выгоду от заключенного полюса со страхуемой компанией.

ОБНАРУЖЕНИЕ ПЭМИ КЛАВИАТУРЫ КОМПЬЮТЕРА

А.В. Грасмик, студент 5-го курса КИБЭВС ФВС

ТУСУР, г. Томск, GrasmikAV@sibmail.com

Одним из наиболее опасных каналов утечки информации является наличие побочных электромагнитных излучений, возникающих в процессе работы различных электронных устройств. Побочные электромагнитные излучения (ПЭМИ) – это паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными.

Постановка задачи – необходимо обнаружить ПЭМИ клавиатуры и рассчитать зоны разведдоступности данного ТС.

Решение. Обнаружение ПЭМИ проводились по магнитной составляющей электромагнитного поля (по электрической составляющей не представляется возможным). Исследования проводились с помощью программно-аппаратного комплекса «Легенда», предназначенного для поиска и измерения в автоматическом и полуавтоматическом режимах

побочных электромагнитных излучений и наводок, создаваемых исследуемыми техническими средствами электронно-вычислительной техники, автоматизированного расчета опасных зон R1 и R2 и контроля защищенности объектов ЭВТ.

В соответствии с методикой специальных исследований технических средств по измерению их собственного электромагнитного излучения проводились следующие действия:

1. Использовался тестовый режим клавиатуры (нажатие клавиши "=").

2. На расстоянии 1 м от устройства устанавливалась антенна для приема магнитной составляющей поля, изучаемого анализируемым устройством.

3. Сигналы с выхода антенны подавались на вход анализатора спектра, с помощью которого по результатам измерений по определенной методике производился расчет контролируемой зоны.

Проблема выделения сигналов, обладающих информационными признаками и относящихся к излучению исследуемого устройства, решалась с использованием:

– энергетического принципа пропадания сигнала при отключении контролируемого устройства;

– информационного принципа – перед проведением исследования производится формирование эталонного образа искомого сигнала, и в процессе исследования осуществляется автоматическое обнаружение сигналов в эфире, похожих на этот эталонный сигнал.

Сравнение обнаруженного сигнала и образа эталонного сигнала производилось путем вычисления программой максимума взаимно-корреля-ционной функции между образами сигналов. При превышении данной величиной установленного порогового значения, принималось решение о схожести образов. При этом исключалась возможность причисления к перечню обнаруженных частот посторонних сигналов и неинформативных ПЭМИ исследуемого технического средства.

В полуавтоматическом режиме работы управляющей программы последовательным сканированием частотного диапазона от единиц килогерц с обзором 0,1 МГц на основе энергетического принципа нашли на частоте 0,311 МГц тестовый сигнал для клавиатуры, который и взяли за эталонный сигнал для последующих операций.

В автоматическом режиме, задав соответствующие настройки и выбрав эталонный сигнал, обнаружили гармоники тестового сигнала, проконтролировали соответствие нашему сигналу.

Автоматизированный расчет минимально допустимых расстояний от элементов технических средств до границы контролируемой зоны (зона

R2), до сосредоточенных случайных антенн (зона r1), до рассредоточенных случайных антенн (зона r1') по 1, 2 и 3-й категориям выполнялся расчетной программой. Далее составлялось задание условий для расчета, которое содержало пункты:

– измерительная аппаратура: анализатор спектра;

– устройство: клавиатура (способ кодирования – последовательный, вид используемого кода – импульсный);

– составляющая: магнитная;

– тактовая частота теста: 311 кГц;

– количество тестируемых разрядов: 1;

– антенна: рамочная активная магнитная АГМ-30;

– нормы отношения сигнал/шум для трех категорий – 0,4.

Полученные результаты. После всех проделанных работ расчетная программа создала «Протокол измерений», представленный ниже.

Протокол измерений

Устройство: клавиатура, серийный номер: б/н;

Составляющая: магнитная;

от 0,01 до 30 МГц, «Заря» МА-1.

Ft = 0,311 МГц; 1/τ = 0,000626 МГц; d = 1 м; h = 1 м; Kn=1; Kc = 1;

δ1 к. =0,4; δ2 к. =0,4; δ3 к. =0,4.

Результаты измерений и расчетов

Категория	R2, м	r1, м	r1′, м
первая	42,1	1,4	0,2
вторая	23,6	0,8	0,1
третья	23,6	0,8	0,1

Выводы. В ходе проделанной работы были проведены специсследования побочных электромагнитных излучений USB-клавиатуры и рассчитаны зоны разведдоступности.

Результаты исследований еще раз доказали, что излучение USB-клавиатур имеют довольно низкий уровень и, соответственно, опасная зона меньше чем, например, у мониторов. Клавиатуры с PC/2 и другими портами имеют еще меньшие зоны разведдоступности.

Литература

1. *Мотуз О.В.* Побочные электромагнитные излучения: моменты истории // Защита информации. Конфидент. 2001. № 1.

2. *Генне В.И.* К вопросу оценки уровня ПЭМИ цифрового электронного оборудования // Защита информации. Конфидент. 1999. № 6.

СОЗДАНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.С. Губенков, студент 5-го курса каф. КИБЭВС
ТУСУР, г. Томск, mustdievul@sibmail.com

Обеспечение комплексной информационной безопасности является необходимым условием функционирования любого предприятия. Комплексность заключается, прежде всего, в разумной достаточности, адекватности защитных мер, разработке четких организационно-технических мер и обеспечении контроля над их исполнением.

Адекватный уровень информационной безопасности (ИБ) на предприятие может быть обеспечен только на основе комплексного подхода, предполагающего использование как программно-технических, так и организационных мер защиты на единой концептуальной основе. Причем организационные меры играют существенно более важную роль. Эффективность любых самых сложных и дорогостоящих программно-аппаратных, технических механизмов защиты может быть сведена к нулю в случае игнорирования пользователями информационной системы (ИС) элементарных правил парольной политики или нарушения сетевыми администраторами установленных процедур предоставления доступа к ресурсам корпоративной сети.

Политика безопасности (ПБ) лежит в основе организационных мер защиты информации.

Политика безопасности организации (organizational security policies) – совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

Жизненный цикл политики безопасности можно разделить на следующие этапы:

1. Аудит безопасности

Аудит безопасности – это процесс, который включает в себя проведение обследования, идентификацию угроз безопасности, ресурсов, нуждающихся в защите и оценку рисков. В ходе аудита производится анализ текущего состояния ИБ, выявляются существующие уязвимости, наиболее критичные области функционирования и наиболее чувствительные к угрозам ИБ бизнес-процессы.

2. Разработка

Аудит безопасности позволяет собрать и обобщить сведения, необходимые для разработки ПБ. На основании результатов аудита определяются основные условия, требования и базовая система мер по обеспечению ИБ на предприятие, позволяющих уменьшить риски до

приемлемой величины, которые оформляются в виде согласованных в рамках рабочей группы решений и утверждаются руководством предприятия.

3. Внедрение

На этапе внедрения необходимо не просто довести содержание ПБ до сведения всех сотрудников предприятия, но также провести обучение персонала.

4. Аудит и контроль

Соблюдение положений ПБ является обязательным для всех сотрудников предприятия и должно непрерывно контролироваться.

Проведение планового аудита безопасности является одним из основных методов контроля работоспособности ПБ, позволяющего оценить эффективность внедрения. Результаты аудита могут служить основанием для пересмотра некоторых положений ПБ и внесения в них необходимых изменений.

5. Пересмотр и внесение изменений

Наблюдение за процессом внедрения ПБ и оценки эффективности ее применения могут привести к решению осуществить ряд доработок. В дополнение к этому используемые технологии и организация бизнес-процессов непрерывно изменяются, что приводит к необходимости корректировать существующие подходы к обеспечению ИБ. В большинстве случаев ежегодный пересмотр ПБ является нормой, которая устанавливается самой политикой.

Существует ряд руководящих документов и стандартов в области ИБ, освещающих подходы в организации обеспечения и управления информационной безопасностью предприятия, а также основных положений политики ИБ. Следует выделить серию ГОСТ Р ИСО/МЭК ТО 13335, ИСО/МЭК ТО 27001, РС БР ИББС-2.0-2007, ГОСТ Р ИСО/МЭК 15408.

Литература

1. *Грибунин В.Г.* Разработка и реализация политики безопасности предприятия: www.bre.ru.

2. *Астахов А.А.* Разработка и внедрение эффективных политик информационной безопасности: www.bre.ru.

3. *Компьюлинк* Разработка концепции политики информационной безопасности: www.cio-world.ru

ОБЗОР ПРОГРАММНЫХ ПРОДУКТОВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ АНАЛИЗА И УПРАВЛЕНИЯ РИСКАМИ

А.В. Хоменко, студент 4-го курса ФВС;
А.А. Шелупанов, зав. каф. КИБЭВС, д.т.н., проф.
ТУСУР, г. Томск, кафедра КИБЭВС, AlexRemote@sibmail.com

Из большего разнообразия методов анализа и управления рисками, а также реализующих их программных средств, существующих сегодня, приведем в качестве примеров наиболее распространенные.

CRAMM

Метод CRAMM (the UK Government Risk Analysis and Management Method) был разработан Службой безопасности Великобритании (UK Security Service), взят на вооружение в качестве государственного стандарта.

В настоящее время CRAMM – это довольно мощный универсальный инструмент, позволяющий, помимо анализа рисков, решать также и ряд других аудиторских задач.

В основе CRAMM лежит комплексный подход к оценке рисков, сочетая количественные и качественные методы анализа. Программный продукт является универсальным и подходит как для больших, так и для мелких организаций как правительственного, так и коммерческого сектора.

К недостаткам метода CRAMM можно отнести следующее:

- Использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора.
- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели для ИС, находящихся на стадии разработки.
- Аудит по методу CRAMM – процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора.
- Программный инструментарий CRAMM генерирует большое количество бумажной документации.
- Возможность внесения дополнений в базу знаний CRAMM недоступна пользователям.
- ПО CRAMM существует только на английском языке.
- Высокая стоимость лицензии.

RiskWatch

Программное обеспечение RiskWatch является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности. Оно включает в себя следующие средства аудита и анализа рисков:

– RiskWatch for Physical Security – для физических методов защиты ИС;

– RiskWatch for Information Systems – для информационных рисков;

– HIPAA-WATCH for Healthcare Industry – для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act);

– RiskWatch RW17799 for ISO 17799 – для оценки требованиям стандарта ISO 17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (Annual Loss Expectancy, ALE) и оценка возврата от инвестиций (Return on Investment, ROI).

Семейство программных продуктов RiskWatch имеет массу достоинств. RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. Используемая в программе методика включает в себя 4 фазы.

К недостаткам RiskWatch можно отнести:

• Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов.

• ПО RiskWatch существует только на английском языке.

• Высокая стоимость лицензии – от $15 000 за одно рабочее место для небольшой компании и от $125 000 за корпоративную лицензию.

COBRA

Система COBRA (Consultative Objective and Bi-Functional Risk Analysis), разрабатываемая компанией Risk Associates, является средством анализа рисков и оценки соответствия ИС стандарту ISO17799. COBRA реализует методы количественной оценки рисков, а также инструменты для консалтинга и проведения обзоров безопасности. При разработке инструментария COBRA были использованы принципы построения экспертных систем, обширная база знаний по угрозам и уязвимостям, а также большое количество вопросников, с успехом применяющихся на практике.

К недостаткам COBRA можно отнести:

• устаревший, не слишком удобный для пользователя интерфейс (несмотря, на то, что данный продукт является в этой области одним из наиболее известных на западе, его разработчики по каким-то причинам не занимаются модернизацией его пользовательского интерфейса);

• отсутствие возможности установки пользователем веса на каждое требование;

• отсутствие системы на русском языке;

• возникают проблемы с генерацией отчета под Win98; возможна нестабильная работа при работе с отчетом под Win2000.

ГРИФ

Основная задача системы ГРИФ – дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе и эффективность существующей практики по обеспечению безопасности компании, а также предоставить возможность доказательно (в цифрах) убедить руководство компании в необходимости инвестиций в сферу ее информационной безопасности.

Используемая в программе методика включает в себя 5 этапов. В результате выполнения всех действий по данным этапам на выходе будет сформирована полная модель информационной системы с точки зрения информационной безопасности с учетом реального выполнения требований комплексной политики безопасности, что позволит перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

К недостаткам ГРИФ можно отнести:

- Отсутствие привязки к бизнесс-процессам (запланировано в следующей версии).
- Отсутствие возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности (запланировано в следующей версии).
- Отсутствие возможности добавления специфичных для данной компании требований политики безопасности.

Литература

1. Современные методы и средства анализа и управления рисками информационных систем компаний. http://www.dsec.ru/about/articles/ar_compare/

2. Современные методы и средства анализа и контроля рисков информационных систем компаний.
http://www.ixbt.com/cm/informationsystem-risks012004.shtml

3. Аудит безопасности информационных систем.
http://www.shop.globaltrust.ru/osnov.php?idstat=50&idcatstat=1&PHPSESSID=d8e786bc1e492efcf64657c9757a4295

ОБЗОР СТАНДАРТОВ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

А.В. Хоменко, студент 4-го курса ФВС;
А.А. Шелупанов, зав. каф. КИБЭВС, д.т.н., проф.
ТУСУР, г. Томск, кафедра КИБЭВС, AlexRemote@sibmail.com

В данной публикации дается обзор стандартов информационной безопасности, являющихся наиболее значимыми и перспективными с точки зрения их использования для проведения аудита безопасности ИС.

ISO 17799: Code of Practice for Information Security Management

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью), принятом в 2000 году. ISO 17799 был разработан на основе британского стандарта BS 7799. ISO 17799 может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Практические правила разбиты на 10 разделов. Также имеется десять ключевых средств контроля которые представляют собой либо обязательные требования, например, требования действующего законодательства, либо считаются основными структурными элементами информационной безопасности, например обучение правилам безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования АС и составляют основу системы управления информационной безопасностью.

Процедура аудита безопасности ИС включает в себя проверку наличия десяти ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности ИС также является анализ и управление рисками.

ISO 15408: Common Criteria for Information Technology Security Evaluation

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий), принятом в 1999 году.

Общие критерии оценки безопасности информационных технологий (далее «Общие критерии») определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

При проведении работ по анализу защищенности ИС, «Общие критерии» целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС.

Первая часть «Общих критериев» содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. Требования к функциональности средств защиты приводятся во второй части «Общих критериев». Третья часть «Общих критериев», наряду с другими требованиями к адекватности реализации функций безопасности, содержит класс требований по анализу уязвимостей средств и механизмов защиты.

При проведении работ по аудиту безопасности данные требования могут использоваться в качестве руководства и критериев для анализа уязвимостей ИС.

SysTrust

По существу, аудит в области информационных технологий, хотя и не имеет никакого отношения к финансовому аудиту, часто является дополнением к нему в качестве коммерческой услуги, предлагаемой аудиторскими фирмами своим клиентам, в связи с повышением зависимости бизнеса клиентов от ИТ. Идея заключается в том, что использование надежных и безопасных ИТ-систем до определенной степени гарантирует надежность финансовой отчетности организации. Хорошие результаты ИТ-аудита в некоторых случаях позволяют проводить финансовый аудит в сокращенном варианте, экономя время и деньги клиентов.

Отвечая потребностям бизнеса, Американским институтом сертифицированных публичных бухгалтеров (American Institute of Certified Public Accountants (AICPA)) и Канадским институтом общественных бухгалтеров (Canadian Institute of Chartered Accountants (CICA)) разработан стандарт SysTrust для проведения ИТ-аудита, который является дополнением к финансовому аудиту. SysTrust позволяет финансовым аудиторам расширить область своей деятельности путем использования простого и понятного набора требований для оценки надежности и безопасности ИС.

BSI\IT Baseline Protection Manual

Немецкий стандарт «Руководство по обеспечению безопасности ИТ базового уровня» (IT Baseline Protection Manual) разрабатывается Агенством информационной безопасность Германии (BSI – Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency). Этот документ является, пожалуй, самым содержательным руководством по информационной безопасности и по многим параметрам превосходит все остальные стандарты. Приятен также тот факт, что этот ценнейший для аудитора источник информации имеется в свободном доступе в сети Интернет. В нем содержатся подробные руководства по обеспечению информационной безопасности применительно к различным аспектам функционирования ИС и различным областям ИТ.

Стандарт в настоящее время занимает три тома и содержит около 1600 страниц текста. «BSI\IT Baseline Protection Manual» постоянно совершенствуется с целью обеспечения его соответствия текущему состоянию дел в области безопасности ИТ.

Практические стандарты SCORE и программа сертификации SANS/GIAC Site Certification

SCORE (Security Consensus Operational Readiness Evaluation) является совместным проектом института SANS и Центра безопасности Интернет (Center for Internet Security(CIS)). Профессионалы-практики в об-

ласти информационной безопасности из различных организаций объединились в рамках проекта SCORE с целью разработки базового (минимально необходимого) набора практических стандартов и руководств по обеспечению безопасности для различных операционных платформ. Требования и рекомендации, предлагаемые для включения в стандарты, широко обсуждаются и проверяются участниками проекта SCORE, и только после их одобрения всеми участниками передаются в CIS, который занимается их формализацией и оформлением, а также разрабатывает программные средства (minimum standards benchmarks) для оценки соответствия операционных платформ предложенным стандартам.

Литература

1. Аудит безопасности информационных систем. http://www.shop.globaltrust.ru/osnov.php?idstat=50&idcatstat=1&PHPSESSID=d8e786bc1e492efcf64657c9757a4295

2. *Астахов А.М.* Аудит безопасности информационных систем // Защита информации. Конфидент. 2003. №2. С. 90–96 (Шифр в БД З6Х02/2003/2) ГРНТИ 50.37.23 + 49.33.35

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ ПО РОССИЙСКОМУ ЗАКОНОДАТЕЛЬСТВУ

Д.С. Иванов, студент 5-го курса ФВС

ТУСУР, г. Томск, pitbull@sibmail.com

В сфере оборота компьютерной информации:

а) неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ);

б) операции с вредоносными программами для ЭВМ (ст. 273 УК РФ);

в) нарушение авторских и смежных прав в отношении программ для ЭВМ и баз данных, а также иных объектов авторского и смежного права, находящихся в виде документов на машинном носителе (ст. 146 УК РФ);

г) незаконные изготовление в целях распространения или рекламирования, распространение, рекламирование порнографических материалов на машинных носителях, в системе или сети ЭВМ, а равно незаконная торговля ими (ст. 242 УК РФ).

д) изготовление и оборот материалов с порнографическими изображениями несовершеннолетних (ст. 242-1 УК РФ).

В сфере телекоммуникаций (ст. 138 УК РФ):

а) незаконное прослушивание телефонных переговоров и иных сообщений;

б) незаконный перехват и регистрация информации с технических каналов связи;

в) неправомерный контроль электронных почтовых сообщений и отправлений.

В сфере информационного оборудования:

а) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ);

б) незаконный оборот специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации (ч. 2 и 3 ст. 138 УК РФ);

в) незаконный оборот специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения (изменения, уничтожения) информации с технических средств ее создания, обработки, хранения и передачи (ч. 2 и 3 ст. 138 УК РФ);

г) незаконное изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт (ст. 187 УК РФ);

д) нарушение авторских прав в отношении топологий интегральных микросхем (ст. 146 УК РФ).

В сфере защиты охраняемой законом информации:

а) незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, в том числе персональных данных – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (ст. 137 УК РФ);

б) разглашение охраняемой законом информации: государственной тайны (ст. 276 УК РФ; ст. 283 УК РФ); служебной тайны и профессиональной тайны (ст. 155 УК РФ; ст. 310 УК РФ; ст. 311 УК РФ; 320 УК РФ);

в) незаконные собирание, разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ);

г) незаконные экспорт или передача иностранной организации или ее представителю научно-технической информации, которая может быть использована при создании вооружения и военной техники и в отношении которой установлен экспортный контроль (ст. 189 УК РФ).

В сфере информационных правоотношений:

а) распространение заведомо ложной информации (ст. 129 УК РФ; ст. 182 УК РФ);

б) неправомерный отказ в предоставлении или уклонение от предоставления информации (ст. 140 УК РФ; ст. 185.1 УК РФ; ст. 287 УК РФ);

в) сокрытие или искажение информации (ст. 237 УК РФ; ст. 198 УК РФ).

В сфере экономики и компьютерной информации:

а) мошенничество в сфере предоставления услуг электросвязи и доступа к информационным ресурсам сети «Интернет» (ст. 165 и 272 УК РФ, 159 и 272 УК РФ, ст. 200 УК РФ);

б) мошенничество в сфере электронного перевода денежных средств (ст. 159, 165, 187, 272 и 273 УК РФ);

в) незаконная деятельность в сфере предоставления услуг электросвязи и доступа к информационным ресурсам сети «Интернет» (ст. 171, 171.1, 173, 178);

г) иные преступления, совершенные в сфере экономики и компьютерной информации (ст. 169, 175, 186, 194, 198, 199 УК РФ).

Литература

1. Уголовный кодекс Российской Федерации. М., 2001.

2. Компьютерная преступность и борьба с нею. http://www.cyberpol.ru/

3. Виды нарушителей информационной безопасности. http://infosec.imi.sitc.ru/

4. Компьютерные преступления и их предупреждения. http://www.hackzona.ru/

ТЕХНОЛОГИЯ ОБХОДА АНТИВИРУСА

Г.В. Петрова, ассистент каф. КИБЭВС;
В.И. Ким, студент 4-го курса КИБЭВС
ТУСУР, г. Томск, pgv@keva.tusur.ru

Введение

За минувшие годы были обнаружены и предотвращены десятки тысяч вирусов, троянских коней, систем удаленного администрирования и прочих опасных объектов.

Могут ли вирусы противостоять антивирусам? Вопрос совсем не так прост, как кажется. С одной стороны, создать абсолютно недетектируемый вирус никому не удалось. И дело тут не столько в отсутствии свежих идей, а скорее в сложности их реализации. Разработка «неуловимого» вируса требует колоссальных усилий, высочайшей квалификации и профессионализма.

При условии, что вирус не обнаруживается при эвристическом поиске, до тех пор, пока он не попадет в базу данных антивируса, он может спокойно выполнять свою работу. Ну а если все-таки он попался, то существуют ведь и другие вирусы. Причем создавать новый вирус «с ну-

ля» совершенно необязательно. Возможно просто слегка изменить исходные тексты уже известной антивирусу программы (или, например, откомпилировать другим компилятором). Если же исходных текстов нет, можно заняться редактированием исполняемых файлов.

Теория

Подавляющее большинство антивирусов используют сигнатурный поиск с жесткой привязкой к точке входа или физическому смещению в файле. Что все это значит? Сигнатурой называется уникальная последовательность байт, однозначно идентифицирующая вирус. Сигнатура может быть как сплошной (например, DE AD BE EF) или разряженной (например, DE ?? ?? AD ?? BE ** EF, где знак ?? обозначает любой байт, а ** любое количество байт в данной позиции). Поиск по разряженной сигнатуре иначе называется поиском по маске и это – наиболее популярный алгоритм распознавания на сегодняшний день.

Для достижения приемлемой скорости сканирования антивирусы практически никогда не анализируют весь файл целиком, ограничиваясь беглой проверкой одной-двух ключевых точек (например, окрестностей точки входа в файл, т.е. тех ячеек, с которых и начинается его выполнение). Реже используется привязка к смещению сигнатуры относительно начала файла.

Полиморфные вирусы, не содержащие ни одной постоянной последовательности байт, сигнатурным поиском уже не обнаруживаются и для их детектирования приходится разрабатывать другие методики, самой известной из которых является эмуляция процессора (называемая также технологией виртуальной машины). Антивирус прогоняет подозреваемый файл через эмулятор, дожидается, пока полиморфный движок расшифрует основное тело вируса (если файл действительно зашифрован), после чего применяет сигнатурный поиск. Это достаточно ресурсоемкая операция и без особой нужды антивирусы к ней стараются не прибегать.

Подлинно полиморфные вирусы, каждый раз на 100% перестраивающие свое тело и обходящиеся без навесных шифровщиков, эмулятором уже не обнаруживаются, однако, во-первых, такие вирусы существуют только теоретически, а, во-вторых, для их детектирования заблаговременно разработана технология логической реконструкции алгоритма исследуемой программы (т.е. антивирус смотрит, что делает данная программа, игнорируя то, как именно она это делает).

Поскольку зараженный файл может быть упакован (и тогда вирусные сигнатуры окажутся искажены), антивирус должен быть готов его распаковать.

Практика

Первое, что возможно сделать – обработать файл каким-нибудь навесным упаковщиком/протектором, полностью уничтожающим все сигнатуры. Если антивирус все-таки этот файл обнаружил как вирус, значит, он успешно его распаковал.

Можно ли противостоять автоматическим распаковщикам? На первый взгляд, стоит лишь найти малоизвестный упаковщик... Но этот прием одноразовый. Как только выбранный упаковщик станет популярным, антивирусы тут же научатся его распаковывать!

Имеются ли другие приемы? Да, и, как минимум, целых три: *уничтожение сигнатур упаковщика, внедрение подложных сигнатур* и *дезактивация эмулятора.*

Если выбранный нами упаковщик не может быть распакован на виртуальной машине антивирусного эмулятора (универсальном распаковщике), антивирус пытается опознать упаковщик в «лицо», передавая бразды правления соответствующей процедуре распаковки, либо распаковывающей файл самостоятельно, либо инструктирующей эмулятор на предмет обхода антиотладочных приемов. Исказив сигнатуру упаковщика, мы предотвратим его опознание.

Как альтернативный вариант, можно не затирать сигнатуру оригинального упаковщика, а, напротив, набить файл подложными сигнатурами других упаковщиков. Ошибочное распознание упаковщика препятствует его распаковке.

Или же можно ударить в самое сердце антивируса – в его виртуальную машину. Преодолеть эмулятор можно различными путями:

а) вставить конструкцию, которую антивирус проэмулировать не в состоянии (самомодифицирующийся или самотрассирующийся код, обработку структурных исключений и т. д.);

б) команду, привязывающуюся к своему местоположению в памяти;

в) команду, не известную эмулятору.

Код, отвечающий одному или нескольким вышеприведенным пунктам, называется антиотладочным кодом. Будучи внедренным в упакованный файл, он способен убить антивирус еще до того, как распаковщик успеет получить управление. При этом простое пополнение сигнатурной базы положение не спасет и разработчикам придется всерьез засесть за совершенствование виртуальный машины, что не только дорого, но и хлопотно.

Литература

1. *Касперски К.* Компьютерные вирусы изнутри и снаружи. СПб.: Питер, 2006. 527 с.

МЕТОД ТЕСТИРОВАНИЯ МАТРИЦ БОЛЬШИХ РАЗМЕРОВ ,В СРЕДЕ MATLAB

В.В. Компанец, студент 3-го курса КИБЭВС
ТУСУР, КИБЭВС, г. Томск, memfis_tm@mail.ru

Тестирование программного обеспечения – процесс, позволяющий определить корректность, полноту и качество разработанного программного обеспечения (ПО). К сожалению, существующие на сегодняшний день методы тестирования ПО не позволяют однозначно и полностью установить корректность функционирования анализируемой программы [1].

При выполнении тестирования программного комплекса для группового проектного обучения требовалось проведения сравнение больших объемов данных, которые размещались в матрицах. При поиске решений были выделены три метода сравнений.

Первый метод состоит в том, чтобы проверять матрицы вручную. Данный метод не являлся рациональным, так как матрицы имели большие размеры и физически проверить их не представлялось возможным.

Второй метод состоит в том, чтобы по данным матрицам строить графики и проводить сравнение матриц при помощи графиков. Данный метод не является точным и при использовании данного метода можно проводить только грубое приблизительное сравнение.

Третий метод состоит в том, чтобы проверять матрицы при помощи компьютера. Так как программный комплекс разрабатывался в среде MATLAB, следовательно, было решено использовать данную среду для написания приложения для сравнения матриц.

В ходе работы было написано приложение, выполняющее статистическое сравнение матриц. В качестве первой матрицы бралась эталонная матрица, а в качестве второй – анализируемая матрица, полученная при помощи программного комплекса. Эталонная матрица рассчитывалась в системе MATHCAD, в которой есть возможность импорта данных в файл с расширением mat – основной формат данных в системе MATLAB [2].

В качестве параметров сравнения были выбраны следующие три параметра.

– Среднеквадратическая погрешность разности матриц.

– Средняя абсолютная погрешность разности матриц.

– Максимальная погрешность разности матриц.

В дополнение к этому производилось сравнивание максимального элемента каждой из матриц и их положение, что давало приблизительный анализ сравнения матриц.

Каждый параметр для более удобного восприятия представлялся в абсолютной и в процентной форме, а в случае максимальной погрешности указывалось еще и положение элемента в матрице разности.

Параметры сравнения анализировались, и в случае если максимальная погрешность в определении оказывалась меньше 1%, то вместо того чтобы искать ошибку в программе просто принималось, что алгоритм правильный. Это позволило значительно ускорить процесс тестирования и разработки.

На рисунке приведен пример работы программы. В качестве параметров на входе были использованы две матрицы размером 605x128, первая – эталонная матрица была импортирована из системы MathCAD, вторая – анализируемая матрица получена в системе MATLAB.

```
>> test(MathCAD,MATLAB)
Максимальный элемент эталонной матрицы: 0.00894812 в (303,1)
Максимальный элемент анализируемой матрицы: 0.00894812 в (303,1)
Среднеквадратическая погрешность: 2.40735e-009 или 2.69034e-005%
Средняя абсолютная погрешность: 8.89862e-018 или 9.94468e-014%
Максимальная погрешность: 7.52436e-017 или 8.40887e-013% или (243,24)
>>
```

Пример работы программы

Разработанное приложение используется для тестирования разрабатываемой в рамках проекта ГПО «Искусственный интеллект в задачах анализа и синтеза речи» системы. Оно представляет собой пример возможности использования нескольких вычислительных сред для получения результатов и их автоматического сравнения.

Литература

1. http://ru.wikipedia.org Википедия. Свободная энциклопедия. Статья-тестирование программного обеспечения.

2. *Потемкин В.Г.* MATLAB 6: среда проектирования инженерных приложений. М.: Диалог, 2003. 448 с.

СПОСОБ ВЫДЕЛЕНИЯ ФОРМАНТ ГЛАСНЫХ И СОНАНТ

Ю.И. Конькова, студентка 3-го курса каф. КИБЭВС

ТУСУР, skave@ms.tusur.ru

Для описания акустических характеристик звуков речи используются спектрограммы – амплитудно-частотный спектр, представляющий собой данные об относительной интенсивности частотных составляющих звука. Области высокой энергии называются формантами. Гласные

и сонанты имеют четкую формантную структуру, что может использоваться для их распознавания. [2]

Выделение формант в данном эксперименте проводилось в два этапа:

1) нахождение огибающей спектра путем кусочно-линейной интерполяции;

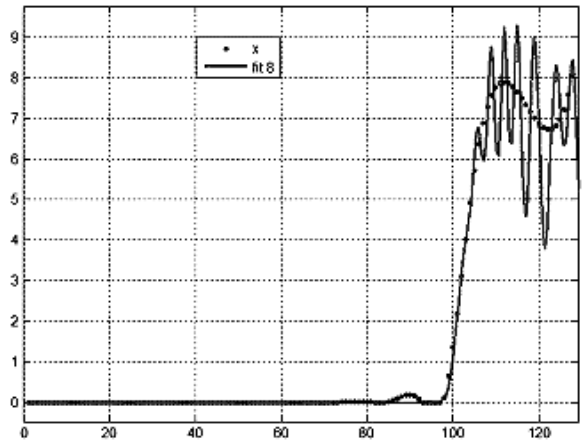
2) аппроксимация огибающей с помощью гауссоид.

Назначение второго этапа заключается в том, чтобы определить точное положение формант, а также выявить близко расположенные форманты, которые нельзя заметить на первом этапе. [1]

Эксперимент проводился при помощи среды MATLAB. Для аппроксимации огибающей спектра можно использовать инструмент Curve Fitting Tool.

Количество гауссоид было взято равным восьми. Затем среди восьми найденных частот были выбраны три частотных канала, для которых интенсивность наибольшая. Эти каналы упорядочиваются, и их частоты считаются первой, второй и третьей формантами. [1]

Следует отметить, что в среде MATLAB данный алгоритм работает не вполне успешно, что, вероятно, связано с особенностями реализации алгоритма аппроксимации. Например, на рисунке изображены огибающая мгновенного спектра чистой гласной *у* и его аппроксимация восемью гауссоидами. Вторая форманта, что хорошо заметно по огибающей, расположена около канала с номером 90. Но в результате аппроксимации данный участок спектра выравнивается и приближается к нулю. Зато появляется множество максимумов в области первой форманты и частоты основного тона.



Аппроксимация сглаженного мгновенного спектра гласной *у*

Таким образом, пользоваться имеющимся в среде MATLAB алгоритмом аппроксимации гауссоидами нельзя из-за потери важной информации. Дальнейшие попытки использовать данный способ для нахождения формант требуют собственной реализации алгоритма аппроксимации.

Литература

1. *Аграновский А.В., Леднов Д.А.* Теоретические аспекты алгоритмов обработки и классификации речевых сигналов. М.: Радио и связь, 2004.

2. *Бондарко Л.В.* Звуковой строй современного русского языка. М.: Просвещение, 1977.

ПРОБЛЕМА ПРИМЕНЕНИЯ ЭВОЛЮЦИОННОГО ПРОГРАММИРОВАНИЯ ДЛЯ ГЕНЕРАЦИИ СИГНАТУР ВРЕДОНОСНЫХ ПРОГРАММ

А.С. Конончук, студент 5-го курса КИБЭВС

ТУСУР, г. Томск, kononchuk@sibmail.com

Одной из важнейших проблем информационной безопасности является предупреждение реализации угроз. Особенно проблематичным является предупреждение угроз в электронно-вычислительных системах по причине их сложности и невозможности представления их в виде модели белого ящика.

Задачей научной работы является разработка метода, позволяющего автоматизировать оценку уровня безопасности и спрогнозировать наиболее вероятные реализации угроз, а также сгенерировать возможные методы их реализации.

Для реализации вышеуказанного метода необходимо применение методов искусственного интеллекта, так как только они предоставляют возможность прогнозирования. Среди всех методов был выбран метод эволюционного программирования, так как исключительно он предусматривает мутации особей на уровне фенотипа, а не генотипа в отличие от генетического программирования. Так как мутация на уровне генотипа лишь позволит выявить наиболее вероятные типы угроз, что не является первостепенной задачей, так как определение наиболее вероятных угроз можно спрогнозировать исходя из отношения сложности реализации этих угроз к размеру ущерба от реализации этих угроз. Таким образом, применение генетического программирование не даст требуемого результата, следовательно, эволюционное программирование – единственный метод, предоставляющий все требуемые возможности, для про-

гнозирования методов реализации угроз и оценки наиболее вероятных угроз.

Основной проблемой применения эволюционного программирования как метода генерации сигнатур вредоносных программ является проблема определения пространства решений для определения критерия оценки особей популяции. Как следствие из вышеуказанной проблемы вытекает проблематичность определения критерия останова, кроме как истечение времени.

Для решения описанной проблемы предлагается сузить спектр направлений применения данного метода до определенных угроз. Таким образом, будут выбраны те угрозы, которые позволяют оценить степень их реализации, и как следствие имеют дискретные состояния реализации. Наглядным примером можно представить DoS атаки на непосредственно сервер методом Ping of Death, который заключается в забивании канала жертвы нестандартными эхо пакетами, обработка достаточно большого числа, которых может вызвать отказ в обслуживании. Этот метод не имеет дискретных состояний реализации, т.е. невозможно оценить степень, насколько загружен сервер жертвы и насколько нужно увеличить нагрузку, чтобы вызвать отказ в обслуживании. Другим методом является атака на непосредственно сервисы жертва, с целью вызвать отказ в обслуживании не сервера в целом, а лишь некоторого его сервиса. Такие атаки наиболее трудно предотвратимы и прогнозируемы. А, следовательно, выявление именно их методов реализации является наиболее критичным, но методы эволюционного программирования работают именно с такими видами атак, так как, увеличивая нагрузку на ресурс, злоумышленник может проверять время отклика этого ресурса и с его увеличением делать выводы о том, что он действует в верном направлении, что позволяет также применять эти методы оценки для определения эффективности жизнедеятельности особи и, как следствие, определение степени соответствия целевой функции, что является необходимым условием реализации эволюционного программирования.

В ходе исследования были сделаны выводы, что метод, предоставляющий возможности, описанные в задаче исследований, может быть определен как метод эволюционного программирования. Однако следует отметить, что применение метода должно быть узко направленно на определенный вид угроз, и для получения максимально полной картины уровня безопасности электронно-вычислительной системы, метод должен применяться многократно, для каждого конкретного вида угроз индивидуально, что позволит, имея оценку возможного материального ущерба от реализации исследуемых видов угроз, сделать вывод о наиболее вероятных.

Литература

1. *Курейчик В.М., Родзин С.И.* Эволюционные алгоритмы: генетическое программирование. Обзор // Изв. РАН. ТиСУ. 2002. №1. С. 127–137..

2. *Родзин С.И.* Гибридные интеллектуальные системы на основе алгоритмов эволюционного программирования // Новости искусственного интеллекта. 2000. №3. С. 159–170.

3. *Родзин С.И.* Параллельные нейроэволюционные вычисления // Изв. НАН Украины. Искусственный интеллект. Донецк: Наука і освіта, 2003. №4. С. 485–492.

СИСТЕМА ИССЛЕДОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ

В.В. Компанец, Ю.И. Конькова, С.Д. Тиунов, Е.Ф. Щипунов – студенты 3-го курса КИБЭВС, Е.Ю. Костюченко, аспирант каф. КИБЭВС;
ТУСУР, г. Томск, key@keva.tusur.ru

Актуальность проблемы анализа речи неоспорима. Преодоление данной проблемы позволит решить ряд важных практических задач, в числе которых следующие:

– бесклавиатурный ввод;

– идентификация диктора;

– поиск ключевых слов в слитной речи;

– простая и эффективная диагностика заболеваний, связанных с изменением речеобразующего тракта (например, рак гортани);

– другие задачи, связанные с анализом речи.

Перед разработчиками была поставлена задача создать исследовательский программный комплекс, предоставляющий пользователям следующие возможности:

– обработка сигнала при помощи системы не рекурсивных фильтров, учитывающих особенности слуховой системы человека, описанных в [1];

– выделение из спектра различных параметров, которые могут быть использованы при анализе речевого сигнала;

– ведение базы данных самих сигналов и параметров, выделенных из этих сигналов;

– представление параметров в виде, удобном для дальнейшей обработки с применением нейронных сетей.

Анализ структуры речевого сигнала носит иерархический характер: сперва определяется наличие речевого сигнала в звуковом, далее осуществляется анализ на уровне звуков (фонем). Потом осуществляется их группировка (анализ на уровне групп фонем), следующие идут уровни

слов, словосочетаний, предложений и т. д. Верхние уровни анализа речи нами пока не рассматриваются по причине их некритичности для решения поставленных задач (например, для задачи диагностики заболеваний, связанных с изменением речеобразующего тракта будет практически бесполезен анализ на уровне предложений по причине того, что изменения наиболее ярко выражаются как раз на нижних уровнях).

На рисунке представлен иерархический анализ структуры речевого сигнала с указанием возможности применения нейронных сетей на некоторых уровнях (при этом не утверждается невозможность применения нейронных сетей на других уровнях).

Иерархический анализ речевого сигнала с применением нейронных сетей

Для разработки данной системы была выбрана среда MATLAB. Данный выбор обусловлен следующими соображениями:

– среда MATLAB представляет собой мощное средство для моделирования и решения различных математических задач;

– среда предлагает разработчику множество уже готовых функций, особый интерес для данного проекта представляют наборы для работы с нейронными сетями, набор статистической обработки данных, набор для обработки сигналов. Нет нужды писать свои функции для решения рутинных задач, не представляющих интереса для исследования. В случае, если предложенный набор не удовлетворяет разработчика, он всегда может быть изменен/дополнен в соответствии с потребностями;

– среда MATLAB позволяет создавать готовые приложения с применением стандартных визуальных компонент ОС Windows.

Данный программный комплекс может представлять интерес как средство исследования речевых сигналов, выбора набора обучающих параметров для нейронной сети, средством ведения базы данных, так и как средство для создания готовых приложений с использованием реализованных в нем функций.

Литература

1. *Bondarenko V.P., Kornilov A.U., Choynzonov E.C., Balackaya L.N.* The automatized rehabilitation of oncological patients with larynx cut out // Proceedings 'SPECOM'2005': 10-th International Conference Speech & Computer. Patras, 2005. P. 707–711.

ВЫБОР ОБУЧАЮЩЕГО НАБОРА КЛЮЧЕВЫХ ПАРАМЕТРОВ РЕЧЕВОГО СИГНАЛА

Е.Ю. Костюченко, аспирант каф. КИБЭВС
ТУСУР, г. Томск, key@keva.tusur.ru

Процедуры выделения параметров речевого сигнала как правило являются довольно трудоемкими. Также трудоемкими являются и процедуры обучения нейронных сетей. Эти факты являются весомыми с учетом того, что для решения некоторых задач анализа речи (например, бесклавиатурный ввод) необходим анализ сигналов в реальном времени. Исходя из этого важным шагом является выбор обучающего набора ключевых параметров речевого сигнала, значения которых будут подаваться на входы нейронной сети при обучении и анализе.

Можно сформулировать следующие требования к параметрам, используемым при анализе:

– параметры должны быть по возможности менее зависимы друг от друга. Так, использование параметров, между которыми существует линейная корреляция, не приносит дополнительной информации при обучении нейронной сети;

– размерность итогового обучающего вектора примера не должна быть слишком большой. Понятно, что можно набрать десятки тысяч различных значений параметров, однако трудоемкость обучения будет крайне велика. Кроме того, растет использование вычислительных мощностей компьютера, что затрудняет приближение к режиму реального времени;

– размерность итогового обучающего вектора примера не должна быть слишком мала. В представленных параметрах для обучения должно быть достаточно информации для последующего анализа сигналов и их классификации;

– размер окна анализа должен соответствовать признаку, который мы пытаемся выделить. Проблематично по одному временному отсчету говорить о наличии вокализации, но вряд ли имеет смысл использовать для этой цели окно в 1 с. Параметр и окно анализа должны соответствовать друг другу.

Исходя из данных требований был проведен анализ ряда параметров речевого сигнала на предмет применимости для обучения нейронной сети на примере задачи определения наличия вокализации на исследуемом участке. Условия эксперимента были следующие:

1) частота дискретизации сигнала 12 кГц;

2) 128 каналов анализа;

3) размер окна выбран исходя из минимальной продолжительности вокализованного участка для речевого сигнала [5] 360 отсчетов, что соответствует 30 мс;

4) исследуемые параметры: результаты одновременной маскировки [2] на первом отсчете окна, номер канала с максимальной интенсивностью на отсчете, среднее значение интенсивности на отсчете, дисперсия интенсивности на отсчете, вариация интенсивности на отсчете, коэффициент асимметрии интенсивности на отсчете, медиана интенсивности на отсчете и отношение медианы интенсивности к среднему значению на отсчете;

5) после составления обучающий выборки на основе наблюдаемого диапазона изменения параметров диапазон приводился к [-1; 1];

6) объем обучающей выборки 200 примеров;

7) для обучения использовался персептрон с количеством нейронов в промежуточном слое равным 50.

Для исследования параметров на степень зависимости была рассчитана матрица коэффициентов корреляции. Примеры полученных значений коэффициентов для одного окна анализа представлены на рис. 1. Значения самих анализируемых параметров представлены на рис. 2.

	Среднее	Вариация	Дисперсия	Асимметрия	Медиана/Ср.	Медиана	Макс. канал
Среднее	1	0.6005	0.9786	0.6309	-0.1856	-0.0495	-0.4419
Вариация	0.6005	1	0.7516	0.9734	-0.8169	-0.7523	-0.3746
Дисперсия	0.9786	0.7516	1	0.7679	-0.358	-0.2308	-0.4656
Асимметрия	0.6309	0.9734	0.7679	1	-0.8038	-0.7213	-0.3694
Медиана/Ср.	-0.1856	-0.8169	-0.358	-0.8038	1	0.9853	0.301
Медиана	-0.0495	-0.7523	-0.2308	-0.7213	0.9853	1	0.2875
Макс. канал	-0.4419	-0.3746	-0.4656	-0.3694	0.301	0.2875	1

Рис. 1. Значения коэффициентов корреляции между параметрами

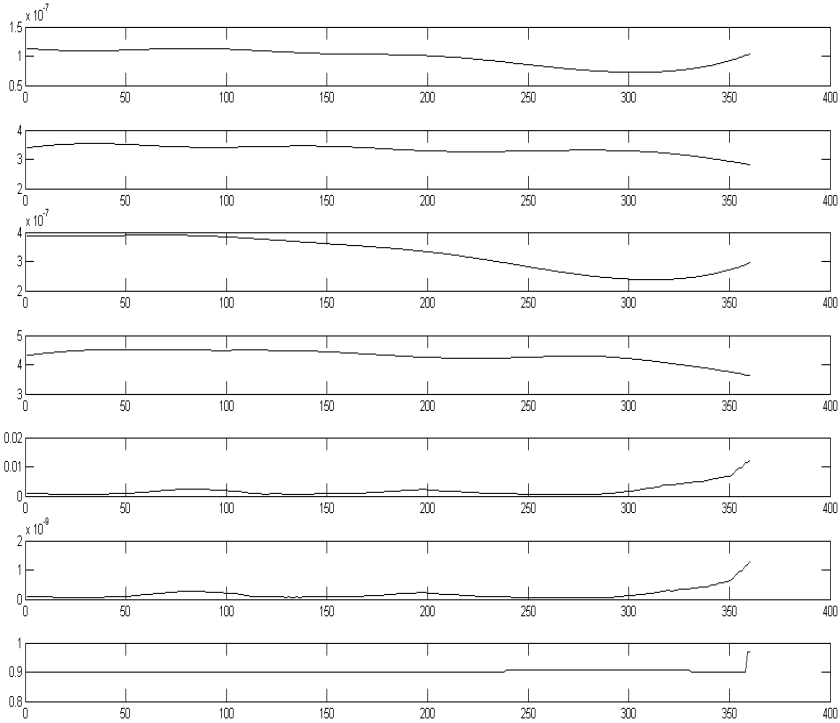


Рис. 2. Значения коэффициентов корреляции между параметрами

Задав пороговое значение модуля коэффициента корреляции 0,8 получим следующий набор параметров: результаты одновременной маскировки на первом отсчете окна (не анализировались, поскольку имеют другую размерность и отражают зависимость по частоте, а не по времени, как остальные параметры), номер канала с максимальной интенсивностью на отсчете, среднее значение интенсивности на отсчете, вариация интенсивности на отсчете и медиана интенсивности на отсчете.

Выбранные 5 параметров определяют количество нейронов во входном слое нейронной сети, равное 128 + 360*4 = 1568. Предельная размерность обучающего вектора на практике составляет около 1300 входов. При 1568 входах достигнуть итогового уровня ошибки менее 0,01 не представляется возможным. Исходя из этих соображений, необходимо отбросить параметр с наибольшей корреляцией – медиану.

В результате исследований определен набор входных параметров: результаты одновременной маскировки на первом отсчете, номер канала

с максимальной интенсивностью на отсчете, среднее значение интенсивности на отсчете, вариация интенсивности на отсчете. Обучение на предложенных параметрах не вызывает затруднений (не зафиксировано нейронных сетей, обучение которых невозможно), коэффициент корреляции между предложенными параметрами не критичен.

Литература

1. *Алдошина И.А.* Основы психоакустики. Ч. 1 // Звукорежиссер. 1999. № 6.

2. *Конев А.А., Тихонова В.И.* Выделение вокализованных звуков в слитной речи. Сб. трудов XVI сессии Российского акустического общества. М.: ГЕОС, 2005. Т. 3. С. 47–50.

ЗАЩИТА ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ УТЕЧКИ ИНФОРМАЦИИ

М.С. Ковалевский, студент 5-го курса КИБЭВС

ТУСУР, г. Томск, sedkemcity@rambler.ru

При выявлении технических каналов утечки информации средств приема, обработки, хранения и передачи информации (ТСПИ) необходимо рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата техническими средствами разведки (ТСР) технические каналы утечки можно разделить на следующие:

1. Технические каналы утечки информации, обрабатываемой ТСПИ.
1.1. Электромагнитные каналы утечки информации.
1.2. Электрические каналы утечки информации.
1.3. Параметрический канал утечки информации.
1.4. Вибрационные технические каналы утечки информации.
2. Каналы утечки информации при ее передаче по каналам связи.
2.1. Электромагнитные каналы.
2.2. Электрические каналы.
2.3. Индукционный канал.
3. Каналы утечки речевой информации.
3.1. Акустические каналы.
3.2. Виброакустические каналы.

3.3. Параметрические каналы.

3.4. Акустоэлектрические технические каналы утечки информации.

3.5. Оптико-электронный технический канал утечки информации.

4. Технические каналы утечки видовой информации.

4.1. Наблюдение за объектами.

4.2. Съемка объектов.

4.3. Съемка документов.

Организация защиты выделенного помещения от утечки информации по техническим каналам включает в себя:

– Общие положения. К защищаемой информации относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

– Подготовительный этап создания системы технической защиты информации. На этом этапе осуществляется подготовка к созданию системы технической защиты информации на защищаемых объектах, в процессе которой проводится специальное обследование защищаемых объектов, разрабатывается аналитическое обоснование необходимости создания СТЗИ и техническое (частное техническое) задание на ее создание.

– Стадия проектирования системы технической защиты информации. Для разработки технического проекта на создание системы технической защиты информации должны привлекаться организации, имеющие лицензию ФСТЭК РФ; Технический проект, рабочие чертежи, смета и другая проектная документация должны быть учтены в установленном порядке.

– Ввод в эксплуатацию системы технической защиты информации. На этом этапе силами монтажных и строительных организаций осуществляется выполнение мероприятий по защите информации, предусмотренных техническим проектом.

Оценка эффективности защиты информации от утечки по техническим каналам включает в себя контроль эффективности и критерий эффективности защиты информации.

Контроль эффективности защиты информации – измерение для получения информации о соответствии эффективности и рациональности защиты информации установленным требованиям или нормам. Контроль эффективности защиты информации основан на научной и законодательной метрологии. Научная метрология устанавливает единые правила передачи единицы физической величины от государственного эталона к рабочим средствам измерений. Условия измерений законодательно за-

креплены для основной и дополнительной инструментальной погрешности средства измерения.

Критерий эффективности защиты информации. Проектирование защищенных от утечки информации сложных информационных систем сопряжено с непредвиденными трудностями. Во-первых, на начальных этапах невозможно оценить характеристики паразитных каналов утечки информации. Во-вторых, их основные каналы утечки информации оценивают с помощью сигналов в шумах. В-третьих, моделирование, как метод исследования сложной информационной системы, приближенно отображает характеристики каналов утечки информации. В процессе моделирования канала утечки информации и его элементов необходимо ввести частные и обобщенные показатели.

Критерий качества защиты информации (при достоверном обнаружении автоматизированной системой контроля хотя бы одного канала утечки):

$$K_{\Sigma \text{АСК}} = \frac{R_{\max i} - R_{\text{задан}\, i}}{R_{\max i} - R_{\min i}} \alpha_i \beta_i \delta [\prod_{i=1}^{n} p_i + p_{\text{a}} (1 - \prod_{i=1}^{n} p_i)] =$$

$$= \frac{R_{\max i} - R_{\text{задан}\, i}}{R_{\max i} - R_{\min i}} \alpha_i \beta_i \delta [(p_a + \prod_{i=1}^{n} p_i) - p_a \prod_{i=1}^{n} p_i] e^{-\frac{|\Delta - \tilde{\Delta}|}{\Delta}} \to \max,$$

где $\Delta_{\text{п}} = e^{-\frac{|\Delta - \tilde{\Delta}|}{\Delta}}$ – показатель точности оценки параметров, определяющих канал утечки информации; Δ – истинное значение измеряемого параметра; $\tilde{\Delta}$ – результат n-го измерения, для которого $|\Delta - \tilde{\Delta}| = \max$; $R_{\max i}$ – максимальный радиус области, ограничивающей информационное пространство по i-му каналу утечки, без принятых мер защиты информации; $R_{\min i}$ – минимально достижимый радиус области, ограничивающей информационное пространство по i-му каналу утечки, после реализации мер защиты информации; $R_{\text{задан}\, i}$ – заданный технической документацией для объекта защиты радиус области, ограничивающей заданное информационное пространство по i-му каналу утечки; β_i – вес по информативности i-го канала утечки; p_i – вероятность невозникновения i-го канала утечки после мероприятий по защиты информации;

Критерий качества защиты информации должен включать научно-технические, информационные и экономические показатели. Задачу формирования критерия качества защиты информации целесообразно решать с помощью моделирования.

Литература

1. *Зайцев А.П., Шелупанов А.А.* Технические средства и методы защиты информации. Ч. 1. Учеб. пособие. Томск: Изд-во Том. гос. ун-та систем управления и радиоэлектроники, 2005.

2. *Железняк В.К.* Защита информации от утечки по техническим каналам: Учебное пособие ГУАП. СПб., 2006. 188 с.

3. Противодействие экономическому шпионажу: Сб. публикаций журнала «Защита информации. Конфидент» 1994–2000. СПб.: Конфидент, 2000, 344 с.

4. *Хорев А.А.* Способы и средства защиты информации: Учеб. пособие. М.: МО РФ, 2000, 316 с.

КРИПТОСИСТЕМА НА ОСНОВЕ КЛЕТОЧНОГО АВТОМАТА НА РАЗБИЕНИИ «KLAV-ST»

С.Л. Крыловский, студент 5-го курса КИБЭВС

ТУСУР, г. Томск, klav-st@mail.ru

Главной задачей является разработка криптосистемы на основе клеточного автомата для защиты информации на ПЭВМ от НСД, исключить доступ посторонних лиц к информации и обеспечить доступ разрешенным пользователям при предъявлении ими специального ключа преобразования.

Криптосистема предназначена для применения в организациях или иных областях, где необходима криптографическая защита информации в качестве доступного программного средства для надежного зашифровывания и расшифровывания указанных исходных файлов с использованием ключевых данных. Разработка криптосистемы предполагает разработку алгоритма шифрования на основе клеточного автомата, в частности алгоритма, заключающего информацию в пространство для дальнейшего ее шифрования, и обеспечивающего надежную криптостойкость при последующем криптоанализе получившегося после шифрования файла.

Алгоритм «KLAV-ST» состоит из нескольких уровней. На самом верхнем находятся практические алгоритмы, предназначенные для шифрования массивов данных. Все они опираются на два алгоритма низшего уровня, называемые циклами. Эти фундаментальные алгоритмы упоминаются как базовые циклы, чтобы отличать их от всех прочих циклов:

а) цикл зашифрования (Заш);

б) цикл расшифрования (Расш);

В свою очередь, каждый из базовых циклов представляет собой многократное повторение одной единственной процедуры, называемой для определенности далее основным шагом криптопреобразования.

В «KLAV-ST» ключевая информация состоит из двух структур данных. Помимо собственно ключа, необходимого для всех шифров, она содержит еще и таблицу замен. Ниже приведены основные характеристики ключевых данных «KLAV-ST».

а) Ключ является массивом от 1 до 32-х 1-байтных элементов кода, далее в настоящей работе он обозначается символом К: $К = \{К_i\}_{0 \le i \le 32}$. В «KLAV-ST» элементы ключа используются как символы: $0 \le К_i < 255^{32}$. Таким образом, максимальный размер ключа составляет 32·8 = 256 бит или 32 байта.

Таблица замен является матрицей 8×256, содержащей битовые элементы, которые можно представить в виде целых чисел от 0 до 15. Строки таблицы замен называются узлами замен, они должны содержать различные значения, то есть каждый узел замен должен содержать 16 различных чисел от 0 до 15 в произвольном порядке. Таблица замен обозначается символом H:

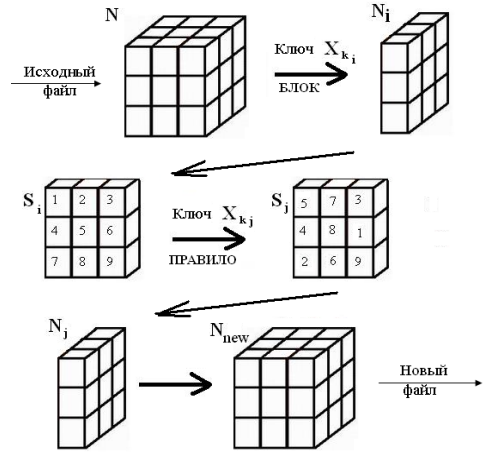
$H = \{H_{i,j}\}_{0 \le j \le 255}^{0 \le i \le 7}$, $0 \le H_{i,j} \le 15$. Таким образом, общий объем таблицы замен равен: 8 элементов × 256 узлов × 1 бита = 2048 бит или 256 байта.

На рисунке приведена обобщенная модель криптосистемы KLAV-ST, в соответствии с которой работает система.

Ключом в данной системе является массив символов, который определяет, к какой грани и какое правило необходимо применить.

При зашифровании выбирается исходный файл и указывается ключ. Получившийся новый файл сохраняется в том же каталоге и имя файла изменяется. К имени исходного файла добавляется слово «crypt», а расширение остается прежним.

При расшифровании алгоритм производит обратные действия.



Обобщенная модель криптосистемы KLAV-ST

В результате была разработана криптосистема «Klav-ST» на языке C++, реализующая алгоритмы зашифрования и расшифрования файла. Программа работает со всеми видами файлов. В основе алгоритма шифрования лежит клеточный автомат на разбиении в окрестности «Кубика Рубика».

Литература

1. *Архангельский А.* C++ Builder 6: Справочное пособие. М.: Бином, 2002.

2. *Страуструп Б.* Язык программирования C++: Спец. издание. М.: Бином, 2002.

3. *Тоффоли Т., Марголус Н.* Машины клеточных автоматов. М.: Мир, 1991.

АТТЕСТАЦИЯ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

А.И. Кривенчук, студент 5-го курса КИБЭВС

ТУСУР, г. Томск, krivenchuk@sibmail.com

Целями статьи являются рассмотрение и анализ методики аттестации объектов информатизации и исследование вариантов используемого оборудования для проведения аттестационных испытаний.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» – подтверждается, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации.

Порядок проведения аттестации объектов информатизации на соответствие требованиям безопасности информации включает следующие действия:

1) подачу заявки на рассмотрение и проведение аттестации;

2) анализ исходных данных по аттестуемому объекту информатизации;

3) проведение предварительного специального обследования аттестуемого объекта информатизации;

4) разработку программы и методики аттестационных испытаний;

5) заключение договоров на аттестацию;

6) испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);

7) проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации;

8) проведение аттестационных испытаний объекта информатизации;

9) оформление, регистрацию и выдачу «Аттестата соответствия»;

10) осуществление государственного контроля и надзора, инспекционного контроля над проведением аттестации и эксплуатацией аттестованных объектов информатизации;

11) рассмотрение апелляций.

Для проведения аттестационных испытаний при аттестации объектов информатизации необходимо специализированное оборудование.

В данной статье рассмотрим следующие виды оборудования:

1. Программно-аппаратный комплекс «Навигатор».

Программно-аппаратный комплекс «Навигатор» предназначен для автоматического, автоматизированного и экспертного поиска сигналов ПЭМИН от проверяемых технических средств, измерения частоты и пикового значения амплитуды найденных сигналов, хранения, обработки и представления результатов поиска и измерений в удобном для оператора виде, и применяется на объектах сферы обороны и безопасности.

2. Программно-аппаратный комплекс «Зонд».

В качестве вспомогательного оборудования для учета реального затухания электромагнитного поля при проведении аттестационных испытаний объектов информатизации предлагается комплекс «Зонд», предназначенный для решения широкого круга задач в комплекте с программно-аппаратными комплексами «Навигатор-Пх» и другим измерительным оборудованием.

3. Программно-аппаратный комплекс «Спрут-7».

Программно-аппаратный комплекс «Спрут-7» предназначен для проведения акустических и виброакустических измерений, для проверки выполнения норм эффективности защиты речевой информации от ее утечки по акустическому и виброакустическому каналам, а также утечки за счет низкочастотных наводок на токопроводящие элементы ограждающих конструкций зданий и сооружений и наводок от технических средств в речевом диапазоне частот, образованных за счет акустоэлектрических преобразований.

Вывод. В рамках статьи была рассмотрена методика проведения аттестации на объекте информатизации, а также рассмотрены варианты оборудования для проведения аттестационных испытаний на примере комплексов «Навигатор», «Зонд» и «Спрут-7».

Литература

1. *Бузов Г.А., Калинин С.В., Кондратьев А.В.* Защита от утечки информации по техническим каналам: Учеб. пособие. М.: Горячая линия – Телеком, 2005. 416 с.

2. Положение по аттестации объектов информатизации по требованиям безопасности информации. (Утверждено Председателем Гостехкомиссии России 25.11.1994). М.: Гостехкомиссия РФ, 1994. 22 с.

3. *Хорев А.А.* Защита информации от утечки по техническим каналам. Ч. 1. Технические каналы утечки информации. Учеб. пособие. М.: Гостехкомиссия России, 1998. 320 с.

4. Холдинг предприятий безопасности. www.nelk.ru

5. *Мотуз О.В.* «Побочные электромагнитные излучения: моменты истории». Защита информации. Конфидент. 2001. № 1. С. 86–89.

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕРВЕРА

А.Р. Курманалиев, М.М. Шуста, студенты 5-го курса КИБЭВС

ТУСУР, г. Томск, ar_kurm@ms.tusur.ru

Данная статья направлена на краткое ознакомление с основными принципами информационной защиты сервера предприятия.

Защита информации в процессе хранения

Современные корпорации сталкиваются с бурным ростом объемов данных, необходимых для их повседневной работы. Этот рост вызван потребностью иметь «на кончиках пальцев» финансовую, маркетинговую, техническую, статистическую и другую информацию для оперативного реагирования на изменения рыночной ситуации, поведение конкурентов и клиентов.

С другой стороны, высокая степень централизации корпоративной информации делает ее особенно уязвимой и увеличивает риск утечки [3].

Информация в корпоративных сетях хранится на жестких дисках; попадание этих носителей в руки злоумышленника создает наиболее серьезную угрозу информационной безопасности и может привести к тяжелым последствиям.

Для защиты информации в процессе хранения применяются в основном комплексы шифрования (например Secret Disk Server [3]) и резервирование.

Защита информации от внутренних угроз

Важнейшей проблемой, стоящей перед руководством и службой безопасности предприятия, является проблема лояльности сотрудников, или, иными словами, проблема внутренних угроз информационной безопасности.

По различным оценкам, от 50 до 80% атак, направленных на получение информации ограниченного доступа, начинается из локальной сети предприятия (интрасети) [2].

Особенную актуальность проблема внутренних угроз получила в связи с появлением и повсеместным распространением мобильных накопителей информации, подключаемых через USB порты – таких как flash-диски, винчестеры с USB-интерфейсом и т.д.

Если службой безопасности не предпринимаются специальные меры, нелояльно настроенный сотрудник компании может практически незаметно пронести на территорию предприятия компактный носитель большого объема и скопировать на него всю интересующую его информацию.

В данном случае применяются системы блокирования портов персонального компьютера, к которым могут подключаться внешние устройства.

Подключаемые устройства могут идентифицироваться по любым признакам, таким как класс устройства, код производителя, код устройства, серийный номер и т.д.

Таким образом, система может запретить использование внешних накопителей информации и разрешить подключение каких-либо других внешних устройств, например USB-ключей для аутентификации пользователей. [2]

Аутентификация пользователей

Как правило, информационная инфраструктура современных предприятий гетерогенна. Это означает, что в одной сети совместно существуют серверы под управлением разных операционных систем и большое количество прикладных программ. В зависимости от рода деятельности предприятия это могут быть приложения электронной почты и групповой работы (GroupWare), CRM- и ERP-системы, системы электронного документооборота, финансового и бухгалтерского учета и т.д. [2].

Количество паролей, которые необходимо помнить обычному пользователю, может достигать 5–6. Пользователи пишут пароли на бумажках и приклеивают на видных местах, сводя тем самым на нет все усилия по защите информации, либо постоянно путают и забывают пароли, вызывая повышенную нагрузку на службу поддержки [1].

Оптимальное решение проблемы – специальное программное обеспечение, позволяющее хранить пароли в защищенной памяти электронных идентификаторов и в нужный момент извлекать их и предоставлять соответствующим системным или прикладным компонентам.

В качестве электронных идентификаторов могут использоваться USB-брелки или смарт-карты, что позволяет контролировать их обращение и организовать строгий учет, в отличие от паролей, для которых это невозможно в принципе [2].

Литература

1. Интернет энциклопедия. http://www.wikipedia.org
2. Информационная безопасность корпоративных серверных платформ. http://www.securit.ru
3. Информационная безопасность бизнеса. http://www.infosecurity.ru

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ

Е.О. Макейчев, студент 5-го курса кафедры КИБЭВС

ТУСУР, г. Томск, makey@sibmail.com

В настоящее время все больше и больше людей осознают важность безопасности информации. Врач, бизнесмен, бухгалтер или юрист – у всех есть свои секреты, которые ни под каким предлогом они не желают раскрывать. Тем более если дело касается предприятий – компании предпочитают скрывать и тщательно охранять корпоративные секреты, разработки и другие конфиденциальные материалы. Иногда эту информацию необходимо предоставлять доверенным лицам, кому доступ к конфиденциальной информации разрешен «хозяином».

Очень важно правильно подойти к решению вопросов информационной безопасности, грамотно выбрать консультантов по безопасности, поставщиков систем защиты, чтобы не выкидывать «на ветер» средства и, самое важное, утраченную информацию, которую требовалось защитить.

Существует такое понятие, как отношение цена/качество, т.е. человек (организация) должен понимать, информацию какой стоимости какой ценой он собирается защищать. Нелогично, если финансовые документы приблизительной стоимости $X защищались системой за $X+X, но можно отметить, что иностранные компании вкладывают до 20% своих средств в информационную безопасность своего предприятия.

Каналы утечки информации

После того как финансовый документ в филиале крупной компании появился на свет, его необходимо отправить электронной почтой в головной офис на подпись руководителю. Типичная ситуация, но вот чем она грозит при неумелой политике информационной безопасности:

- Документ создан, и счастливый сотрудник, после долгой работы над ним отошел на обед. В это время злоумышленник осуществил несанкционированный доступ к персональному компьютеру сотрудника и подменил или уничтожил документ.
- Документ создан, сотрудник положил его в папку на файловом сервере корпоративной сети и пошел домой. В это время его конкурент по карьерной лестнице или недоброжелатель, добравшись до сервера, подменил или уничтожил документ.

• Документ создан, сотрудник положил его в папку на файловом сервере корпоративной сети. Произошла атака на корпоративную сеть компании со стороны сети Интернет, и все базы данных и другие материалы уничтожены.

• Документ создан и отправлен по электронной почте или отправлен на ftp-сервер в головной офис. При передаче документа произошел его перехват и подмена.

• Документ создан, переписан на дискету и отправлен с курьером в головной офис. Курьер за день очень устал и забыл папку с дискетой в метро.

• Документ создан, обработан и содержится где-то на диске какого-то компьютера. Компьютер списывается и новый владелец находит в скрытых файлах годовой финансовый отчет. Обрадованный, он его продает конкуренту.

• По сети или через обмен дискетами компьютер сотрудника или сервер сети был заражен вирусом, что повлекло за собой уничтожение баз данных и другой важной информации.

В любом из этих случаев компания терпит финансовые убытки и, если информация о происшествии выходит за пределы компании, теряет свою репутацию на рынке.

Типичные способы ликвидации основных каналов утечки информации

Персональный компьютер

Есть несколько методов защиты информации на персональном компьютере или рабочей станции сети. Основной из них – шифрование с достаточной длиной ключа. Применяя персональное шифрование, можно быть полностью уверенным в сохранности информации. Существует множество реализаций этого способа: от бесплатной программы PGP до системы защиты информации Secret Disk, использующей для хранения паролей электронные ключи. Зашифрованную информацию можно передавать любыми способами (и по электронной почте, и с курьером), так как злоумышленник, каким-либо способом получив зашифрованный файл, ничего не сможет с ним сделать. Подмена также исключена.

Существуют и системы защиты, блокирующие загрузку компьютера до предъявления электронного идентификатора.

Не стоит забывать и об антивирусной защите персональных ресурсов. В этом отлично зарекомендовал себя антивирусный комплекс «Kaspersky Antivirus» Лаборатории Касперского, ранее известный как «Антивирус Касперского».

Корпоративная сеть

В настоящее время уже многие компании владеют доступом в Интернет, пользуются электронной почтой. Соответственно, появляется вопрос о защите внутренних корпоративных сетевых ресурсов, защите файловых, почтовых и web-серверов и безотказной их работе, ограничении и разделении полномочий сотрудников, работающих с сетью Интернет. Как правило, организации используют для этого так называемые межсетевые экраны.

Проблема – защита каналов передачи данных между головным офисом и филиалами компании. Так как данные передаются через открытые сети (например, Интернет), то это вынуждает полностью «закрывать» канал. Для этого используются VPN (Virtual Private Network), т.е. виртуальные частные сети. Сейчас к этой аббревиатуре добавилась буква S (SVPN – Secure Virtual Private Network), т.е. защищенная виртуальная частная сеть. VPN организует шифрованный канал точка–точка или точка – многоточка между офисами, филиалами или удаленными сотрудниками компании.

Среди всего разнообразия межсетевых экранов особенно выделяется продукция компании Check Point Software Technologies – мирового лидера по производству систем сетевой защиты. Компания вошла в рейтинг NASDAQ и в этом году выпустила новый продукт Next Generation, который пришел на смену выдающемуся МЭ Check Point Firewall-1/VPN-1.

Для защиты информации на корпоративных серверах также используется шифрование и применяется антивирусная защита.

Сети питания и другие каналы

Существует вероятность снятия информации и другими, более изощренными способами, например по сетям электропитания, по электромагнитным и виброакустическим излучениям.

Для предотвращения таких случаев обычно используют помехоподавляющие фильтры или проводят серию мероприятий, направленных на невозможность использования технических средств снятия информации.

Уничтожение информации

Некоторые организации или частные лица не доверяют обычному стиранию информации, отслужившей свой срок, форматированию носителей. Также у некоторых компаний есть желание иметь систему, которая срочно, за доли секунды, сможет гарантировано уничтожить носитель на магнитных дисках (жесткий диск, дискета, zip, стримерная кассета). Причем как работающий, так и хранящийся в сейфе.

В такой ситуации оправданным будет использование уничтожителей информации на магнитных носителях и специальные информацион-

ные сейфы с источником бесперебойного питания, в которых, например, жесткий диск может работать и, при необходимости, его можно безвозвратно уничтожить.

Комплексный подход

Как Вы могли заметить, проблема обеспечения информационной безопасности становится проблемой, на которую трудно закрыть глаза, и которая быстро не решается. Требуются комплексный и всесторонний подход, точный анализ и обширная исследовательская работа по проектированию комплекса мер защиты корпоративной информации.

В настоящее время существуют компании, предоставляющие такие вида услуги. Необходимо отметить, что компания, в которую вы обратитесь по вопросами безопасности информации, обязана иметь большой опыт работы в этой сфере, а ее специалисты должны грамотно управлять базой знаний в этой области и точно определять потребности клиента.

После определенного времени работы такая компания предоставит Вам технико-экономическое решение, отвечающее вашим требованиям и пожеланиям по безопасности, ориентированное исключительно на вашу компанию.

Так что, если вы считаете, что ваша информация представляет ценность, то настало время задуматься о ее безопасности.

Литература

1. *Вихорев С.В., Кобцев Р.Ю.* Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Защита информации. Конфидент. 2002. № 2. С. 44–49.

2. *Зегжда Д.П., Ивашко А.М.* Основы безопасности информационных систем. М.: Горячая линия – Телеком, 2000. С. 18.

3. *Малюк А.А., Пазизин С.В., Погожин Н.С.* Введение в защиту информации. Учеб. пособие. для вузов. 2-е изд.

СИСТЕМА АВТОРИЗАЦИИ ЧЕЛОВЕКА НА ОСНОВЕ РАСПОЗНАВАНИЯ ОБРАЗОВ.

Я.С. Малышкин, студент 5-го курса каф. КИБЭВС

ТУСУР, г. Томск, imnobody@sibmail.com.

Авторизация – это процесс распознавания и проверки подлинности. Обычно она используется при принятии решения, можно ли разрешить доступ к системным ресурсам пользователю или процессу. Авторизация имеет ряд проблем. Достаточно легко можно перехватить данные идентификации и аутентификации (или вообще любые данные) и повторить их, чтобы выдать себя за пользователя.

Биометрические технологии основаны на биометрии, измерении уникальных характеристик отдельно взятого человека. В отличие от аутентификации пользователей по паролям или уникальным цифровым ключам, человеку необходимо, лишь наличие присуших толькр ему биометрических признаков. Поэтому биометрические даные для аутентификации нельзя забыть, потерять или сообщить другому пользователю. Фактически пропадает необходимость соблюдения пользователями жестких правил создания и хранения паролей. При этом пользователь не запоминает сложных комбинаций пароля, не рискуя тем самым их забыть.

Разрабатываемая система базируется на технологии распознавания лиц как уникальной биометрической характеристике человека. Программными методами в совокупности с техническим устройством снятия биометрического параметра (пример: веб-камера) осуществляется распознавание человеческого лица.

Регистрация нового пользователя заключается в распознавании его лица, что будет являться его авторизационными данными. Далее необходимо авторизационным данным приписать определенные свойства: ФИО, должность и прочее. Полученные данные заносятся в базу данных.

Когда пользователь проходит авторизацию, он располагает свое лицо напротив камеры в фас. Программа авторизации считывает его биометрические параметры и отправляет сервису авторизации. После чего сервис согласовывается с базой данных. В базе данных происходит сопоставление полученного идентификатора с идентификаторами расположенными в базе данных, при нахождении зарегистрированного пользователя происходит его авторизация, если пользователь не был найден, то следует отказ в доступе к ресурсам.

При решении задачи распознавания лиц возникают две проблемы.

Во-первых, любая картинка представляет собой массив пикселей. В то же время один пиксель картинки ничего не значит. Это делает такое представление картинок избыточным и неэкономичным. Для решения задачи распознавания лиц требуется мало информации. Это связано в первую очередь с тем, что нет необходимости определять, как выглядит данный человек из базы данных, а требуется решить обратную задачу: какой человек из коллекции выглядит данным образом.

Вторая проблема заключается в том, что одно и то же лицо может быть сфотографировано при различных внешних факторах, таких как свет, поза, эмоции.

Исходя из соображений простоты реализации и выполнения поставленой задачи распознавания изображения лица, выбрано преобразование изображения на основе вейвлетов Габора. Этот метод позволяет опери-

ровать изображением целиком за счет его фрактальных свойств, тем самым точнее характеризовать изображение, выделение характеристик имеющегося лица. После выделения характеристик картинка больше не нужна.

Система авторизации человека на основе распознавании образов позволит осуществлять авторизацию человека по биометрическим параметрам, а именно по уникальности черт лица человека. Данная система имеет ряд преимуществ, для того чтобы заявить системе о себе, не нужно запоминать и хранить какую нибудь информацию, все необходимое для «узнавания» уже есть – это черты лица. Элементарная простота представления авторизационных данных: люди узнают друг друга при встрече. Нет возможности заменить или подменить авторизационные данные человека, единственный выход – это дорогостоящая в настоящее время пластическая операция, результат которой не всегда удачен.

ЗАЩИЩЕННЫЙ ПОЧТОВЫЙ КЛИЕНТ

А.Б. Миронов, студент 5-го курса КИБЭВС
ТУСУР, г. Томск, Andrey.Mir@gmail.com

Динамичное развитие компьютерных сетей и коммуникаций значительно расширяет возможности их применения для обмена информацией между пользователями. Вместе с распространением различных средств обмена информацией в электронном виде, все острее становится проблема защиты передаваемой информации. Пользователь хочет быть уверен, что никто не получит доступ к отправленным данным, кроме указанного адресата. Получатель же, в свою очередь, хочет быть уверен, что информация получена именно от отправителя и осталась неизмененной в процессе передачи. Для достижения обеих целей во всем мире все шире применяются технологии криптографической защиты с использованием открытых ключей.

Исторически сложилось, что наибольшее распространение для обмена информацией между отправителем и получателем получила электронная почта. Практически все современные почтовые программы имеют возможности шифрования передаваемой информации и электронной цифровой подписи. Однако большинство из них используют не сертифицированные в России алгоритмы. Также существуют отечественные разработки криптографических сертифицированных средств. Некоторые из них предлагают собственное клиентское программное обеспечение, другие же могут интегрироваться в стандартную почтовую программу Windows – Outlook Express. Но пользователю удобнее было

бы иметь возможность работать со всеми криптографическими средствами из одной программы. Чтобы можно было использовать и стандартные средства ОС Windows и криптографические разработки российского производства, как существующие в настоящее время, так и те, которые, возможно, появятся в будущем.

В разрабатываемой программе можно выделить ядро программы, к которому подключаются дополнительные модули. Ядро программы используется для управления дополнительными модулями, а вся основная функциональность переносится в плагины. Плагины можно разделить на два типа: транспортные, в которых реализуются протоколы передачи данных, например POP и SMTP и криптографические.

Криптографические подключаемые модули (плагины) позволяют добавлять поддержку различных шифровальных средств. Также, если появляется необходимость в добавлении поддержки новых криптографических средств, не нужно разрабатывать всю систему с нуля, а можно лишь добавить необходимый плагин. И даже если для конкретной реализации криптографической системы еще нет плагина, то его разработка займет значительно меньше времени, чем системы целиком.

К настоящему моменту реализована поддержка криптографических средств, способных взаимодействовать с клиентским приложением через стандартный механизм криптопровайдеров (CSP). В их число входят стандартные криптографические алгоритмы ОС Windows, а также сертифицированные российские средства «КриптоПро 2» CSP и «СигналКом» CSP. Криптографический модуль позволяет использовать функции шифрования/расшифрования с помощью алгоритмов, реализуемых указанными системами. В их число входят такие алгоритмы с симметричного шифрования, как DES, 3DES, RC4, ГОСТ 28147-89; алгоритмы с закрытым ключом RSA, ГОСТ 34.11-94. Возможность цифровой подписи с использованием сертификатов с открытым ключом (RSA, ГОСТ 34.10-01).

Формат зашифрованных и подписанных сообщений соответствует стандарту PKCS #7. Данный стандарт является международным и описан в RFC2315. Поэтому имеется возможность расшифровать и проверить подпись сообщений, созданных с использованием других средств, если они поддерживают данный формат, и, наоборот, сообщения, созданные с помощью данной программы, могут быть расшифрованы с использованием других средств.

В настоящее время ведется работа над модулем для поддержки криптографической системы «Верба». А в дальнейшем планируется поддержка «Домен-К», «КриптоПро 3».

Литература

1. Стандарты RFC 2315, 1421, 4357, 2437

2. КриптоПро: Руководство разработчика. http://msdn2.microsoft.com – MSDN – Cryptography API

КРАТКИЙ ОБЗОР СУБД (ORACLE, INTERBASE, ACCESS) В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Г.В. Петрова, ассистент каф. КИБЭВС;
Е.А. Мошников, студент 5-го курса ФВС
ТУСУР, г. Томск, pgv@keva.tusur.ru, john_js@rambler.ru

Данная статья направлена на краткое ознакомление с InterBase, Oracle Database и MS Access в области обеспечения безопасности.

InterBase

В 1986 г. была выпущена СУБД InterBase 2. В основном эта СУБД использовалась в системах военного и специального назначения. К сведению: она до сих пор используется в системе управления американской системы залпового огня MLPRS, а также в компании «Боинг» для специальных расчетов жесткости крыльев. [1]

В настоящее время крайней версией является InterBase 2007.

Несмотря на низкие требования к системе (минимальные системные требования: процессор с тактовой частотой 300 или более мегагерц, 32 Мб оперативной памяти, 20 Мб свободного пространства на жестком диске для установки программы), IterBase обладает рядом решений, направленных на улучшение безопасности БД.

Безопасность InterBase основана на концепции «пользователя» (user). В СУБД реализована двухуровневая модель безопасности. На первом уровне осуществляется аутентификация пользователя в момент подключения к базе данных, при этом используется база данных безопасности. Второй уровень реализуется уже на уровне самой базы данных [2]. Также присутствуют: временные таблицы (создаются и используются в момент работы приложения), встраиваемая аутентификация пользователей, журналирование, кросс-платформенность (InterBase поддерживает GNU/Linux, Microsoft Windows, Unix и Solaris), автоматическое восстановление после сбоев, оперативное резервное копирование, автоматизирование процесса управления учетными записями пользователей.

Единственным найденным недостатком является достаточно неудобный и ненадежный инструмент администрирования IBConsole, поставляемый вместе с СУБД, поэтому иной раз приходится использовать продукцию сторонних разработчиков.

Цена: от $195 за простую работу с IB до $4135 за приобретение сервера IB на неограниченное количество пользователей.

Oracle Database

Корпорация Oracle более десяти лет занимает лидирующие позиции в сфере построения промышленных БД.

На данный момент крайней является десятая версия СУБД Oracle.

Ядром системы является сервер базы данных. В зависимости от масштаба использования существует четыре варианта СУБД: Oracle Database Enterprise Edition, Oracle Database Standard Edition, Standard Edition One и Personal Edition. При этом все версии СУБД имеют практически один и тот же код, но отличаются отдельными опциями, службами и модулями, отвечающими за специализацию версии.

Данный подход к построению сервера БД является огромным преимуществом, так как для разных платформ поставляется практически одна и та же СУБД, что положительно влияет на безопасность и функциональность системы. Ведь куда проще отследить ошибки и уязвимости при таком подходе.

Продукт Oracle Database 10g рассматривает безопасность с точки зрения критически важных требований к конфиденциальности информации и защите данных, соблюдению нормативных документов и обеспечению целостности данных [3]. Есть возможность ограничения доступа к отдельным частям таблицы, регулирование доступа к данным внешними средствами. Присутствуют встроенные средства: аудита, резервного копирования и восстановления, логического восстановления недавних изменений в БД, обнаружения внутренних разрушений в БД, обнаружения нарушений в БД на физическом уровне, организации физического горячего резерва БД, обнаружения нарушений в процессе работы СУБД и др.

Не лишена СУБД и недостатков. СУБД требовательна к ресурсам системы (минимум 512 MB оперативной памяти и 5 ГБ свободного пространства на жестком диске). Главным недостатком же является цена.

Цена: от $190 за Oracle Database Standard Edition для одного пользователя, $120000 за Oracle Database Enterprise Edition для 4-процессорного сервера рассчитанного на 100 пользователей (цена рассчитана с помощью калькулятора цен на сайте компании [4]) и выше.

Microsoft Access

MS Access – СУБД от корпорации Microsoft. Данная СУБД поставляется вместе с пакетом программ MS Office.

Крайней версией на данный момент является MS Access 2007.

По умолчанию Access 2007 отключает все потенциально небезопасные программы или другие компоненты независимо от версии Access, в которой создавалась эта база данных. Данной СУБД также предоставляются шифрование или дешифрование базы данных с использованием

пароля, упаковка, подпись и развертывание базы данных, работа с сертификатами и др. [5].

У такой СУБД есть и недостатки. Защита информации от сбоев реализована сохранением данных после любого действия, что отрицательно влияет на быстродействие системы. Отсутствие встроенного компилятора EXE-файлов, что не позволяет правильно закончить технологический цикл разработки приложения без привлечения других средств программирования. СУБД использует библиотеки ОС Windows, что также отрицательно влияет на быстродействие и безопасность.

Но несмотря на недостатки, MS Access все равно остается достаточно популярной СУБД.

Цена: от 3856,85 руб. за Microsoft Office 2007 Home and Student, до 12967,78 руб. За Microsoft Office 2007 Professional.

Все рассмотренные СУБД обеспечивают достаточно хорошую защиту. Так какую же выбрать? Это зависит от того, для чего нужна СУБД, для малого бизнеса, для корпорации или для личной работы. Не стоит приобретать Oracle Database Enterprise Edition за $120000 для ведения БД по своей коллекции марок, как и не выгодно приобретать Microsoft Office 2007 Home and Student за сотню долларов для работы трансатлантической корпорации. так как разрабатываемая программа предназначена для работы ограниченного круга пользователей (малый бизнес), то лучшим выбором будет MS Access.

Литература

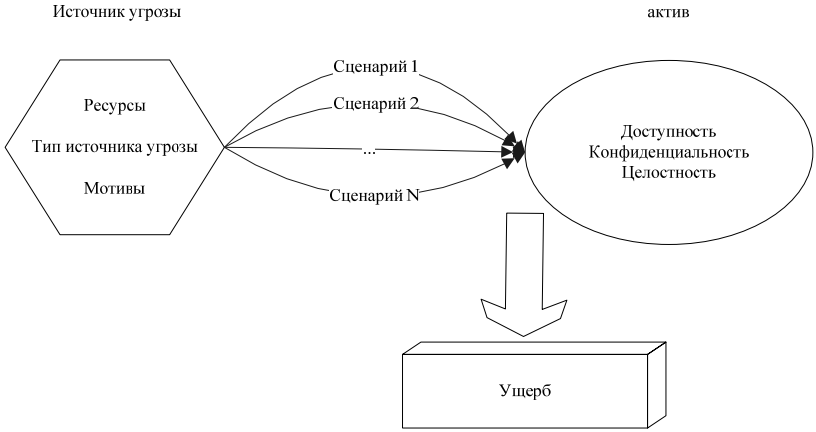
1. Интернет-энциклопедия. http://www.wikipedia.org
2. Информация об InterBase. http://www.ibase.ru
3. Информация об Oracle DataBase. http://www.oracle.com
4. Калькулятор цен на продукцию Oracle. http://www.orashop.ru
5. Информация об Access Office 2007. http://www.microcoft.ru

ОЦЕНКИ УРОВНЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.М. Нечунаев

Отделение Пенсионного Фонда Российской Федерации по Удмуртской Республике, г. Ижевск, nvm@019.pfr.ru

Для постановки проблемы используется модель «угроза-актив», позволяющая производить классификацию угроз информационной безопасности, воздействующих на корпоративную информационную систему (КИС).



Модель «угроза-актив»

В настоящей модели можно выделить следующие компоненты:

- источник угрозы – субъект, который воздействует на активы;
- актив – то, на что воздействует угроза, КИС / элементы КИС;
- ущерб – отрицательный количественный или качественный результат выполнения определенного сценария угрозы;
- сценарии – типовые наборы действий, которые источник угрозы прикладывает к активу для причинения ущерба.

Источники угрозы (ИУ) характеризуются следующими свойствами:

- тип источника угрозы – люди, природные явления, технические средства;
- мотив источника угрозы – материальная прибыль, принуждение, месть, политические амбиции;
- ресурсы источника угрозы – любые средства, которые могут применяться для нанесения ущерба.

В качестве **активов** в настоящей модели рассматривается КИС / элементы КИС / совокупность элементов КИС (технические средства, программное обеспечение, информационные ресурсы, организационная структура). Активы характеризуются следующими свойствами: конфиденциальность, целостность, доступность.

Потенциальный ущерб определяется совокупностью критериев, отражающих важность защищаемых активов для выполнения миссии организации. Критерии, определяющие потенциальный ущерб, зависят от направления деятельности организации. Перечислим некоторые из наиболее распространенных критериев:

• потери, связанные с восстановлением элементов ИС (нарушение свойства доступности);

• потери, связанные с нарушением конфиденциальности;

• ущерб репутации организации;

• невозможность выполнения бизнес-процесса;

• финансовые потери;

• угроза жизни персонала.

Сценарии – это действия, которые источник угрозы применяет к активам для нанесения ущерба. Сценарии угрозы характеризуются следующими свойствами:

• свойства актива, на которые воздействует источник угрозы;

• мотивация источника угрозы;

• ресурсы, которыми располагает источник угрозы.

Оценка уровня угроз производится на основе характеристики источника угроз с учетом косвенных факторов, описывающих статистические данные по угрозам.

В качестве косвенных факторов используются характеристики системы (потенциальная ценность активов для злоумышленника), статистика инцидентов информационной безопасности.

Оценка потенциала угрозы, вероятности угрозы и уровня угрозы производится с использованием количественно-качественной шкалы, содержащей пять уровней:

• (О)тсутствует – 0

• (Н)изкий – 0.25

• (С)редний – 0.5

• (В)ысокий – 0.75

• (К)ритический – 1

Значение уровня угрозы определяется как функция от потенциала угрозы и вероятности угрозы.

Потенциал угрозы определяется свойствами источника угрозы, необходимыми для реализации определенных сценариев атак.

В силу высокой стохастичности проблемы информационной безопасности вероятность угрозы определяется методом экспертных оценок. Вероятность угрозы определяется по следующим косвенным факторам: статистика по зарегистрированным инцидентам, тенденции в статистике по подобным инцидентам, ценность активов, на которые могут воздействовать источники угроз, уровень доверия к персоналу КИС.

Оценка уровня риска

Вероятность угрозы	Потенциал угрозы				
	Отсутств.	Низкий	Средний	Высокий	Критич.
Отсутствует	(О)	(О)	(О)	(Н)	(Н)
Низкая	(О)	(Н)	(Н)	(С)	(С)
Средняя	(О)	(Н)	(С)	(С)	(В)
Высокая	(Н)	(С)	(С)	(В)	(К)
Критическая	(Н)	(С)	(В)	(К)	(К)

Литература

1. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком, 2004. 280 с.

2. *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК Пресс, 2004. 384 с.

3. *Шумский А. А., Шелупанов А. А.* Системный анализ в защите информации. М.: Гелиос АРВ, 2005. 224 с.

ЗАЩИЩЕННЫЙ ПОЧТОВЫЙ КЛИЕНТ

С.А. Пахандрин, студент 5-го курса КИБЭВС
ТУСУР, г. Томск, Sergey.Pakhandrin@gmail.com

В наше время одной из самых распространенных задач в области защиты информации является обеспечение защищенности, целостности обмена электронными сообщениями. Ведь электронные сообщения могут нести в себе конфиденциальную информацию. Поэтому задача обеспечения защиты этих данных особенно актуальна, так как электронные сообщения на данный момент являются самым популярным видом общения по сети. Но не менее важной задачей является выбор алгоритмов, методов шифрования, создания ЭЦП, а также транспорта, с помощью которого будет отправлено или принято письмо. Поэтому была поставлена задача разработки защищенного почтового клиента с возможностью шифрования, создания ЭЦП. Но главная цель это разработка приложения с расширяемыми модулями, а точнее возможность изменения, подключения новых модулей (плагинов), без изменения главного приложения.

Почтовые программы служат для отправки и получения электронных писем, используя различные протоколы передачи данных. Для обеспечения защищенности электронных писем многие почтовые программы используют различные алгоритмы шифрования. Данная возможность позволяет сохранять обмен электронными сообщениями защищенным.

Также основной особенностью, нацеленной на обеспечение целостности и неизменяемости сообщения, является создание ЭЦП для письма. Это позволяет удостовериться в оригинальности посланного сообщения, что дает гарантию получения именно тех данных, которые были посланы отправителем.

Для отправки электронных сообщений почтовые программы используют различные протоколы передачи данных. Одними из самых популярных протоколов для передачи сообщений, являются POP3 и SMTP. Данные протоколы передачи данных позволяют вести передачу по открытым каналам связи, так и по закрытым с использованием авторизации, различных сертификатов и т.п.

Электронное письмо может содержать как текст, так и любую другую информацию в виде прикрепляемого файла. Самым распространенным форматом электронного сообщения является MIME. MIME определяет механизмы для отправки разного рода информации с помощью электронной почты, включая текст на языках, отличных от английского, для которых используются символьные кодировки, отличные от ASCII, помимо этого, 8-битный бинарный контент, такой как картинки, музыка, фильмы и программы.

Одной из основных преследуемых целей, является разработка независимого, динамически подключаемого транспортного модуля, способного работать с самыми популярными протоколами передачи данных электронных сообщений и поддержка всех стандартов MIME, SMTP, POP3.

При разработке класса разбора электронного сообщения необходимо в точности соблюдать все предписания стандартов формата MIME. Это необходимо для того, чтобы при получении электронного письма, созданного в любом другом почтовом клиенте (с соблюдением формата MIME версии 1.0), была возможность разобрать его на мелкие составляющие (заголовки, тело письма и прикрепленные файлы). Также другой составляющей класса письма является создание полноценного электронного сообщения с соблюдением всех стандартов, для того чтобы любой другой клиент, работающий с форматом MIME версии 1.0, мог разобрать всю структуру полученного письма.

Транспортный модуль, должен иметь независимые настройки от почтового клиента. Основной упор при разработке транспортного модуля, ставится на то, что в дальнейшем без труда можно будет дополнять протоколы передачи данных, при этом сам почтовый клиент останется нетронутым.

В рамках проекта «Защищенный почтовый клиент» также разрабатывается независимый, динамически подключаемый криптографический модуль. Основные возможности криптографического модуля:

1) работа с СКЗИ, поддерживающими алгоритм шифрования ГОСТ 28147-89, алгоритм хэширования и выработки ЭЦП ГОСТ Р.34.10/11-94 и алгоритм выработки ЭЦП ГОСТ Р.34.10-2001;

2) обязательная поддержка СКЗИ «КриптоПро CSP 2.0», «КриптоПро CSP 3.0», «ДоменК», «СКЗИ Верба 6.1», «Сигнал-Ком», Microsoft Crypto API;

3) шифрование, выработка и проверка ЭЦП осуществляется при использовании сертификатов ОК;

4) инструмент работы с сертификатами (вывод нужных данных, выбор сертификата для шифрования, проставления ЭЦП, просмотр системных хранилищ и пр.).

Литература

1.Стандарты RFC 2822, 2045, 2046, 2047, 2049, 2633, 1847.

2.http://ru.wikipedia.org/wiki/MIME – описание MIME-формата

РЕШЕНИЕ ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕССНОГО ПОДХОДА

А.А. Пономарев, аспирант кафедры информационной безопасности в управлении УдГУ

г. Ижевск, ponart@mail.ru

Существование любого предприятия связано с выполнением на предприятии бизнес-процессов. Бизнес-процесс – структурированный набор действий, охватывающий различные сущности предприятия и подчиненный определенной цели (ISO/CD 15531-1). Целью любого коммерческого предприятия в конечном итоге является получение прибыли. Прибыль же извлекается из бизнес-процессов, происходящих на предприятии. Бизнес-процессы охватывают собой всю структурированную деятельность предприятия. По сути, коммерческое предприятие нуждается в защите своих бизнес-процессов. Исходя из этого и должна быть, построена система защиты информации на предприятии. Такой подход позволяет более детально поставить приоритеты в защите той или иной информации.

Деятельность предприятия можно представить в виде трех групп высокоуровневых процессов [4]: процессы управления организацией; основные процессы (процессы основной деятельности); вспомогательные процессы (процессы, связанные с ресурсообеспечением).

Характерными признаками трех перечисленных групп процессов являются:

• процессы управления организацией предназначены для координации и управления деятельностью всей организации. Данные процессы предназначены для формирования целей деятельности для основных процессов, а также синхронизации основных, вспомогательных и управленческих процессов внутри организации;

• основные процессы предназначены для создания основного продукта производства (услуги). Данные процессы добавляют продукту ценность для потребителя;

• вспомогательные процессы обеспечивают деятельность основных процессов. Результатом являются ресурсы и сервисы для основных процессов. Деятельность вспомогательных процессов не касается основных продуктов, поэтому они добавляют продукту стоимость.

Приоритетами СЗИ должны стать защита основных бизнес процессов организации, защита процессов управления, участие во вспомогательных процессах (работа с персоналом, участие в деятельности служб информатизации и др.). При этом сама деятельность службы защиты информации или специалиста по защите информации может быть представлена и как вспомогательный бизнес-процесс, так как данная деятельность не участвует в выпуске продукции и по своей сути является затратной для предприятия. Также деятельность СлЗИ может быть представлена как основной бизнес-процесс, так как создает экономию при возможных потерях, т.е. формирует прибыль.

Важнейшими исходными данными для построения СЗИ являются информационные модели (описание реализованных бизнес-процессов, реализуемых технологий и т.п.). Данные модели определяют приоритеты деятельности СлЗИ, так как они позволяют понять, где в структуре деятельности предприятия имеются уязвимые места для потенциальных злоумышленников, какие меры (организационные, технические, криптографические и др.) могут потребоваться и какие будут наиболее эффективны.

Процессный подход позволяет преодолеть недостатки функционального подхода, фокусируясь на сквозном управлении процессами и методах их внутренней организации, выделении взаимосвязей процессов (в частности информационными потоками), которые определяются технологическими особенностями. Процессный подход – это представление о бизнес-процессе как последовательности операций, реализуемых во времени в соответствии с определенной технологией для извлечения прибыли (получение какого то результата).

Наличие или отсутствие в организации формализованной модели ее управленческой, основной или вспомогательной деятельности не является препятствием к организации деятельности по обеспечению информационной безопасности на базе процессного подхода.

Деятельность по выявлению и описанию существующих бизнес-процессов (анализ бизнес-процессов), а также проектированию новых (проектирование бизнес-процессов) называется бизнес-моделированием.

Существует множество нотаций для описания бизнес-процессов. Самыми авторитетными стали нотации IDEF, которые были приняты как стандарты в частности в России (см. [2]). Стандарт [2] предназначен для использования при анализе и синтезе производственно-технических и организационно-экономических систем методами функционального моделирования. Рекомендации содержат описание комплекса средств для наглядного представления широкого спектра деловых, производственных и других процессов и операций предприятия на любом уровне детализации, а также организационные и методические приемы применения этих средств [2]. На основе данных стандартов выпущено множество программных продуктов позволяющих представить деятельность организации с помощью бизнес-процессов.

Деятельность службы защиты информации также можно представить в виде модели, написанной в стандарте IDEF0. Модель может быть построена с разной степенью детализации. В частности представим, что организация приступила к введению режима коммерческой тайны. Тогда этапами выполнения этого бизнес-процесса будет выполнение пунктов указанных в ст. 10 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», которая устанавливает, какие мероприятия должны быть организованы на предприятии, чтобы считался введенным режим коммерческой тайны. При этом в законе не сказано, каким образом должны быть выполнены те или иные пункты ст. 10. Выполнение всех требований Закона дает цепочку организационных мероприятий. Перечень таких мероприятий можно посмотреть в [3]. Тогда удобно воспользоваться стандартом IDEF0, построить процесс установления режима коммерческой тайны на предприятии. Функциями рассматриваемого процесса будут: определение перечня информации составляющей КТ, ограничение доступа к информации, учет лиц, получивших доступ к КТ, регулирование отношений на основании договоров, нанесение на материальные носители грифа КТ. Каждая функция подвергается декомпозиции до выведения конкретных задач, исполнителей, документов, которыми они должны руководствоваться. Таким образом, применение нотации IDEF0 является полезным с точки зрения формализации процессов защиты информации.

Литература

1. Федеральный закон Российской Федерации от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

2. Р 50.1.028-2001 Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования.

3. *Фадеев Ю.И., Лупачева А.П.* Организация защиты информации на предприятии на основе закона о коммерческой тайне // Вестн. Удм. ун-та. Сер. Правоведение. 2006. Вып. 1.

4. *Курило А.П., Зефиров С.Л., Голованов В.Б. и др.* Аудит информационной безопасности. М.: Изд. группа «БДЦ-пресс», 2006. 304 с.

ОХРАННО-ПРОЖАРНАЯ СИГНАЛИЗАЦИЯ

А.А. Ремизов, студент 5-го курса КИБЭВС
ТУСУР, г. Томск, remizovaa@sibmailcom

Актуальность охранных систем и пожарных сигнализаций в настоящее время очевидна. Случаи, когда любая искра, излишняя тепловая либо электрическая энергия могут привести к пожару, являются типичными.

Современная охранно-пожарная сигнализация – это технический комплекс, который способен вовремя выявить незаконное проникновение или зафиксировать зону риска, связанную с пожароопасными ситуациями. Объединение охранных систем и пожарных сигнализаций дает некоторые преимущества, при этом позволяя использовать каждую из них независимо друг от друга. Еще один положительный момент в составной защитной системе – то что она служит для преждевременного оповещения охранных служб о несанкционированном вторжении или возможном возгорании.

Система охранно-пожарной сигнализации представляет собой сложный комплекс технических средств, служащих для своевременного обнаружения возгорания и несанкционированного проникновения в охраняемую зону. Как правило, охранно-пожарная сигнализация интегрируется в комплекс, объединяющий системы безопасности и инженерные системы здания, обеспечивая достоверной адресной информацией системы оповещения, пожаротушения, дымоудаления, контроля доступа и др.

В зависимости от масштаба задач, которые решает охранно-пожарная сигнализация, в ее состав входит оборудование трех основных категорий:

1. Оборудование централизованного управления охранно-пожарной сигнализацией, как правило, центральный компьютер с установленным на нем программным обеспечением для управления охранно-пожарной сигнализацией; в небольших системах охранно-пожарной сигнализации задачи централизованного управления выполняет охранно-пожарная панель.

2. Оборудование сбора и обработки информации с датчиков охранно-пожарной сигнализации: приборы приемно-контрольные охранно-пожарные (панели).

3. Сенсорные устройства – датчики и извещатели охранно-пожарной сигнализации.

Интеграция охранной и пожарной сигнализации в составе единой системы осуществляется на уровне централизованного мониторинга и управления. При этом системы администрируются независимыми друг от друга постами управления, сохраняющими автономность в составе системы охранно-пожарной сигнализации. На небольших объектах охранно-пожарная сигнализация управляется приемно-контрольными приборами.

Приемно-контрольный прибор осуществляет питание охранных и пожарных извещателей по шлейфам, прием тревожных извещений от извещателей, формирует тревожные сообщения, а также передает их на станцию централизованного наблюдения и формирует сигналы тревоги на срабатывание других систем.

Система охранной сигнализации в составе охранно-пожарной сигнализации выполняет задачи своевременного оповещения службы охраны о факте несанкционированного проникновения или попытке проникновения людей в здание или его отдельные помещения с фиксацией даты, места и времени нарушения рубежа охраны.

Система пожарной сигнализации предназначена для своевременного обнаружения места возгорания и формирования управляющих сигналов для систем оповещения о пожаре и автоматического пожаротушения.

Литература

1. *Зайцев А.П.* Программно-аппаратные средства обеспечения информационной безопасности: Учеб. пособие. В 2 разд. Томск: Том. Межвуз. центр дистанционного образования, 2004. Разд. 1. 120 с.

2. *Зайцев А.П., Шелупанов А.А.* Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Томск: Изд-во Том. гос. ун-та систем управления и радиоэлектроники, 2004. 204 с.

ОБЗОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ИДЕНТИФИКАЦИИ АВТОРСТВА ТЕКСТОВ

А.С. Романов, аспирант кафедры КИБЭВС

ТУСУР, г. Томск, ras@ms.tusur.ru

Существующие в настоящее время разработки программного обеспечения в области идентификации авторства текстов можно разделить на несколько классов:

1. Программы, предназначенные непосредственно для определения авторства текстов:

– «Штампомер» (Л.Л. Делицын);

– «Лингвоанализатор» (Д.В. Хмелев);

– «СМАЛТ» (ПетрГУ);

– «Стилеанализатор» (О.Г. Шевелев) и др.

2. Программы, ставящие целью выявление факта плагиата:

– «Антиплагиат» (ЗАО «Анти-Плагиат», «Форексис»);

– «Плагиат Информ» («СофтИнформ»);

– «АУРА-Текст» (СПбГУ) и др.

3. Программы интеллектуального анализа данных (Data Mining, Text Mining), предназначенные для сбора и анализа лингвистической информации о тексте, классификации, кластеризации, реферирования текстов, выделения ключевых понятий текста и т.д.:

– «Intelligent Miner for Text» (IBM);

– «TextAnalyst», «PolyAnalyst» (Мегапьютер Интеллидженс);

– «Text Miner» (SAS);

– «SemioMap» (Semio Corp.);

– «Oracle Text», «Oracle Data Mining» (Oracle);

– «Knowledge Server» (Autonomy) и др.

4. Специализированное программное обеспечение для определения психологического портрета автора текста, психологического содержания текста:

– «ЛИНГВА-ЭКСПРЕСС» (В.И. Батов);

– «Prostyle»;

– «ВААЛ» (В.П. Белянин) и др.

Анализ известных методов определения авторства показал, что пока не существует универсального подхода, обеспечивающего стабильный достоверный результат [1]. Небольшой объем текстов, действительно нуждающихся в атрибуции, не позволяет применять большинство известных методов. Эти факты ставят под сомнение возможность применения программ первого класса как основанных на методах идентификации авторства для решения реальных практических задач.

В основе программ второго класса лежат алгоритмы поиска текстовой информации. Перестройка предложений, замена ключевых слов синонимами с большой вероятностью позволяют полностью обойти данные системы.

Программы интеллектуального анализа данных обладают широкими возможностями, но пользователями систем должны быть квалифицированные инженеры по знаниям, так как большая часть этих программ

не ставит задачу определения авторства как первостепенную и требуется определеить ключевые параметры. Стоит также отметить высокую стоимость систем этого класса.

Программы для определения психологического содержания текста не используются непосредственно для определения авторства текстов, но также представляют интерес для специалистов за счет применяемых в них подходов.

Таким образом, можно сделать вывод, что к настоящему времени на рынке не представлено эффективных программных решений, предназначенных для определения авторства текста. Поэтому необходимо ввести дальнейшие исследования, направленные на поиск новых, совершенствование или комбинирование уже имеющихся методов определения авторства, с помощью которых станет возможной работа с малыми объемами выборки, разработка программных систем на их основе и проверка методов на большом корпусе текстов для определения их состоятельности.

Работа поддержана грантом ФСРМПНТ.

Литература

1. *Romanov A.S.* The analysis of identification methods of Text's authors// Interactive Systems and Technologies: The Problems of Human-Computer Interaction. Collecction of scientific papers. Ulyanovsk: UlSTU, 2007. 270 p.

СТАНДАРТЫ В ОБЛАСТИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.С. Рюхова, студентка 5-го курса
ТУСУР, г. Томск

В настоящее время организация режима информационной безопасности становится критически важным фактором развития любой организации РФ. При этом большое внимание уделяется требованиям и рекомендациям как российской нормативно-методической базы, так и международной в области защиты информации. В настоящих документах подробно рассматриваются не только организационные вопросы, касающиеся информационной защиты, но и важные аспекты поддержания безопасности на должном уровне.

Приведем перечень стандартов и руководящих документов, которые являются основополагающими при организации системы защиты автоматизированных систем управления:

Российские стандарты:

– ГОСТ Р 50739-95 Защита от несанкционированного доступа к информации. В стандарте ГОСТ Р 50739 говорится только о программно-технических средствах защиты от НСД, но не упоминается о программно-аппаратных средствах, которые играют значительную роль для повышения уровня безопасности;

– ГОСТ Р 51241-98 Средства и системы контроля и управления доступом. Стандарт устанавливает классификацию, общие технические требования и методы испытаний средств и систем контроля и управления доступом.

В стандарте отражены классификация систем контроля управления доступом, общие технические требования, методы испытаний средств и систем контроля управления доступом;

– СТО БР ИББС 1.0-2006 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. Данный стандарт распространяется на организации банковской системы Российской Федерации (БС РФ) и устанавливает положения (политики и требования) по обеспечению информационной безопасности в организациях БС РФ;

– СТО БР ИББС 1.1-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности. Стандарт распространяется на организации БС РФ, а также на организации, проводящие аудит ИБ, и устанавливает требования к проведению внешнего аудита;

– СТО БР ИББС 1.2-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия организации банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2006. Этот стандарт применяется для проведения самооценки уровня защищенности предприятия;

– РС БР ИББС 2.0-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0. Настоящий стандарт устанавливает требования к структуре, составу, назначению, содержанию внутренних документов по обеспечению информационной безопасности (ИБ). В данном стандарте представлена структура документов по обеспечению ИБ, состав внутренних документов, менеджмент документов.

Международные стандарты:

– ISO 17799-2005 Информационные технологии. Методики безопасности. Практические правила управления информационной безопас-

ностью. Настоящий стандарт устанавливает правила по управлению информационной безопасности лицам, ответственным за планирование, реализацию или поддержку решений по вопросам безопасности в организации. Он предназначен для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации;

– NIST 800-30 Технология управления информационными рисками. Настоящий стандарт подробно рассматривает вопросы, касающиеся управления рисками и позволяет оценить уровень защищенности системы;

– ISO/IEC 27001-2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования. Данный стандарт предоставляет модель для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшении Системы Менеджмента Защиты информации (СМЗИ). Данный стандарт предназначен для того, чтобы способствовать организации совместить или интегрировать ее СМЗИ с имеющими к ней отношение требованиями системы менеджмента качества.

Руководящие документы, утвержденные Гостехкомиссией при Президенте Российской Федерации:

– «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Настоящий документ рассматривает основные принципы, которые закладываются в основу проблемы защиты информации от несанкционированного доступа (НСД), являющейся частью общей проблемы безопасности информации. Концепция предназначена для заказчиков, разработчиков и пользователей СВТ и АС, которые используются для обработки, хранения и передачи требующей защиты информации;

– «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Настоящий руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований;

– Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Данный руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. Документ может использоваться как нормативно-методический материал для заказчиков и

разработчиков АС при формулировании и реализации требований по защите.

– Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Настоящий руководящий документ (РД) содержит систематизированный каталог требований к безопасности информационных технологий (ИТ), порядок и методические рекомендации по его использованию при задании требований, разработке, оценке и сертификации продуктов и систем информационных технологий по требованиям безопасности информации. Руководящий документ состоит из трех частей. Наиболее значимым документом является Часть 2 РД, в контексте вопроса аудита ИБ, так как в ней описаны функциональные требования к безопасности АС.

Итак, очевидно, что для достижения высокого уровня безопасности не рекомендуется использовать только руководящие документы, потому что они не отражают все аспекты защиты информационной безопасности. Совместно с руководящими документами необходимо использовать стандарты в области защиты информационных технологий, но следует учитывать специфику деятельности предприятия при организации информационной безопасности.

Литература

1. ГОСТ Р 50739-95 Защита от несанкционированного доступа к информации.

2. ГОСТ Р 51241-98 Средства и системы контроля и управления доступом;

3. СТО БР ИББС 1.1-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности.

4. РС БР ИББС 2.0-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0.

5. СТО БР ИББС 1.0-2006 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.

6. СТО БР ИББС 1.2-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия организации банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2006.

7. ISO 17799-2005 Информационные технологии. Методики безопасности. Практические правила управления информационной безопасностью.

8. NIST 800-30 Технология управления информационными рисками.

9. ISO/IEC 27001-2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.

10. Руководящие документы Гостехкомиссии РФ.

МЕТОДЫ РАЗРАБОТКИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАНСОСТИ

А.С. Рюхова, студентка 5-го курса КИБЭВС
ТУСУР, г. Томск

Чтобы корректно говорить об обеспечении защиты информации, в первую очередь рассмотрим некоторые понятия.

Под информацией понимается сведения о лицах, факторах, явлениях, событиях и процессах независимо от формы их представления. В нашем случае информация – это информационный актив (что-либо имеющее ценность для организации).

Информационная безопасность – это защита информации от широкого спектра угроз с целью обеспечения непрерывности бизнес-процессов и минимизации рисков. Также информационная безопасность подразумевает обеспечение целостности, конфиденциальности, доступности, подлинности, надежности информации. Под целостностью понимается свойство информации, состоящее в ее существовании в неискаженном виде, неизменном по отношению к некоторому фиксированному ее состоянию.

Под конфиденциальностью будем понимать свойство информации, состоящее в том, что она не может быть обнаружена и стать доступной без разрешения отдельным лицам, модулям или процессам.

Доступность – свойство системы, в которой циркулирует информация, характеризуемое способностью обеспечивать своевременный беспрепятственный доступ к интересующей информации, когда в этом возникает необходимость.

Информационная безопасность достигается внедрением приемлемого набора средств управления, включая политики безопасности, процессы, процедуры, организационные структуры, а также программное и аппаратное обеспечение.

Политика безопасности – это совокупность определенных правил, требований для обеспечения безопасности информационных активов. Она определяет, каким образом организация хочет обеспечить безопасность своей деятельности и позволяет повысить уровень защищенности системы.

Целью политики безопасности является обеспечение управления и поддержки информационной безопасности в соответствии с требованием бизнеса и соответствующими законами и нормами.

ПБ должна описывать следующие этапы создания системы защиты информации (СЗИ):

– определение информационных и технических ресурсов, подлежащих защите;

– выявление полного множества потенциально возможных угроз и каналов утечки информации;

– проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

– определение требований к системе защиты;

– осуществление выбора средств защиты информации и их характеристик;

– внедрение и организация использования выбранных мер, способов и средств защиты;

– осуществление контроля целостности и управление системой защиты.

При разработке политики безопасности целесообразно руководствоваться следующими принципами:

– принцип невозможности миновать защитные средства. Он означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через СЗИ;

– усиление самого слабого звена, при помощи которого определяется надежность системы. Часто таким звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер;

– принцип недопустимости перехода в открытое состояние. При любых обстоятельствах (в том числе нештатных) СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ;

– принцип минимизации. Выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей;

– принцип разделения обязанностей. Должно быть такое разделение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс;

– принцип многоуровневой защиты. Нужно использовать не один защитный рубеж, а несколько, т.е. использовать не только средства физической защиты, но и программно-технические средства, а также управление доступом, протоколирование и аудит;

– принцип простоты и управляемости информационной системы;

– принцип обеспечения всеобщей поддержки мер безопасности.

На данный момент предлагаются несколько типов ПИБ:

– дискреционная ПИБ;

– мандатная ПИБ;

– ПИБ на основании стандарта ISO 17799.

При использовании дискреционной политики безопасности пользователи могут принимать участие в определении функций политики и присвоении атрибутов безопасности. Соответственно, дискреционные механизмы не могут противостоять злоумышленнику, так как переносят все бремя обеспечения безопасности на пользователя, халатность которого в любой момент времени может привести к нарушению политики (в отличие от мандатных механизмов безопасности, которые перекладывают бремя обеспечения безопасности на администратора политики безопасности).

При наличии же мандатных механизмов защиты утечка конфиденциальной информации возможна лишь через скрытые каналы, что ограничивает размеры утечки и обеспечивает контроль за ней, при условии аудита скрытых каналов.

Стандарт ISO 17799, основанный на анализе и управлении рисками, занял лидирующие позиции в Европе и Азии и стал стандартом де-факто в построении систем управления информационной безопасностью.

Наблюдая за последние годы экспоненциальный рост интереса к стандарту, очевидно, что в ближайшие годы нас ждет бум интереса как к применению стандарта на практике, так и к процессу официальной сертификации по ISO 27001. ISO 17799 – это та объективная реальность, которая уже не имеет альтернативы. Политика, созданная посредством данного стандарта, является наиболее полным перечнем указаний, требований и правил по организации информационной защиты, дает нам полное представление каким образом нужно строить защиту систему.

Современный рынок средств защиты информации можно условно разделить на две категории:

1. Средства защиты для государственных структур.
2. Средства защиты для коммерческих компаний и структур.

В структурах, где необходима конфиденциальность информации, и государственных структурах наиболее приемлемым было бы использование мандатной политики безопасности в связи с тем, что она предотвращает утечку информации от объектов с высоким уровнем доступа к объектам с низким уровнем.

Очевидно, что в коммерческих компаниях, в которых нет сверхважной информации, целесообразно использование дискреционной политики информационной безопасности, так как обеспечивается простота реализации механизмов защиты информации и меньше финансовые затраты.

Литература

1. ISO 17799-2005 Информационные технологии. Методики безопасности. Практические правила управления информационной безопасностью.

2. Информационная безопасность бизнеса. www.InfoSecurity.ru

3. CIO: руководитель информационной службы. www.cio-world.ru
4. *Петренко С.А.* Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТИ; ДМК Пресс, 2005. 384 с. (Информационные технологии для инженеров).
5. Проект InfoSecurity.ru – Информационная безопасность: Виды угроз.
6. http://skb.inural.ru/index.php/article/archive/74/9/74/

СИСТЕМА КОМПЛЕКСНОГО СЕТЕВОГО СКАНИРОВАНИЯ

М.М. Саматов, студент 5-го курса КИБЭВС
ТУСУР, г. Томск, samatovm@gmail.com

Цель работы – разработка системы комплексного сетевого сканирования, позволяющей изменять базовый функционал с помощью дополнительных модулей.

Развитие информационных систем и технологий сопровождается ростом доли угроз, связанных с наличием уязвимостей программных ресурсов. Широкое распространение средств реализации таких угроз, в том числе вирусного типа, делает чрезвычайно актуальным применение различных систем анализа защищенности. При аудите безопасности, аттестации и сертификации информационных систем широко используются сетевые сканеры, позволяющие проводить инвентаризацию сети и идентификацию уязвимостей. В настоящее время на рынке программных средств представлено достаточно много подобных сканеров: от условно-бесплатных и с открытым кодом до специализированных комплексов аудитора информационной безопасности. Однако эти системы в основном имеют либо излишне специализированные функции, либо слишком общие.

Среди средств защиты сетей сканеры занимают особое место. Во-первых, потому что они могут быть как средством обеспечения безопасности, так и средством нападения. Данные об обнаруженных уязвимостях, предоставляемые сетевым сканером безопасности, могут быть одинаково полезны и администратору безопасности, контролирующему состояние защищенности узлов сети, и нарушителю, осуществляющему поиск наименее защищенных сетевых служб.

Во-вторых, далеко не во всех случаях очевидна польза от применения сканеров безопасности. Например, польза от межсетевого экрана очевидна – он осуществляет фильтрацию трафика и не пропускает в защищаемую им сеть «ничего лишнего». Или, например, система обнаружения сетевых атак. Ее роль тоже предельно ясна – непрерывный мониторинг трафика и обнаружение в нем признаков атак. То есть результат ее работы виден сразу – события, происходящие в данный момент вре-

мени, часть из которых требует немедленного реагирования. Основной результат работы сканера безопасности – перечень уязвимостей, которые могут быть использованы при проведении атак. Но в данном случае речь идет лишь о потенциальной возможности атаки, а не о свершившемся факте реализации угрозы. К тому же в некоторых случаях возможность использования обнаруженной уязвимости может быть маловероятна.

В-третьих, сканеры безопасности могут оказывать нежелательное влияние на объекты защиты. Например, сетевой сканер в процессе работы может порождать значительное количество сетевого трафика, существенно повышая нагрузку на сеть. К тому же некоторые проверки, выполняемые сетевым сканером, могут привести к выведению из строя сканируемого узла или отдельной службы

Существующие системы сетевого сканирования не используют оптимальный набор методов для реализации основных функции, и в то же время все они имеют достаточно высокую стоимость лицензии что обусловлено поддержкой излишнего дополнительного функционала. Разрабатываемая система будет лишена этих недостатков благодаря использованию полного комплекса методов для реализации основных функций и модульной системе подключения дополнительных функций.

Разрабатываемая система предназначена для проведения комплексного сетевого анализа под управлением ОС Windows NT, Windows 2000 и Windows XP

Базовые функции:

Идентификация узлов сети

Используются методы:

– ICMP Ping;

– другие сообщения ICMP;

– TCP Ping;

– UDP Discovery;

– ARP Scan;

– пассивные методы (анализ сетевого трафика).

Идентификация открытых портов

Используются методы:

– TCP connect() – сканирование портов TCP с установлением соединения;

– SYN Scan – «полусканирование»;

– UDP Scan – сканирование портов UDP обычным образом;

– скрытое сканирование.

Идентификация служб и приложений

Используются методы:

– анализ «баннеров»;

– использование команд служб прикладного уровня;

– учет особенностей работы сервисов прикладного уровня;

– эвристические методы.

Идентификация ОС

Используются методы:

– простейшие;

– опрос стека TCP/IP;

– анализ пакетов ICMP;

– анализ работы таймера повторной передачи TCP;

– тесты в отношении порта 0;

– эвристические.

Базовая система протоколирования

Автоматическое обновление БД системы

Главной особенностью этой системы является модульная структура. Пользователь может значительно расширить функционал программы, приобретая дополнительные модули. Этот подход удобен тем, что каждый пользователь на основе базовой комплектации с помощью дополнительных модулей может создать конфигурацию, максимально удовлетворяющую его требованиям и не перегруженную ненужными в его случае функциями.

Дополнительные функции, поставляемые с модулями:

– добавление проверок для конкретного ПО;

– расширенная система мониторинга;

– анализ уязвимостей сетевых служб беспроводных устройств;

– планировщик заданий;

– редактор шаблонов;

– создание своих проверок;

– предопределенные шаблоны сканирования.

Аналоги данной системы лишены подобной гибкости, также в них используется более ограниченный ряд методов для реализации основных функций сетевого сканера, чем в представленной системе.

Литература

1. http://www.3dnews.ru/- 3DNews: Daily Digital Digest.

2. http://www.securitylab.ru/analytics/243179.php Сравнительный анализ сканеров безопасности.

СЛОГ КАК МИНИМАЛЬНАЯ ПРОИЗНОСИМАЯ ЕДИНИЦА

Е.Ф. Щипунов, студент 3-го курса каф. КИБЭВС
ТУСУР, @sibmail.com

Слог – одна из важнейших единиц звукового строя русского языка. Звуки в нашей речи не произносятся отдельно, они взаимосвязаны друг с другом. Каждый звук в слоге взаимодействует с соседними непосредственно. Таким образом, слог представляет собой важный элемент исследований в задачах распознавания и синтеза речи.

Слоги бывают односложные и составные. Односложные конструкции имеют вид: гласный + согласный, согласный + гласный, одиночный гласный и другие подобные конструкции. Составные конструкции имеют вид: согласный + гласный + согласный и другие подобные конструкции. В свою очередь, слоги делятся на открытые (оканчивающиеся гласным), закрытые (оканчивающиеся согласным), прикрытые (начинающиеся с согласного) и неприкрытые (начинающиеся с гласного).

На первый взгляд кажется, что проблем при распознавании слогов нет. Но при детальном изучении слогов можно сделать вывод, что все звуки в таких конструкциях очень тесно связаны между собой. Звуки в слогах искажаются относительно их «чистого» звучания. Это связано прежде всего с механизмами образования речи, а также с особенностями тех или иных звуков.

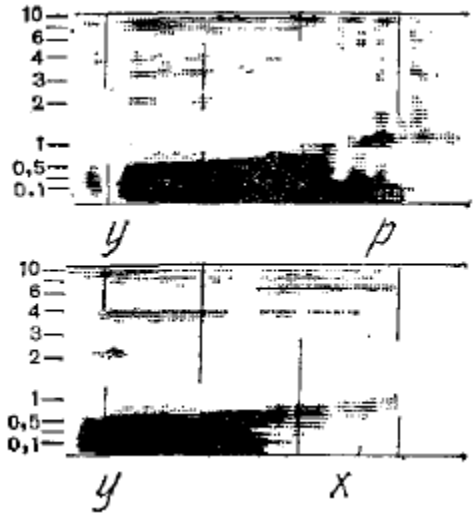
Рассмотрим процесс влияния согласного звука на гласный в закрытом слоге. Для этого приведем спектрограммы выбранных слогов.

На спектрограммах, представленных на рисунке, можем наблюдать, как согласный звук, следуя за огубленным гласным, быстро «освобождается» от влияния гласного звука. Что характерно, в сочетаниях согласный + гласный, согласный звук более сильно подвержен влиянию гласного звука, так как при произнесении такого слога согласный звук как бы предвосхищает гласный звук, тем самым изменяя фонетику гласного звука. В конструкциях гласный + согласный звуки меньше подвержены влиянию друг друга.

Практическая проблема распознавания с применением нейронных сетей заключается в сложности создания универсальной системы, способной реализовывать распознавание различных языковых конструкций. Огромное многообразие звуков русского языка ставит перед исследователями многие задачи, одной из которых является изучение элементарных ячеек, составных частей слов – слогов.

Реализация нейронной сети, распознающей различные типа слогов, может помочь продвинуться на шаг в задачах распознавания речи. Однако эта задача совсем не тривиальная. Встает вопрос о возможных типах слогов, об их комбинациях, характере произношения, стиле речи.

Таким образом, основной проблемой в данной задаче является подбор количества слоев, составляющих нейронную сеть, алгоритмы, согласно которым сеть будет функционировать. Комбинаций слогов может быть очень много. Настолько много, что реализовать все многообразие в рамках одной нейронной сети практически невозможно.



Спектрограммы сочетаний гласного «у» с последующим согласным

Как альтернативу такому методу можно применить системный подход. Исследовательская система позволяет применить при анализе речи совокупность нейронных сетей, заранее обученных на выделенных особо значимых параметрах. Разбивая слоги на несколько групп, каждая из которых будет содержать слоги, объединенные по характерным признакам, получаем возможность реализации такого подхода. На практике это есть ощутимый выигрыш в построении подобных нейронных сетей. Так как, решая несколько более простых задач, предоставляется возможность в полном объеме реализовать каждую из них, а значит, более гибко и грамотно разрешить комплекс поставленных вопросов.

Итак, исходя из вышесказанного, можно сделать следующие выводы. Программировать двухслойный перцептрон на распознавание всех типов слогов является сложной задачей, реализация которой для практического применения маловероятна. Оптимальным вариантом является использование совокупности нейронных сетей, обученных на группах слогов, сгруппированных по единому признаку. Такой подход обеспечивает гибкость и системность при решении задач распознавания речи.

Литература

1. *Бондарко Л.В.* Звуковой строй современного русского языка. М.: Просвещение, 1997.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫДЕЛЕННОМ ПОМЕЩЕНИИ ДЛЯ ПЕРЕГОВОРОВ

И.М. Шагманов, студент 5-го курса КИБЭВС
ТУСУР, г. Томск, shagmanov@yandex.ru

За последние годы отношение к проблеме защиты информации сильно изменилось. Люди стали осознавать, что утечка конфиденциальной информации или информации, содержащей государственную тайну, может привести к серьезным последствиям как для государства в целом, так и для конкретного человека в отдельности. Обеспечение защиты информации является важным направлением в деятельности службы безопасности любого предприятия. Для достижения защиты следует применять меры по ее обеспечению, такие как применение аппаратных, программных и программно-аппаратных комплексов. А также своевременная проверка помещений подлежащих защите. Поэтому необходимо организовывать мероприятия по внедрению технических средств защиты. Для организации защиты техническими средствами необходимо исследование помещения и анализ оборудования необходимый для защиты.

Для обеспечения защиты информации в выделенном помещении необходимо провести тщательный анализ технических каналов утечки информации. Под техническим каналом утечки информации понимают совокупность объекта разведки, технического средства разведки и физической среды, в которой распространяется информационный сигнал.

В выделенном помещении для переговоров основным каналом утечки информации является виброакустический. Под акустической понимается информация, носителем которой являются акустические сигналы. Если источником информации является человеческая речь, то акустическая информация называется речевой. Первичными источниками акустических колебаний являются механические колебательные системы, в том числе и органы речи человека, а вторичными – преобразователи различного типа, главным образом электроакустические.

Средами передачи речевой информации закладными устройствами могут служить радиоканал, оптический канал, сети переменного тока, соединительные линии ВТСС, посторонние проводники (проложенные вблизи кабели, трубы водоснабжения и канализации, металлоконструкции и т.п.). Для передачи информации по трубам и металлоконструкциям могут использоваться также механические ультразвуковые колебания.

При решении задачи обеспечения безопасности помещения необходимо учитывать, что злоумышленник может использовать телефонные и электросиловые линии, проходящие в здании. Электросиловые линии используются для подслушивания разговоров в помещениях, через ко-

торые проходит линия. Как правило, линия используется в качестве источника питания подслушивающих устройств, передающих информацию из помещения по радиоканалу. Линия может использоваться и в качестве проводного канала.

В качестве защиты помещения необходимо применять технические средства защиты, такие как генераторы виброакустических помех, устройства противодействия несанкционированного съема информации по проводным сетям, устройства защиты телефонных линий, а также устройства подавления диктофонов и сотовой связи.

Помимо технических средств защиты следует периодически проверять помещение на наличие закладок. Для этого необходимо использовать различного рода локаторы и поисковые устройства. При обнаружении закладки ее уничтожают или используют для передачи дезинформации.

После анализа помещения необходимо установить требуемое оборудование. В совокупности использование этих устройств должно дать оптимальную защиту помещению, соответствующую требуемой категории информационной безопасности объекта информатизации.

Литература

1. *Зайцев А.П.* Программно-аппаратные средства обеспечения информационной безопасности: Учеб. пособие. В 2 разд. Томск: Том. межвуз. центр дистанционного образования, 2004. Разд. 1. 120 с.

2. *Зайцев А.П., Шелупанов А.А.* Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Томск: Изд-во Том. гос.ун-та систем управления и радиоэлектроники, 2004. 204 с.

3. http://www.irsural.ru – Институт Радиоэлектронных Систем.

4. http://www.evraasgr.ru – Евро-Азиатская ассоциация производителей товаров и услуг в области безопасности.

СТРУКТУРА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ РЕАБИЛИТАЦИИ ОНКОЛОГИЧЕСКИХ БОЛЬНЫХ

И.Е. Щеголев, студент 5-го курса КИБЭВС

ТУСУР, г. Томск, ivvel@mail2000.ru

Рак гортани относится к группе наиболее социально-значимых болезней, так как инвалидизация этой категории пациентов в значительной степени снижает трудовой потенциал общества. Ведущим методом лечения является хирургическое вмешательство, которое приводит к нарушению дыхательной и голосообразующей функций.

Отличительной особенностью ларингэктомированных больных является то, что после операции нарушается естественная система звукообразования. Больной утрачивает способность произносить вокализованные звуки не только в силу отсутствия органа фонации, но также за счет разобщения дыхательного аппарата и речевого тракта. Теряется возможность создавать перепады давления в полости рта, необходимые для произнесения большинства звуков, утрачивается функция экспрессивной речи при сохранности артикуляционного аппарата и нейрофизиологических механизмов речи [1].

В голосообразующем тракте происходят изменения параметров гортани: массы, размера, подвижности органа. Нарушение подвижности голосовых складок или их удаление влечет за собой изменения в речевом сигнале больного. Прежде всего, это отражается на основном тоне, так как частота основного тона по своей сути является частотой колебаний голосовых складок. Таким образом, исследование различных характеристик основного тона может дать информацию об изменениях в гортани. Полученные данные могут использоваться для диагностики заболеваний гортани (в том числе злокачественных новообразований на ранних стадиях), динамического контроля, эффективности лечебного процесса, например, при химиотерапии, а также при голосовой реабилитации.

Очевидно, что одним из решений данной проблемы может быть создание измерительного комплекса (рис. 1), включающего компьютер в качестве базового компонента измерительных комплексов.

На рис. 2 представлена структурная схема программного комплекса по исследованию и обработке речевых сигналов для реабилитации больных с онкологией голосообразующего тракта [2].

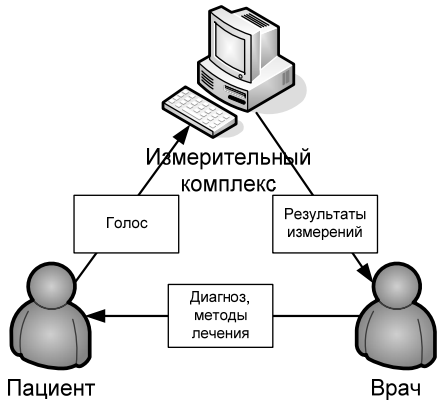


Рис. 1. Измерительный комплекс в медицинских исследованиях

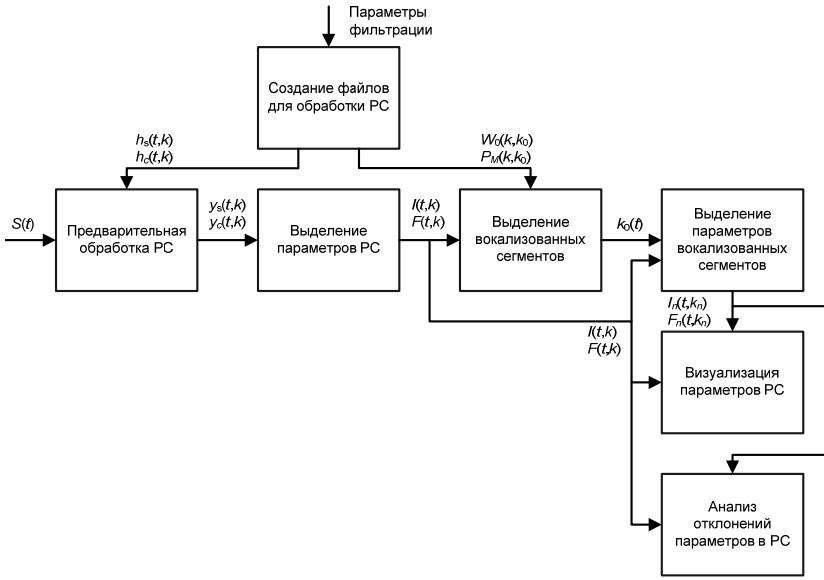


Рис. 2. Структурная схема программного комплекса

Здесь t – время, k – номер канала, $h_c(t, k)$ и $h_s(t, k)$ – импульсные переходные характеристики фильтров для косинусной и синусной составляющих соответственно, W_0 – весовые коэффициенты одновременной маскировки, $P_м$ – набор масок для определения периодической структуры, $S(t)$ – входной сигнал, $F(t, k)$ – мгновенные значения частоты, $I(t, k)$ – интенсивности гармоник частоты основного тона [3].

Блок создания файлов для обработки речевого сигнала предназначен для расчета весовых функций $h_c(t, k)$ (4) и $h_s(t, k)$, $W_0(k, k_i)$, формирования набора масок $P_м(k)$ на основе $W_0(k, k_i)$.

Блок предварительной обработки речевого сигнала предназначен для выполнения свертки речевого сигнала $S(t)$ с весовыми функциями системы фильтров $h_c(t, k)$ и $h_s(t, k)$.

Блок выделения параметров речевого сигнала предназначен для вычисления массива значений интенсивностей $I(t, k)$ и массива значений мгновенных частот основного тона $F(t, k)$.

Блок выделения вокализованных участков речевого сигнала осуществляет одновременную маскировку речевого сигнала, сегментацию речевого сигнала по наличию голосового источника.

Блок выделения параметров вокализованных сегментов речевых сигналов предназначен для определения номеров каналов k_n и вычисления величины девиации частоты основного тона.

Блок визуализации параметров речевого сигнала позволяет сохранять полученные графики как в автоматическом, так и в автоматизированном режиме.

Блок анализа отклонений параметров речевого сигнала содержит следующие модули:

– модуль для выделения средней частоты основного тона;

– модуль для вычисления среднего отклонения первых трех относительных интенсивностей гармоник основного тона;

– модуль анализа исторических данных, позволяющий оценивать динамику протекания заболевания.

Литература

1. *Чойнзонов Е.Л., Мухаммедов М.Р., Балацкая Л.Н.* Рак гортани. Современные аспекты лечения и реабилитации. Томск: Изд-во НТЛ, 2006. 280 с.

2. *Конев А.А., Костюченко Е.Ю., Пономарев А.А.* Программный комплекс для исследования речи. Сб. тр. XVII сессии Российского акустического общества. Т. 3. М.: ГЕОС, 2006. С. 23–27.

3. *Бондаренко В.П., Коцубинский В.П., Мещеряков Р.В.* Адаптивный анализ голосового сигнала // Интеллектуальные системы в управлении, конструировании и образовании. Томск: STT, 2004. С. 58–61.

ПРЕОБРАЗОВАНИЯ ЦИКЛОВ ПРИ ЗАПУТЫВАНИИ ПРОГРАММНОГО КОДА

О.О. Шевцова, аспирант каф. КИБЭВС;
Д.Н. Буинцев, к.т.н., инженер каф. КИБЭВС
ТУСУР, г. Томск, studprof@tusur.ru

Одним из современных подходов в защите кода программных средств является применение методов запутывающих преобразований, в частности преобразования циклов.

Такие подходы в реализации различных видов преобразований мало эффективны по отдельности. Необходимо осуществлять комплексное запутывание, используя реализацию всех преобразований для более эффективного запутывания с минимальным снижением работоспособности программы. При этом задача автоматизации процесса запутывания сводится к автоматизации применений отдельных видов преобразований.

Преобразования графа управления в автоматизированном режиме предложно осуществлять путем избавления от стандартных циклов. Схема «избавления» от циклов представлена в таблице.

Преобразование циклов

Цикл в исходной программе	Преобразованный цикл
FOR	
For i:=1 to n do	i:=1
begin	1:
(тело цикла)	(тело цикла)
End;	i:=i+1; if i<=n then goto 1;
WHILE	
While (условие i<n) do	goto 2;
begin	102:
(тело цикла)	(тело цикла)
End;	2: if i>n then goto 102;
REPEAT	
Repeat	1:
(тело цикла)	(тело цикла)
until (условие i<n)	if not (i<=n) then goto 1;

При реализации преобразований структур данных в автоматизированном режиме предложено производить преобразование, которое объединяет переменные одного типа в массив, что естественно дополняет преобразования циклов.

Преобразования текста программы с помощью введения мертвого кода предлагается проводить в автоматизированном режиме с помощью вставки стандартных циклов (как правило, из существующего набора с использованием вариативной составляющей существующего программного кода). Такого рода преобразования целесообразнее осуществлять перед преобразованием графа потока управления.

Заключение. В результате исследований предложены способы осуществления методов запутывающих преобразований применительно к циклам. В дальнейшем планируется провести оценку применения данных видов преобразований в автоматизированном режиме.

Литература

1. *Мещеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П.* Основы информационной безопасности. Томск: Изд-во ТУСУР, 2001. 350 с.

2. *Чернов А.В.* «Интегрированная среда для исследования «обфускации» программ»: Доклад на конференции, посвященной 90-летию со дня рождения А.А. Ляпунова. Россия, Новосибирск, 8–11 октября 2001 г. http://www.nsc.ru/ws/show_abstract.dhtml?ru+19+2350

МОТИВАЦИОННЫЙ ПОДХОД ПРИ СОЗДАНИИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Р.В. Силиненко студент 5-го курса КИБЭВС
ТУСУР, г. Томск, cisecs@yandex.ru

В настоящее время проблема защиты персональных данных стоит достаточно остро. Автоматизированных систем обработки и передачи персональной информации вокруг становится все больше. Не учитывая таких распространенных примеров как указание своей персональной информации с сети Интернет, в каждой организации любой формы собственности можно обнаружить систему обработки персональных данных.

Согласно федеральным законам «Об информации, информационных технологиях и защите информации» и «О персональных данных» оператор по обработке персональных данных обязан принимать необходимые организационно технические меры, для защиты персональных данных от несанкционированного доступа к ним.

Для защиты персональных данных обычно проводят комплекс мероприятий начинающийся с обследования информационных потоков, выявления потоков, содержащих персональные данные. Далее переходят к составлению списка возможных угроз безопасности и разработке модели нарушителя. На основе полученных сводных данных руководство принимает решение о внедрении тех или иных средств защиты персональных данных. Обычно руководство полагает, что чем дороже программно-аппаратные комплексы, тем качественнее защита информации, и упускает тем самым из вида важный аспект информационной безопасности – мотивационную составляющую. Этот аспект может быть решающим фактором в построении хорошо защищенной среды, даже при применении минимальных материальных ресурсов.

Мотивированные персонала может проводиться по двум путям – принудительно и на добровольной основе. Принудительная или законодательная мотивация довольно проста и заключается в обязательном ознакомлении персонала с нормами законодательного права, положениями по организации и нормами ответственности за нарушение соответствующих положений. Мотивация на добровольной основе представляет довольно большой интерес, так как именно на добровольной основе можно создать сплоченный коллектив способствующий повышению ответственности каждого сотрудника.

В итоге каждый сотрудник вырабатывает систему ценностей и привязанностей. И даже, например, при увольнении он дважды подумает, прежде чем принять деструктивные меры с целью мести.

Данный аспект защиты информации особенно интересен именно при обработке персональной информации, так как эти данные «имеют лицо», что в конечном итоге приводит к тому, что человеку труднее нанести ущерб кому-то конкретному, нежели некой плохой организации, его уволившей.

Что касается получения доступа посторонними лицами, то и здесь предлагается проведение обязательных тренингов, с целью выработки навыков поведения в опасных ситуациях. Под «опасными» понимаются, например, ситуации, когда персоналу звонят на рабочее место, представляются именем начальства (либо от его имени) и просят назвать секретную информацию. Перечни ситуаций составляются на предприятии.

Итак, при проектировании системы защиты персональной информации, наряду с техническими мерами защиты информации, должна быть проанализирована обстановка в коллективе, на предмет взаимоотношений и ответственности работников. На основе полученных данных предлагается создавать системы подготовки персонала к внештатным ситуациям и адаптации личности в коллективе. Данные системы могут в значительной мере уменьшить затраты на создание защищенной системы и одновременно сильно повысить ее устойчивость к негативным воздействиям.

Литература

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Материалы курса Digital Security «Администратор безопасности сети» – «Социально-психологические аспекты защиты информации».

СИСТЕМА ПОЛУЧЕНИЯ И ХРАНЕНИЯ ИНФОРМАЦИИ О ИСТОРИИ БОЛЕЗНИ ОНКОЛОГИЧЕСКИХ БОЛЬНЫХ

В.С. Смагин, студент 5-го курса; В.Н. Щербаков;
Р.В. Мещеряков, к.т.н., доцент КИБЭВС
ТУСУР, г. Томск, 21h@blindage.org

Статья посвящена разработке системы, автоматизирующей процесс ведения истории болезни онкологических больных.

Пользователю системы предоставляется удобный и информативный интерфейс для ввода и поиска информации о больном. Интерфейс каскадного типа и горячие клавиши увеличат производительность врача, высвободив время для работы с пациентом.

Основой программы является ее СУБД Firebird, которая является достаточно быстрой и удобной в использовании, чтобы хранить и обра-

батывать большое количество информации. Подключение происходит через прослойку ODBC, что позволит хранить информацию не только локально, но и на сервере в сети.

Вся информационная структура базы данных состоит из двух частей: информация о пациенте (в том числе и его лечении) и информация о курсе его реабилитации.

Первая часть базы данных содержит в себе личностную, биометрическую, биохимическую информацию, а также информацию о курсе лечения больного. Эта часть представлена четырнадцатью таблицами, объединенными одной большой таблицей. Для экономии времени специалиста, некоторые таблицы хранят в себе сканированные изображения результатов анализов. Этот метод наиболее удобен, так как специалист не должен будет переносить огромное количество цифр в компьютер, а просто укажет изображение для загрузки в базу данных. Конечно же, анализов может быть несколько, поэтому предусмотрен вариант с дополнительным полем «Дата», обозначающий дату сдачи анализа.

В программе созданы таблицы, в которых хранится наиболее часто используемая информация. Например, сопутствующие заболевания выбираются из специальной таблицы. Если такого заболевания нет, то можно его добавить одним щелчком мыши.

Вторая часть базы данных представлена в виде банка данных для работы программы реабилитации больного после хирургического удаления гортани. Цель программы – обучение пациента пищеводному голосу. На этой стадии происходит анализ речевого сигнала. На основе анализа делается предположение, лучше или хуже пациент справляется с заданием. Для работы программы реабилитации в базе данных созданы специальные таблицы для хранения фильтров, записей голоса, сверток и тому подобной информации. Поля таблиц максимально унифицированы для создания возможности последующего расширения функциональности.

Работа с базой данных начинается с появления главного управляющего окна. Специалисту предлагается в меню либо начать работать с карточками пациентов, либо начать занятие по обучению пищеводному голосу. Все карточки пациентов выводятся в отдельном окне, в меню которого можно добавить нового пациента в базу данных, отредактировать информацию об уже существующем или вообще удалить карточку.

При создании новой карточки больного вся информация делится на два раздела (закладки на окне карточки пациента):

1) личностная и биометрическая информация;
2) информация относительно лечения пациента.

В первой закладке предлагается ввести имя, фамилию, отчество, возраст, вес и другие данные общего характера. Вторая закладка предна-

значена для ввода информации о курсах лечения, результатах анализов, сопутствующих заболеваниях.

Занесение данных о прохождении курса реабилитации начинается с окна выбора пациента. Далее начинается занятие, на котором пациент тренируется говорить пищеводным голосом. Программа сообщает пациенту, насколько он приблизился к идеалу. Тренировки проходят вместе со специалистом, что дает положительный эффект, в том числе и психологический. Если у пациента плохо получается, то специалист сможет поддержать его и объяснить, как сделать лучше. Также возможно указать уже готовый файл с записью голоса больного. Специалист сможет отредактировать звуковой файл и поместить его в базу данных программы.

Таким образом, разрабатываемая база данных может быть использована как хранилище информации по текущему состоянию больного, изменению его состояния, включая характеристические параметры речевого сигнала на различных этапах лечения.

МОДЕЛЬ ЗАЩИЩЕННОГО АВТОМАТИЗИРОВАННОГО ПРОЦЕССА МЕЖДУ КЛИЕНТАМИ И СОТРУДНИКАМИ ОРГАНИЗАЦИИ

А.В. Старицын, студент 5-го курса КИБЭВС
ТУСУР, г. Томск, staritsyn@mail.ru

Организация *А* предоставляет услуги для организации *Б* (для организации *А* организация *Б* является клиентом). Организация *А* регистрирует организацию *Б* и ведет учет по зарегистрированной организации.

В основном весь процесс обработки информации происходит вручном режиме и на бумажных носителях.

Например:

− заполнение регистрационной карты (РК) организацией *Б* (РК представлена в твердой копии);

− ручной ввод данных в компьютерную программу;

− ручной ввод данных в компьютерную программу для формирования пакета документов;

− ручной ввод данных в компьютерную программу для формирования других пакетов документов;

− отсутствие в организации *А* общей базы данных (БД).

− Существенные недостатки приведенного процесса:

− организация *Б* может подать регистрационную карту с ошибкой либо не полностью заполненную;

− трудно читаемые данные регистрационной карты (наложение строк при отправке-приеме факса, трудно читаемый почерк);

− данные в программу хранения и обработки данных вносятся вручную;

− невозможность просмотра статистики по зарегистрированным организациям, за приделами компьютера, где обрабатывается информация по организациям.

Приведенные недостатки, как правило, приводят:

− к ошибке при заполнении РК;

− повторному вводу данных;

− затрату времени на процесс обработки данных по одной организации. Время на процесс обработки данных по одной организации, составляет в среднем 20–30 мин (начиная с того момента, когда в организацию *А* поступает РК).

В ходе исследования была построена схема (рисунок) автоматизированного процесса обработки информации по организации *Б* между сотрудниками организации *А*.

Предлагаемый процесс документооборота после исследования:

− Сотрудник организации Б – заполняет регистрационную карту в HTML форме и оправляет ее по протоколу HTTP. Данные, поступившие от клиента, сохраняются в программе обработке данных.

− Сотрудники организации А – ведет работу с данными (например бухгалтерскую), поступившими от организации Б.

− Сотрудники организации А – просматривает статистику по организации Б в защищенном режиме.

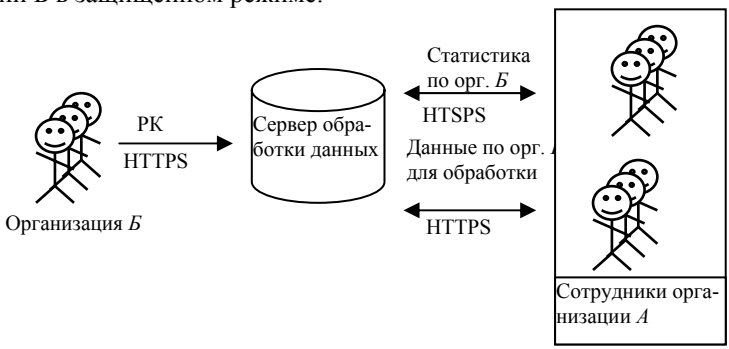


Схема взаимодействия организации *Б* и сотрудников организации *А*

Преимущества предложенной схемы:

− HTML-форма контролирует ввод данных;

− данные, поступившие от организации Б, не искажаются;

− данные с HTML-страницы сохраняются в базе данных;

− возможность просмотра статистики в on-line режиме, по организациям *Б*, за приделами компьютера, где обрабатывается информация по зарегистрированным организациям;

− время, на обработку данных по одному клиенту, составляет в среднем от 5 до 10 мин.

Программный продукт, реализующий предложенную схему, должен основываться:

− на платформе независимости – программа должна разрабатываться на серверных языках программирования(PHP, ASPServer, JavaScript Server, др.); для интерактивного взаимодействия конечного пользователя с программой можно использовать клиентский язык программирования(ASP, JavaScript, др.);

− защищенности каналов передачи информации – веб-сервер должен поддерживать протокол передачи данных HTTPS;

− технологии «тонкий-клиент» – большая часть информации должна обрабатываться на сервере (на сервере обрабатывается конфиденциальная информация), как правило на стороне клиента работают вспомогательные функции (например проверка на ошибочный ввод данных в РК);

− клиент-серверной базе данных – информация должна сохраняться на сервере БД.

Литература

1. *Маклаков С.В.* BPwin и Erwin. CASE-средства разработки информационных систем. М.: ДИАЛОГ-МИФИ, 1999. 256 с.

2. *Быков В.А*. Электронный бизнес и безопасность. М.: Радио и связь, 2000. 200 с.

3. *Кудряев В.А.* Организация работы с документами: Учеб. пособие. М.: ИНФРА-М, 1998. 575 с.

4.*Гудман Д.* JavaScript и DHTML: Сборник рецептов. Для профессионалов. СПб.: Питер, 2004. 523 с.

5. *Котеров Д.В., Костарев А.Ф.* PHP5. СПб.: БХВ-Петербург, 2005. 1120 с.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ВИРТУАЛЬНЫХ СЕРВЕРОВ

Т.В. Степанова, специалист;
И.А. Волков, специалист; М.В. Чуркин, начальник; ОБИТ
ЗАО «Сургутнефтегазбанк», г. Сургут, t.stepanova@sngb.ru

Самое ценное в любой информационной системе, во имя чего она, собственно, и существует, – это хранящиеся в ней данные. Но как бы ни были надежны аппаратные средства, как бы хорошо ни было протести-

ровано программное обеспечение, всегда существует вероятность потери информации. Информация в вычислительных сетях может быть утрачена по следующим причинам (в процентном соотношении):

- аварии аппаратуры и программного обеспечения – 12%,
- ошибки персонала – 75%,
- вирусы – 10%,
- прочие причины (например, злой умысел) – 3%.

В ряде случаев можно предпринять меры, снижающие вероятность потери данных, например, воспользоваться передовыми техническими средствами, позволяющими достаточно надежно защитить информационную систему от аварий аппаратуры. Но даже это не исключает риска потери данных. Кроме того, от ошибок персонала защититься вообще невозможно, ибо они обусловлены самой человеческой природой.

Исходя из всего сказанного, можно сделать вывод, что важной частью мер, направленных на обеспечение надежного функционирования информационных систем, является разработка технологии наиболее быстрого восстановления данных в случае их потери, что позволит свести урон от простоя к минимуму. Решением этой задачи служит создание развитой системы резервного копирования и восстановления данных.

Сервер [server] – служебное устройство, в компьютерных сетях – высокопроизводительная ЭВМ с быстродействующим процессором и большим объемом памяти, обслуживающая другие ЭВМ сети. Служит для организации обмена данными, управления разделяемыми ресурсами, такими, как базы данных, запоминающие устройства, средства связи, принтеры.

По характеру разделяемых ресурсов различают файловые, почтовые, серверы приложений, печати, и т.д.

Виртуальной машиной (англ. virtual machine) называют программную или аппаратную среду, исполняющую некоторый код (например, байт-код, шитый код, p-code или машинный код реального процессора), или спецификацию такой системы.

Зачастую виртуальная машина эмулирует работу реального компьютера. На виртуальную машину, так же как и на реальный компьютер можно инсталлировать операционную систему, у виртуальной машины также есть BIOS, оперативная память, жесткий диск (выделенное место на жестком диске реального компьютера), могут эмулироваться периферийные устройства. На одном компьютере может функционировать несколько виртуальных машин.

Виртуальные машины могут использоваться:

− для защиты информации и ограничения возможностей процессов

− для исследования производительности ПО или новой компьютерной архитектуры

− для эмуляции различных архитектур (например, эмулятор игровой приставки)

− для моделирования информационных систем с клиент-серверной архитектурой на одной ЭВМ (эмуляция компьютерной сети с помощью нескольких виртуальных машин).

− для упрощения управления кластерами – виртуальные машины могут просто мигрировать с одной физической машины на другую во время работы.

Виртуальные машины имеют следующие неоспоримые *преимущества*:

1. Возможность работать одновременно в нескольких системах, осуществлять сетевое взаимодействие между ними.

2. Возможность сделать «снимок» текущего состояния системы и содержимого дисков одним кликом «мыши», а затем в течение очень короткого промежутка времени вернуться в исходное состояние.

3. Простота создания резервной копии операционной системы (не надо создавать никаких образов диска, всего лишь требуется скопировать папку с файлами виртуальной машины).

4. Возможность иметь на одном компьютере неограниченное число виртуальных машин с совершенно разными операционными системами и их состояниями.

5. Отсутствие необходимости перезагрузки для переключения в другую операционную систему.

Тем не менее, несмотря на все преимущества, виртуальные машины также имеют и свои *недостатки*:

1. Потребность в наличии достаточных аппаратных ресурсов для функционирования нескольких операционных систем одновременно.

2. Операционная система работает несколько медленнее в виртуальной машине, нежели на «голом железе». Однако, в последнее время показатели производительности гостевых систем значительно приблизились к показателям физических ОС (в пределах одних и тех же ресурсов), и вскоре, за счет улучшения технологий реализации виртуальных машин, производительность гостевых систем практически будет равна реальным.

3. Различные платформы виртуализации пока не поддерживают полную виртуализацию всего аппаратного обеспечения и интерфейсов. В последнее время количество поддерживаемого аппаратного обеспечения стремительно растет у всех производителей платформ виртуализации. Помимо основных устройств компьютера, уже поддерживаются сетевые

адаптеры, аудиоконтроллеры, интерфейс USB 2.0, контроллеры портов COM и LPT и приводы CD-ROM. Но хуже всего обстоят дела с виртуализацией видеоадаптеров и поддержкой функций аппаратного ускорения трехмерной графики. В этом плане впереди всех находится компания VMware с экспериментальной поддержкой функций Direct 3D (однако некоторые важные функции, такие как Vertex-шейдеры все еще не поддерживаются). Но в ближайшем будущем эта проблема, безусловно, будет решена.

Все перечисленные недостатки виртуальных машин являются в принципе разрешимыми и, по сравнению с большим списком их достоинств, являются не столь существенными. Именно поэтому, виртуальные машины развиваются взрывными темпами, а пользователи находят им все новые и новые применения.

Наиболее известные виртуальные машины:

– Java Virtual Machine Forth
– IBM zVM
– VMWare Workstation
– VMWare ESX Server
– Microsoft VirtualPC и т.д.

Если использовать виртуальные машины на своих рабочих станциях, можно создавать их резервные копии путем копирования папки с файлами виртуальной машины. Учитывайте, что файл конфигурации виртуальной машины настоятельно рекомендуется хранить в той же папке, что и виртуальный диск, который будет создан позднее, а значит, на диске, на котором вы сохраните файл, должно быть достаточно места для установки гостевой ОС. В случае краха системы, сохраненную копию не надо восстанавливать – она уже полностью готова к работе. К тому же многие платформы виртуализации позволяют создавать несколько снимков состояния виртуальной машины, откат к каждому из которых может быть произведен за несколько минут.

В заключение можно сделать вывод, что повышенная гибкость виртуальных систем и их независимость от оборудования позволяют обеспечить повышенную надежность хранения данных, удобство использования и простоту развертывания.

РАЗРАБОТКА КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПРЕДПРИЯТИЯ ОАО ‹‹СУРГУТНЕФТЕГАЗ›› ТРЕСТ СНДСР

А.И. Титаренко, студент 5-го курса КИБЭВС
ТУСУР, г. Томск,

Трест «Сургутнефтедорстройремонт» является структурным подразделением ОАО «Сургутнефтега» и относится к нефтепромышленной группе предприятий.

Основной функцией треста является строительство, реконструкция, капитальный и текущий ремонт и содержание мостов, дорог и дорожных сооружений, контроль качества при осуществлении дорожной деятельности.

Объектом исследования является организация ОАО «Сургутнефтегаз» трест СНДСР г.Сургут.

Для данной системы :

1) построена полная модель системы на основании реальных данных;
2) все ресурсы, на которых хранится ценная информация;
3) все сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);
4) произведен анализ информированных рисков и угроз;
5) средства защиты информации;
6) предложены средства предотвращения информационных рисков и угроз;
7) предложены рекомендуемые мероприятия по нейтрализации угроз;

Была предложена политика обеспечения информационной безопасности:

1. Документы по информационной безопасности.
2. Требования безопасности к информационной системе.
3. Инструкции по обеспечению защищенности информационной системы:

– инструкция по действиям в случае наступления нештатных ситуаций и ликвидация последствий;
– инструкция по приему на работу и увольнение сотрудников имеющих доступ к информационной сети;
– инструкция по антивирусной защите;
– инструкция по организации парольной защиты;
– инструкция по порядку работы с базами данных;
– инструкция о резервном копировании информации;

– инструкция по безопасному уничтожению информации и оборудования;

Проделанная работа позволила провести анализ информационной системы предприятия и выявить основные недостатки в обеспечении защищенности своих ресурсов, выработать контрмеры по усилению слабых сторон защиты и основные документы, направленные на упорядочивание действий сотрудников при работе с информационными ресурсами.

Литература

1. *Мещеряков Р.В., Шелупанов А.А., Белов Е.П., Лось В.П.* Основы информационной безопасности. ТУСУР, 2002.

2. *Белов Е.Б., Лось В.П, Мещеряков Р.В., Шелупанов А.А.* Основы информационной безопасности. Учеб. пособие для вузов. М.: Горячая линия – Телеком, 2006. 544 с.

3. *Шумский А.А*. Системный анализ в защите информации: Учеб. пособие для студентов вузов. М.: Гелиос АРВ, 2005. 224 с.

4. *Степанов Е.А., Корнеев И.К.* Информационная безопасность и защита информации: Учеб. пособие. М.: ИНФРА-М, 2001. 304 с.

5. Международный стандарт безопасности ISO 17799.

АРХИТЕКТУРА СИСТЕМЫ ИССЛЕДОВАНИЯ ПРИЛОЖЕНИЯ НЕЙРОСЕТЕЙ К РЕЧЕВОМУ АНАЛИЗУ

С.Д. Тиунов, студент 3-го курса каф. КИБЭВС

ТУСУР, t5d@ms.tusur.ru

В статье будет дан обзор созданной архитектуры, предназначенной для исследования возможностей нейросетей в работе с речевой информацией. Эта система была создана в рамках ГПО по теме «Искусственный интеллект в задачах анализа и синтеза речи».

Целью создания архитектуры было то обстоятельство, что обучение нейросетей средствами MATLAB (именно этот пакет использовался для моделирования) достаточно автоматизировано и производится одним вызовом функции. Однако подготовка примеров для обучения занимает достаточно много времени и перед каждой подготовкой включает в себя некоторые общие элементы, которые замедляют процесс исследования, и как следствие производительность исследовательской группы падает.

Другими словами, исследовательская система должна максимально автоматизировать работу группы и сконцентрировать внимание ее участников на цели исследования, а не на рутинной его части.

Перед созданием архитектуры был выявлен ряд факторов, определивших ее:

– система должна быть спроектирована таким образом, чтобы способствовать исследовательской работе и максимально исключать рутинную ее составляющую.

– имеет место постоянная необходимость исследователя в обучении нейросетей, обучение нейросетей влечет за собой необходимость подготовки примеров для обучения, что является трудоемкой задачей.

– достаточно трудоемким процессом является подготовка примеров для обучения. Эта задача невыполнима без участия человека, парадигма обучения с учителем (именно она используется в проекте) требует этого участия.

Эти факторы позволили определить основные архитектурные требования к системе (или задачи системы):

– исследовательская система должна быть надстройкой над выходным программным продуктом. Это позволит группе тратить меньше времени на завершение проекта, а сконцентрироваться на исследовании.

– система нуждается в базе данных. Это очень удобный вариант автоматизации процесса выбора примеров для обучения.

– как следствие, база данных должна хранить только те данные, которые объективно необходимы для процесса исследования. Так, например, обученные нейросети, которые являются частью выходного программного продукта, должны храниться отдельно.

– система должна предоставлять интерфейс для подготовки примеров на обучение. (Примеры должны автоматически сохраняться в базе данных).

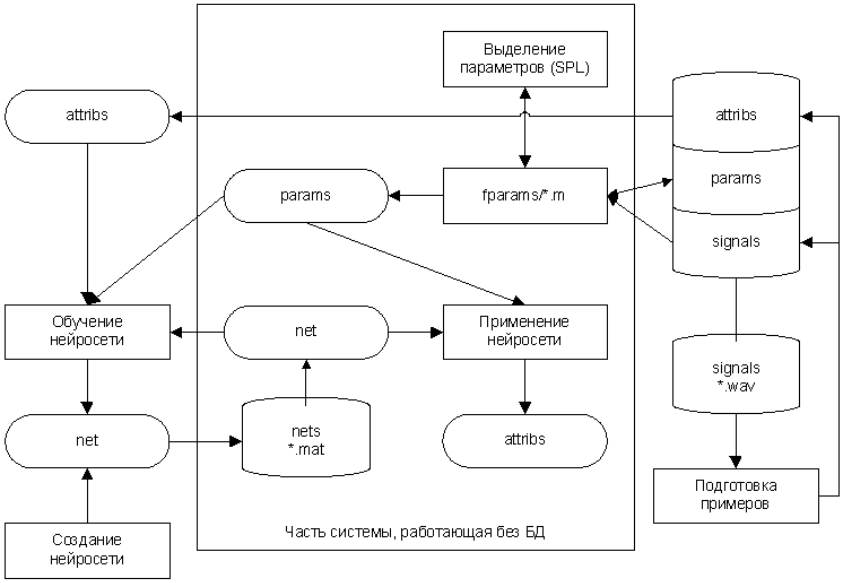
– как следствие, от системы требуется поддержка синхронизации участников.

– система должна предоставлять интерфейс для быстрого создания, обучения и использования нейросетей с заданными входными параметрами и выходными атрибутами.

Можно предложить очевидную архитектуру основы: имеются файлы с нейронными сетями, система должна принимать на вход нейронную сеть и звуковой сигнал и давать на выходе результат работы нейронной сети.

Перед передачей сигнала на нейронную сеть необходимо выделить параметры сигнала, которые ей требуются. Для этого будет использоваться разработанная ранее библиотека выделения параметров (SPL), основанная на алгоритмах, описанных в [1]. После выделения параметров они объединяются и подаются на вход нейронной сети. Выход нейронной сети интерпретируется и отображается пользователю программы.

Базируясь на этом «каркасе» далее была разработана архитектура исследовательской системы. Упомянутые выше задачи нашли в ней свое отражение. Архитектура изображена графически на рисунке.



Архитектура исследовательской системы

Прямоугольниками на рисунке показаны функциональные блоки системы, скругленными прямоугольниками – временные данные, цилиндрами – постоянные хранилища данных, большой цилиндр показывает базу данных. Также показана граница системы, которая будет основой для прикладной программы.

Параметры и атрибуты нейронной сети должны быть зарегистрированы в базе данных. Также база данных содержит соответствие кусков определенных звуковых сигналов атрибутам и выделенные для этих кусков параметры. Причем, выделением атрибутов в базе данных занимается человек, а выделение параметров протекает по мере необходимости автоматически.

Каждому параметру соответствует его название. Это название также определяет одноименную процедуру в папке fparams проекта, которая для заданного куска сигнала вычисляет соответствующий параметр.

Такой подход позволяет автоматизировать подготовку и выборку примеров для обучения нейросети. Подготовка примеров облегчается в

том смысле, что человек должен показать лишь соответствие атрибутов кускам сигналов, а параметры выделяются автоматически. Выборка примеров выполняется автоматически и облегчается в том смысле, что выделенные параметры сохраняются в базе данных и при следующем требовании могут быть быстро извлечены.

Литература

1. *Bondarenko V.P., Kornilov A.U., Choynzonov, E.C. Balackaya L.N.* The automatized rehabilitation of oncological patients with larynx cut out. Proceedings 'SPECOM'2005': 10-th International Conference Speech & Computer– Patras, 2005. P. 707–711.

ПРОБЛЕМЫ ПОСТРОЕНИЯ СИСТЕМЫ РАСПОЗНАВАНИЯ РЕЧИ И ЕЕ ДИКТОРОНЕЗАВИСИМОСТИ

С.Д. Тиунов, студент 3-го курса каф. КИБЭВС
ТУСУР, t5d@ms.tusur.ru

Согласно акустической теории речеобразования источник сигнала и передающий тракт независимы друг от друга. При этом источник имеет свой спектр, а передающий тракт – свою передаточную характеристику. Эта передаточная характеристика соответствует положению артикуляторных органов и, следовательно, произносимому звуку. Одной из важнейших характеристик передающего тракта являются форманты – частоты резонансов передающего тракта. Также известно, что каждому звуку, который растянут во времени, соответствует достаточно определенные частоты формант. [1]

Именно передаточная характеристика, а более точно – частоты формант являются целью при попытке построения системы распознавания речи. Однако наличие источника сигнала и передающего тракта затрудняет задачу анализа формант – характеристик передающего тракта. Для того, чтобы выделить форманты, необходимо устранить влияние спектра источника на передаточную характеристику, а для этого, в свою очередь, нужно сделать предположение о форме спектра источника.

В данном эксперименте было сделано предположение об экспоненциальном убывании интенсивности гармоник источника сигнала и на основе этого был получен параметр спектра, который позволял оценить положения формант и/или интенсивность в областях формант.

На основе параметра была построена нейронная сеть, задачей которой было распознавание гласных букв (*и, ы, э, а, о, у*). При обучении нейронной сети на примерах чистых звуков одного диктора оказалось, что, несмотря на очень маленький размер параметра (5–8 чисел), были

достигнуты результаты, не уступающие нейронным сетям, основанным на нескольких «больших» параметрах, таких как одновременная маска по каналам анализа, канал с максимальной интенсивностью и других, не имеющих непосредственное отношение к положениям формант. Этот факт означает полезную информативность такого параметра.

Однако, обучившись на чистых звуках, такая нейронная сеть столкнулась с двумя проблемами. Первая проблема заключается в том, что приложение нейронной сети к реальному речевому сигналу (например, фразе) закончилось неудачей: нейронная сеть не смогла различить гласные в спектре. Это объясняется прежде всего тем, что в фразах гласные звуки не являются чистыми. Большинство звуков являются безударными, а они отличаются нечеткостью, быстротой произношения. В английской фонетике даже выделен специальный звук – безударный гласный. В русской прикладной фонетике также есть подобный звук – Z [2].

Также вследствие инертности артикуляторного аппарата человека предшествующая гласному звуку согласная вносит в его спектр дополнительные изменения. Так, после мягких согласных спектр любой гласной похож на спектр гласной И, а предшествующие гласным звуки Л, М, Н добавляют в спектр звука форманту назализации [1].

Эту проблему можно попытаться решить путем обучения нейронной сети на звуках из реальных сигналов. При этом следует обратить внимание на разнообразие речевого материала, этого требуют вышеописанные и многие подобные факторы.

Другая проблема заключается в том, что при смене диктора нейронная сеть дает неправильную оценку (при подаче чистого звука). Так, при подаче звука А на нейронную сеть на ее выходе были подняты флаги А и И, а при подаче звука О – флаги А и О.

Стоит, однако, заметить, что уже упомянутые работающие на других параметрах нейронные сети, которые были обучены для одного диктора, были вообще неустойчивы к смене диктора. Например, они могли давать противоположные значения для разных участков одного и того же звука. Полученная же нейронная сеть может дать неправильный, но уверенный ответ, и это ее очевидный плюс.

При обучении системы распознавания речи под диктора можно эмпирически (например, с помощью тестовой фразы) узнать типичные положения формант для определенных звуков и в дальнейшем распознавать звуки по этим формантам. Для дикторонезависимой системы распознавания речи это неверно, так как форманты каждого человека индивидуальны. Это приводит к проблемам нахождения более универсальных параметров.

С другой стороны, для распознавания речи будет достаточно грубой оценка нейронной сети. Например, если для данного звука нейронная сеть укажет флаги А и О, то необходимое слово можно подобрать по словарю.

Этот факт можно также использовать для построения «нечетких» нейронных сетей. Можно обучать нейронную сеть на реальных примерах, где человек будет давать экспертную оценку звуку. При этом допускается несколько флагов (И/Э, И/Ы, и т.д.).

Дальнейшее изучение предполагает расширение «словаря» нейронной сети: добавление сонантов (л, м, н), а также невзрывных согласных (имеющих равномерную по времени мощность), попытку обучения нейронных сетей для нескольких дикторов и проверку их для других дикторов, попытку обучения нейронной сети на звуках шепота (где отсутствует вокализация сигнала – это будет способствовать обобщению нейронной сети) и, наконец, нахождение параметров и их сочетаний, которые будут иметь хорошие качества для задач обработки речи.

Литература

1. *Бондарко Л.В.* Звуковой строй современного русского языка. М.: Просвещение, 1977.

2. *Михайлов В.Г., Златоустова Л.В.* Измерение параметров речи. М.: Радио и связь, 1987.

СИСТЕМА АВТОРИЗАЦИИ С ИСПОЛЬЗОВАНИЕМ USB FLASH DRIVE

М.А. Толстоногов, Д.А. Окрушко, студенты 5-го курса каф. КИБЭВС

ТУСУР, г. Томск, drhawk@sibmail.com, okrushko@sibmsil.com

В настоящее время, как правило, используется метод авторизации, в котором применяется пара «логин + пароль». Данный метод имеет ряд проблем: достаточно легко перехватить данные идентификации и аутентификации; при аутентификации пользователи часто испытывают неудобства и совершают ошибки, что делает возможным получение данных идентификации и аутентификации с помощью социальной инженерии; наличие данных идентификации и аутентификации делает необходимым их распространение среди пользователей, что усложняет их работу; пользователь может забыть логин или пароль; логин и пароль можно достаточно просто подсмотреть при вводе; данные авторизации возможно перехватить различными программами – шпионами и так далее.

Разрабатываемая система предназначена для решения этих проблем. Пользователю больше нет нужды придумывать, запоминать, хранить,

вводить свои идентификационные данные, вся необходимая информация находится на его персональном USB Flash Driver (ключ). Весь процесс авторизации автоматизирован, пользователю остается только вставить ключ и запустить предлагаемую программу. Отличие данной системы состоит в том, что в качестве ключа используется обычный flash-носитель, тогда как другим подобным системам приходится применять специальное устройство token.

Система использует метод аутентификации без передачи знаний на основе алгоритма шифрования ГОСТ 28147-89. Система состоит из двух частей: клиентская и серверная, клиентская часть системы доступна каждому пользователю, а серверная устанавливается и настраивается на объекте, к ресурсам которого зарегистрированный пользователь хочет получить доступ.

Регистрация. Для регистрации клиенту необходимо скачать клиентскую часть системы на свой USB Flash Drive и запустить программу в режиме регистрации. Программа считает уникальный номер носителя информации и вычислит его хеш-значение по алгоритму ГОСТ Р 34.11-94. Далее считанный уникальный номер модифицируется (добавляется случайное число) и еще раз вычисляется хеш-значение, которое будет отличаться от первоначального. Оба хеш-значения вместе с данными пользователя (ФИО, должность и т.д.) отправляются на сервер и помещаются в базу данных.

Авторизация. Пользователь устанавливает ключ и запускает предлагаемую программу (клиентскую часть системы) в режиме авторизации, программа считывает уникальный номер USB Flash Drive и модифицирует его таким же способом, как и при регистрации, далее модифицированный номер преобразовывается в хэш-значение и отправляется на серверную часть системы.

На сервере при получении хэш-значения (полученного из модифицированного номера) система определяет открытый ключ (хеш-значение оригинального номера), которому сопоставлен принятый идентификатор в базе данных, затем система генерирует случайное число и отправляет его к клиенту. Если идентификатор не найден в базе данных сервера, то клиенту отправляется отказ.

Приняв отправленное сервером число, клиентская часть генерирует из открытого ключа (хеш-значения оригинального номера) таблицу перемен 8×15 с числами от 0 до 15, которая будет являться закрытым ключом и шифрует случайное число, полученное от сервера, алгоритмом шифрования ГОСТ 28147-89. Зашифрованные данные клиентская часть системы отправляет на сервер.

После получения шифртекста серверная часть системы генерирует из открытого ключа такую же таблицу перемен, какую генерировала клиентская программа при зашифровывании данных. Таким образом, серверная программа обладает как открытым ключом, так и таблицей перемен (закрытым ключом), с помощью этих данных система расшифровывает полученные данные и сравнивает результат с изначально сгенерированным числом. Если числа равны, то сервер принимает решение об авторизации пользователя, иначе отправляется отказ. Таким образом, происходит авторизация пользователей с нулевой передачей знаний.

Данная система является неким компромиссом в противоречии между удобством пользователя и безопасностью авторизации. Во-первых, пропадает необходимость постоянного ввода аутентификационной информации, тем самым пользователь освобождается от соблюдений строгих правил использования и хранения своего идентификаора и аутентификатора. Во-вторых, работа алгоритма данной системы является максимально безопасной, ведь через каналы передачи данных не передаются данные, необходимые для авторизации, закрытые ключи не покидают пределы программ, на которых они используются, этот метод делает бессмысленным перехват и замену авторизационных данных.

АЛГОРИТМЫ И МЕТОДЫ ЗАЩИТЫ ПРОГРАММ ОТ ИЗУЧЕНИЯ

В.И. Удалов, студент 5-го курса КИБЭВС
ТУСУР, г. Томск,

Системы защиты программного обеспечения (ПО) широко распространены и находятся в постоянном развитии, благодаря расширению рынка ПО и телекоммуникационных технологий. Поэтому необходимость использования систем защиты программ от взлома и изучения обусловлена рядом причин:

– незаконное использование алгоритмов, являющихся интеллектуальной собственностью автора, при написании аналогов продукта (промышленный шпионаж);

– несанкционированное использование программного обеспечения (ПО) (кража и копирование);

– несанкционированная модификация ПО с целью внедрения программных злоупотреблений;

– незаконное распространение и сбыт ПО (пиратство).

Для защиты ПО используются следующие методы:

– алгоритмы запутывания – используются хаотические переходы в разные части кода, внедрение ложных процедур – «пустышек», холостые

циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и т.п.

– методы затруднения дизассемблирования – используются различные приемы, направленные на предотвращение дизассемблирования в пакетном режиме.

– методы, затрудняющие работу отладчиков – используются различные приемы, направленные на усложнение отладки программы.

– эмуляция процессоров и операционных систем – создается виртуальный процессор и/или операционная система (не обязательно реально существующие) и программа-переводчик из системы команд IBM в систему команд созданного процессора или ОС, после такого перевода ПО может выполняться только при помощи эмулятора, что резко затрудняет исследование алгоритма ПО.

– алгоритмы навесной защиты (протекторы) – специальные программы, предназначенные для защиты других программ от взлома.

Однако идеального способа защиты не существует, в связи с этим разработчики защитных систем не стремятся лишить потенциального взломщика самой возможности нейтрализации защиты, но стараются максимально усложнить этот процесс. Поэтому необходимо решить проблему – качественной защиты от изучения. Какие бы ни применялись алгоритмы защиты ПО, их стойкость к обратной инженерии определяет стойкость всей системы защиты в целом.

Сегодня на рынке существует большое количество коммерческих защит, однако многие из них давно взломаны. Зачастую их подводит именно слабая защищенность от изучения. После анализа взломщиком алгоритмов работы защиты, серийные ключи генерируются, аппаратные – успешно эмулируются. Ситуацию могла бы исправить разработка эффективного метода защиты ПО от изучения, применяя который к алгоритмам других защит, можно было бы качественно поднять их уровень.

Приведем сравнительный анализ всех описанных выше алгоритмов в виде таблицы. В качестве критериев были выбраны:

– основной принцип работы алгоритма;

– методы анализа;

– достоинства метода;

– недостатки метода;

– эффективность защиты.

Средняя эффективность защиты означает, что злоумышленник с малым запасом знаний не сможет преодолеть данную защиту. Однако высококвалифицированный специалист сможет ее преодолеть. Высокая эффективность защиты – это нетривиальная задача для специалиста, имеющего хорошие знания и опыт в работе с архитектурой целевой машины.

Сравнительный анализ алгоритмов защиты программ от изучения

Алгоритм защиты	Методы затруднения дизассемблирования	Методы, затрудняющие работу отладчиков	Алгоритмы запутывания	Протекторы	Виртуальный процессор
Основной принцип	Шифрование	Отслеживание прерываний *int1 и int3*	Разброс участков кода по разным областям ОЗУ и т.п.	Преобразование исполняемого файла и добавление своего кода в файл	Программа компилируется под виртуальный процессор
Методы анализа	Использование дизассембера	Трассировка; контрольные точки останова	Синтаксические; Статические; Динамические; Статистические;	Расшифровка кода программы; Получение оригинальной точки входа; Удаление кода протектора	Изучение архитектуры симулятора, симулируемого процессора и создание дизассемблера
Достоинства	Невысокая стоимость реализации	Невысокая стоимость реализации	Усложняет процесс изучения программ	Создание версий с ограничениями	Стоимость взлома сильно большая
Недостатки	Применяемые методы хорошо известны взломщикам	Против эмулирующих отладчиков методы бессильны	Не существует ни одного метода запутывания, которое нельзя было распутать	Существуют методы, позволяющие успешно преодолевать протекторы	Скорость работы ниже, чем кода оригинального
Эффективность защиты	Средняя	Средняя	Средняя	Средняя	Высокая

В результате получаем, что использование комбинированных методов защиты позволит сделать защиту ПО от взлома и изучения более стойкой к атакам исследователей. Таким образом, применяя запутываю-

щие преобразования и протекторы, можно достигнуть большей защищенности ПО.

Литература

1. *Скляров Д.* Искусство защиты и взлома информации. М.: ИД Мир безопасности. 1997. 112 с.

2. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и Техника, 2004.

3. *Касперски К.* Техника отладки программ без исходных текстов. СПб.: БХВ-Петердург, 2005. 832 с.

4. *Хогланд, Грег, Мак-Гроу, Гари*. Взлом программного обеспечения: анализ и использование кода: Пер. с англ. М.: Изд. дом «Вильяме», 2005. 400 с. Парал. тит. англ.

ИНФОРМАЦИОННАЯ ВОЙНА

Н.В. Власов, студент 5-го курса каф. КИБЭВС
ТУСУР, г. Томск, vnv@sibmail.com

Информационная война – целенаправленные действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем.

В настоящее время с развитием технологий, информационная война выглядит все более актуальной. Информационная война выступает как составная часть военного противоборства, при этом используются любые средства воздействия на информационную сферу противоборствующей стороны.

Объектом информационного противоборства является любой объект, в отношении которого возможно осуществление информационного воздействия (в том числе – применение информационного оружия) либо иного воздействия (силового, политического, экономического и т.д.), результатом которого будет модификация его свойств как информационной системы.

Общим признаком объекта, который можно рассматривать как объект информационного противоборства, является любая форма использования информации в его функционировании.

− родовые объекты информационного противоборства:
− система социальных отношений информационного общества;
− система политических отношений информационного общества;

Субъекты информационного противоборства:

− государства, их союзы и коалиции;

− международные организации;

− негосударственные незаконные (в том числе – незаконные международные) вооруженные формирования и организации террористической, экстремистской, радикальной политической, радикальной религиозной направленности;

− транснациональные корпорации;

− виртуальные социальные сообщества;

− медиа-корпорации (контролирующие средства массовой информации и массовой коммуникации – СМИ и МК);

− виртуальные коалиции.

Мною разрабатывается модель поведения злоумышленника (контрагента) в ходе незаконного проникновения на охраняемую зону, с целью выявить слабые места и попытаться организовать более сильную систему защиты.

Для моделирования такого состояния системы используем математическую теорию рефлексивных игр. Для этого выделим следующие параметры:

− множество агентов;

− множество предпочтений агентов (конечные состояния информационных подсистем в общем информационном поле);

− множество допустимых действий агентов (множество информационных операций, применительно к каждой из информационных подсистем общего информационного поля);

− информированность агентов (информация, которой обладают агенты на момент принятия решений и которая образуется в результате экономически оправданных атак на информационные ресурсы контрагентов), в том числе представления агентов о представлениях друг друга.

Делая соответствующие предположения о рациональности действий агентов, находим точку равновесия игры, т.е. точку, отклонение от которой не выгодно ни одной из сторон. В результате приходим к следующему определению безопасного состояния системы:

– состояние системы безопасно, если управляющее устройство может обеспечить необходимый уровень LI-управляемости в точке равновесного состояния игры, а соответствующая стратегия управляющего устройства называется стратегией информационной безопасности.

Литература

1. *Панарин И.Н.* Информационная война и геополитика.

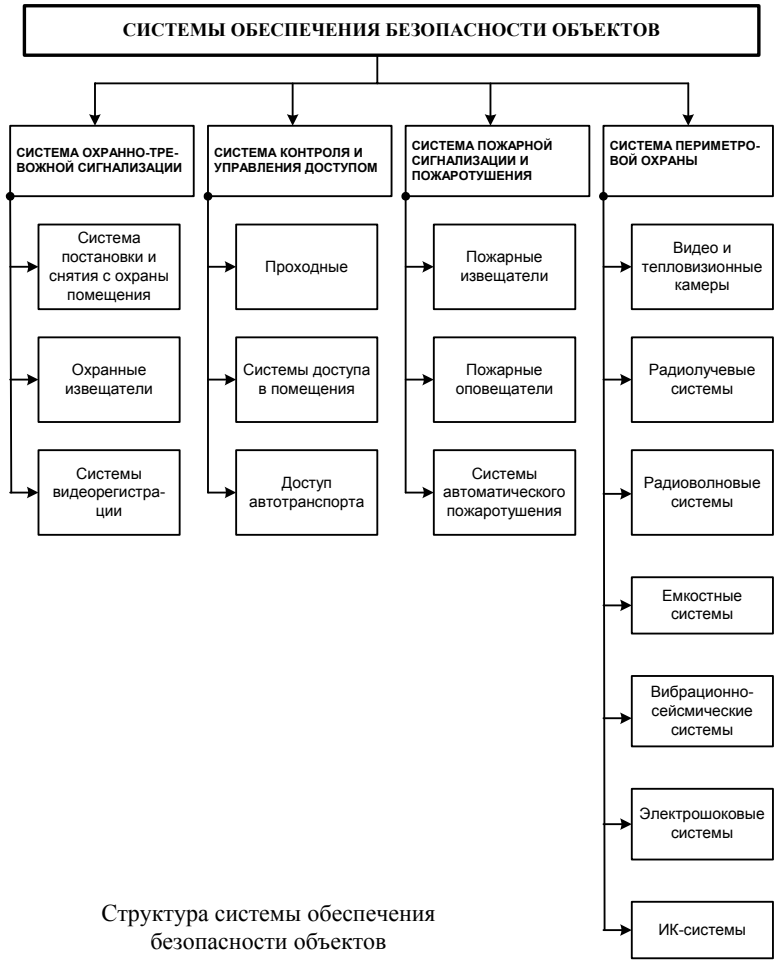
2. *Стюгин М.А.* Статья по моделированию стратегии информационной безопасности. http://psyfactor.org/lib/infowar1.htm.

3. *Расторгуев С.П.* Информационная война.

КОМПЛЕКСНАЯ ОХРАНА ПРЕДПРИЯТИЯ

М.Г. Власова, студентка 5-го курса КИБЭВС
ТУСУР, г. Томск, margo108@bk.ru

Физические средства представляют собой первую линию защиты информации и элементов вычислительных систем, и поэтому обеспечение физической целостности таких систем и их устройств является непременным условием защищенности информации. Развитию и внедрению физических средств защиты уделяется большое внимание в ведущих зарубежных странах, а в последнее время и в России.



Структура системы обеспечения безопасности объектов

Основные задачи, решаемые физическими средствами:

1. Охрана территории.
2. Охрана оборудования и перемещаемых носителей информации.
3. Охрана внутренних помещений и наблюдение за ними.
4. Осуществление контролируемого доступа в контролируемые зоны.
5. Нейтрализация наводок и излучений.
6 Препятствия визуальному наблюдению.
7. Противопожарная защита.
8. Блокирование действий злоумышленника.

Целью проделанной работы являлись анализ и исследование физических средств, обеспечивающих безопасность объекта для комплексной охраны предприятия. В самых общих чертах структура системы обеспечения безопасности объектов может содержать элементы и системы, показанные на рисунке. В конкретных случаях в зависимости от специфики объектов какие-то элементы структурной схемы могут отсутствовать, а какие-то другие – присутствовать.

Проанализировав все существующие физические средства, было принято решение выбрать в качестве основы комплексной охраны предприятия прибор приемно-контрольного охранно-пожарного (ППКОП) «Рубеж-08». Данный прибор применяется для организации систем охранной, тревожной и пожарной сигнализации, управления исполнительными устройствами контроля доступа, технологической сигнализации, автоматического пожаротушения. Все указанные системы интегрируются на уровне оборудования и функционируют независимо от наличия ПЭВМ, что обеспечивает высокую надежность безопасности в целом.

По результатам исследования был собран материал достаточный для разработки комплексной охраны предприятия, и сделан вывод о неоспоримом преимуществе ППКОП «Рубеж-08» по сравнению с другими приборами.

Литература

1. *Зайцев А.П.* Курс лекций. 177 с.

2. Научно-производственная фирма «Сигма – Интегрированные Системы». www.sigmais.ru

3. www.description.sec.ru

4. Журнал «Системы безопасности». www.secuteck.ru

АРХИТЕКТУРА ЗАЩИЩЕННОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ

В.Д. Зыков, аспирант КИБЭВС
ТУСУР, г. Томск, zvd@udcs.ru

Современные информационные технологии играют важнейшую роль в медицинской отрасли, но одной из наиболее серьезных проблем, препятствующих их повсеместному внедрению, является обеспечение защиты информации, в том числе защиты персональных данных граждан и сведений, составляющих врачебную тайну – персональных медицинских данных. Актуальность проблемы защиты персональных медицинских данных сегодня не вызывает сомнений. Кибертерроризм, доступ физических лиц к базам персональных данных усиливают риск вторжения в сферу частной жизни и нарушения права на ее неприкосновенность. Защита персональных медицинских данных является одной из наиболее острых проблем в информатизации организаций медицинской области.

27 июля 2006 г. был принят Федеральный закон «О персональных данных» [1]. Согласно ст. 19 ч. 1 этого нормативного акта «оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».

Предлагаются комплексное решение по защите персональных медицинских данных, в качестве базовой составляющей использующее инфраструктуру открытых ключей, и реализация следующих услуг по защите информации:

1. Идентификация и аутентификация обеспечивается сертификатами открытых ключей.

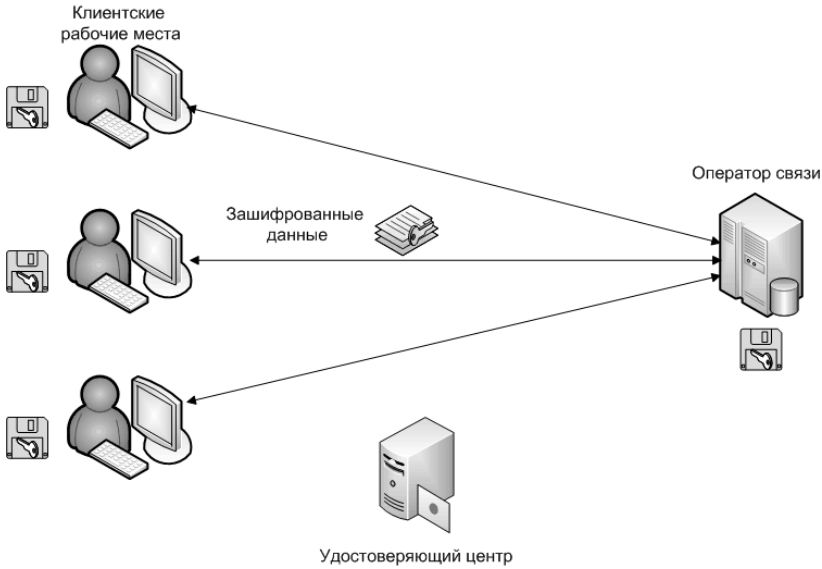
2. Конфиденциальность и контроль доступа обеспечивается шифрованием.

3. Контроль целостности обеспечивается электронной цифровой подписью.

4. Неотказуемость – услуга, предотвращающая успешный отказ от предшествующих действий пользователя, обеспечивается использованием ЭЦП и сертификата открытого ключа [2].

В предлагаемом случае комплексное решение по защите персональных медицинских данных на основе инфраструктуры открытых ключей

включает в себя следующие организационно-технические компоненты (рисунок):



Компоненты решения по защите персональных медицинских данных

– клиентские рабочие места, на которых осуществляется сбор, обработка, хранение и передача персональных медицинских данных;

– оператор связи, обеспечивающий выполнение функций передачи, промежуточного хранения персональных медицинских данных и информационной поддержки документооборота;

– автоматизированная информационная система, включающая программно-аппаратные средства защиты информации на основе инфраструктуры открытых ключей;

– удостоверяющий центр, обеспечивающий выполнение функций выпуска и управления сертификатами открытых ключей пользователей;

– защищенные средства для хранения цифровых сертификатов и закрытых ключей пользователей. В качестве таких средств могут выступать USB-ключи, смарт-карты, внешние носители и др.;

– каналы передачи информации.

Автоматизированная информационная система в данном случае будет иметь клиент-серверную архитектуру.

Очевидно, что предложенное комплексное решение устанавливает защищенную среду функционирования персональных медицинских дан-

ных, а также удовлетворяет требования Федерального закона «О персональных данных». В настоящее время данный проект по защите персональных медицинских данных реализуется на базе лечебно-профилактических учреждений города Томска.

Литература

1. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. *Зыков В.Д.* Требования к системам защищенного электронного документооборота // Научная сессия ТУСУР-2007.

ЗАЩИТА ОТ УГРОЗ СО СТОРОНЫ ПОЛЬЗОВАТЕЛЕЙ С МАКСИМАЛЬНЫМИ ПРИВИЛЕГИЯМИ ПРИ ХРАНЕНИИ И ПОИСКЕ ИНФОРМАЦИИ В БАЗАХ ДАННЫХ

П.В. Волченков; С.В. Запечников, к.т.н, доц.

МИФИ, г. Москва, vpv@mephi.edu

В задачах, связанных с хранением и поиском информации в базах данных (БД), современные системы управления базами данных (СУБД) и сети хранения данных (СХД) интенсивно используют средства криптографической защиты информации (СКЗИ). При построении комплексных решений для защиты информационных систем СКЗИ в частности применяются для решения следующих задач:

1) шифрования БД с целью защиты конфиденциальной информации от стороннего нарушителя;

2) вычисления и проверки кодов аутентификации (MAC) записей БД с целью контроля целостности и подлинности информации;

3) контроля доступа к записям БД на основе аутентификации субъектов компьютерной системы по признаку обладания некоторым ключевым материалом: паролями, секретными ключами на смарт-картах или жетонах и др.;

4) генерации и проверки ЭЦП клиентскими и серверными компонентами СУБД при удаленном доступе к БД;

5) выполнения протоколов безопасного поиска и восстановления информации из БД (PIR – Private Information Retrieval).

Для успешного решения этих и других задач в СУБД (СХД) требуется, в частности, построение некоторой структуры ключевой системы (КС). КС включает, как правило, ключевой материал трех уровней иерархии:

1) мастер-ключи, доступные пользователям с максимальными привилегиями;

2) ключи защиты ключей, используемые для обеспечения безопасности ключевого материала всех остальных пользователей, сами защищаемые посредством мастер-ключей;

3) ключи обработки данных, используемые для защиты пользовательской информации, сами защищаемые ключами более высокого уровня иерархии.

Максимально уязвимы к атакам противника мастер-ключи, для которых отсутствует возможность защиты криптографическими методами. Методы защиты мастер-ключей от внешнего злоумышленника (противника) достаточно хорошо отработаны: их безопасность может быть обеспечена за счет комплекса организационных, физических, аппаратных, программных и иных мер защиты. Вместе с тем требуют решения и задачи защиты мастер-ключей от внутреннего нарушителя – пользователей с максимальными привилегиями, которыми обычно являются администраторы компьютерной системы или лица, исполняющие обязанности администраторов безопасности информационной системы (СУБД, СХД). В связи с тенденцией к неуклонному возрастанию стоимости содержащейся в БД информации, увеличению объема хранимых данных возрастает риск, связанный с нарушением конфиденциальности ключевого материала СКЗИ.

Конфиденциальность ключа k на непрерывном временном интервале λ определим как свойство ключа *k*, заключающееся в том, что его значение в произвольный момент времени τ в течение временного интервала λ известно только владельцам ключа и неизвестно никому более. Конфиденциальность ключа, в отличие от доступности или аутентичности, не является объективно фиксируемой величиной.

Предположим, что противник может нарушать конфиденциальность отдельных компонентов ОКС (иными словами, ключи могут быть скомпрометированы противником), что не может обнаруживаться системными средствами СКЗИ, способен выполнять любые полиномиально ограниченные алгоритмы и, кроме того, имеет доступ к применяемым в СКЗИ алгоритмам симметричного и открытого шифрования как к «черным ящикам». Вероятность успеха противника, т.е. вероятность того, что противнику в некоторый момент времени τ в течение временного интервала λ станет известно значение *k*, обозначим $\gamma(k, \lambda)$, считая, что она постоянна на данном временном интервале. Если эта вероятность зависит от времени, то в качестве $\gamma(k,\lambda)$ примем ее максимальное значение на интервале λ. Назовем $\gamma(k, \lambda)$ *показателем конфиденциальности* ключа *k* на временном интервале λ.

Как показано в [1], показатель конфиденциальности криптографического ключа определяется следующим уравнением:

$$\gamma(k,\lambda)=1-\left(1-p_{\text{ПДК}}(k)\right)\cdot\prod_{i}\left(1-p_i(k,\lambda)\cdot p_{\text{НСП}}(k)\right),$$

в котором p_i – вероятности атак противника различными способами: i= 1 – вероятность случайного угадывания ключа, i = 2 – вероятность восстановления ключа из функционально зависимых ключей, i = 3 – вероятность восстановления ключа из последовательности изменяющихся во времени значений ключа, i = 4 – вероятность восстановления ключа из последовательности изменяющихся во времени значений функционально зависимых ключей, а $p_{\text{ПДК}}(k)$ – вероятность прямого доступа противника к ключу – определяется по формуле:

$$p_{\text{ПДК}}(k)=p_{\text{ПДК}}\left(k^{(n)}\right)=1-\prod_{(j)}\left(1-p^{(j)}_{\text{ПДК}}(k)\cdot p^{(j)}_{\text{обх}}(k)\right),$$

где $p^{(j)}_{\text{ПДК}}$ – вероятность прямого доступа к j-му экземпляру ключа, $p^{(j)}_{\text{обх}}$ – вероятность «обхода» противником механизма аутентификации, n – количество экземпляров ключа в СКЗИ.

Одним из рациональных способов повышения стойкости мастер-ключей СУБД и СХД к нарушению конфиденциальности является применение к ним пороговых схем разделения секрета (СРС). Обозначим через k^{TSS} ключ, разделенный на доли с помощью (m,n)-пороговой СРС. Можно показать, что для них

$$\gamma\left(k^{\text{TSS}},\lambda\right)=1-\left(1-p_1(k)p_{\text{НСП}}(k)\right)\cdot\left(1-p_{\text{НСП}}(k)\cdot\left(1-\sum_{l=0}^{m-1}C_n^l\left(\gamma(s,\lambda)\right)^l\left(1-\gamma(s,\lambda)\right)^{n-l}\right)\right),$$

где k – исходный ключ, s – доли разделенного ключа, $p_{\text{НСП}}(k)$ – вероятность несанкционированного применения ключа. Обозначим: $R=1-p_1(k)p_{\text{НСП}}(k)$. Если дополнительных мер по контролю доступа к ключу не предпринимается, $p_{\text{НСП}}(k)=1$, а $p_1(k)=1/|D(k)|$, где $D(k)$ – область допустимых значений ключа. Отсюда $R=1-1/|D(k)|$. При предположении о том, что суммарная интенсивность μ атак противника, приводящих к нарушению конфиденциальности k, до и после применения (m,n)-пороговой СРС не изменяется, отношение показателей конфиденциальности ключевого материала на временном интервале длины $|\lambda|$ при примененной к нему СРС и без таковой будет равно

$$K^{TSS}=\frac{1-R\cdot\sum_{l=0}^{m-1}C_n^l\left(1-e^{-\mu|\lambda|}\right)^l\left(e^{-\mu|\lambda|}\right)^{n-l}}{1-R\cdot e^{-\mu n|\lambda|}}\approx\frac{1-\sum_{l=0}^{m-1}C_n^l\left(1-e^{-\mu|\lambda|}\right)^l\left(e^{-\mu|\lambda|}\right)^{n-l}}{1-e^{-\mu n|\lambda|}}.$$

Применение СРС приводит к повышению конфиденциальности ключа, если $K^{TSS}<1$. Полученная формула позволяет численными методами определять величины n и m, требуемые для достижения заданного показателя $\gamma(k, \lambda)$ и синтезировать КС соответствующей структуры.

Литература

1. *Запечников С.В.* Принципы обеспечения стойкости криптосистем к компрометации ключей // Безопасность информационных технологий. 2008. № 1. 7 с.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМЫ ДИРЕКТУМ

И.А. Волков, специалист ОБИТ ЗАО «СНГБ»
i.volkov@sngb.ru

Для обеспечения электронной цифровой подписью пользователей СЭД «Директум» был развернут корпоративный удостоверяющий центр ЗАО «СНГБ». Его работа организована на базе удостоверяющего центра представленного в операционной системе Windows 2000 server. Выполнение криптографических функций как на стороне сервера, так и на стороне клиента реализовывалось с использованием встроенного в данную операционную систему криптопровайдера Microsoft Enhanced Cryptographic Provider v.1, технические параметры которого представлены в таблице.

Каждый пользователь, который имеет право подписи в СЭД «Директум», должен сгенерировать ключевую пару и получить соответствующий сертификат ключа подписи. Генерация ключевой пары производится пользователем самостоятельно с использованием соответствующего сервиса УЦ по средствам веб-интерфейса.

Параметры используемого криптопровайдера

Алгоритм	Значение
RSA ключи подписи	1024 бита
RSA ключи обмена	1024 бита
RC2 размер блока шифрования	128 бит
RC4 размер блока шифрования	128 бит
DES	56 бит
TripleDES (2 ключа)	112 бит
TripleDES (3 ключа)	168 бит

После генерации ключевой пары пользователь отправляет администратору заявку на сертификат в бумажном виде (распечатанная веб-

форма, отображаемая при запросе на сертификат). Администратор, рассмотрев заявку, производит процедуру одобрения выдачи сертификата на сервере УЦ, и распечатывает его аналог на бумажном носителе.

Каждый пользователь, допущенный к работе в корпоративной сети, имеет свой личный сетевой ресурс, на данный ресурс администратор УЦ копирует сертификат пользователя в электронном виде, также на данный сетевой ресурс записывается файл, содержащий закрытый ключ, данная процедура осуществляется пользователем в процессе генерации ключевой пары.

Бумажный носитель сертификата подписывается начальником отдела безопасности информационных технологий в двух экземплярах и отправляется пользователю. Пользователь, подписав оба, один отправляет обратно в отдел безопасности информационных технологий.

Следующим и последним шагом пользователя на пути получения возможности ЭЦП документов в СЭД «Директум» является импорт сертификата ключа подписи и ключевой пары. Эта процедура выполняется посредством специально написанного для этих целей пакетного файла.

Данный пакетный файл реализует две функции: создание из файлов сертификата и закрытого ключа подписи ключевого контейнера и импорта его в локальное хранилище используемого криптопровайдера.

Пользователь, после того как получил и отправил в отдел безопасности информационных технологий подписанный собственноручно сертификат на бумажном носителе, импортирует ключевой контейнер и сертификат в локальное хранилище криптопровайдера по средствам пакетного файла.

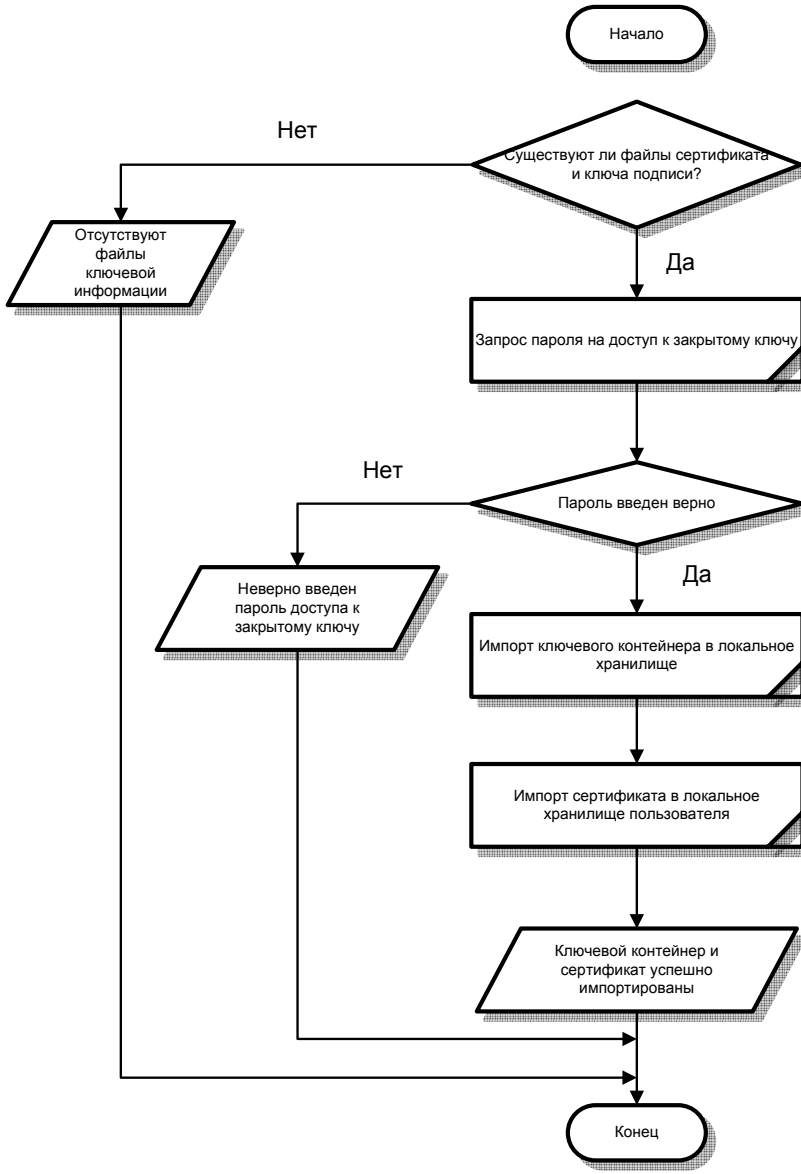
Доступ к закрытому ключу ограничивается паролем, задаваемым пользователем на этапе генерации ключевой пары, а также правами доступа к файловой системе файл-сервера. Введенный пароль запрашивается при импорте ключевой пары и сертификата в хранилище.

Импорт ключа и сертификата осуществляется следующим алгоритмом:

1. Проверка наличия файлов сертификата и ключевого контейнера в личной папке пользователя на сетевом ресурсе.
2. Запрос пароля на доступ к закрытому ключу.
3. Импорт ключевого контейнера.
4. Импорт сертификата.

Блок-схема данного алгоритма представлена на рисунке.

Разработанная система в полной мере позволяет обеспечить полнофункционирующий защищенный документооборот и его защиту с использованием современных организационно-технических решений.



Блок-схема алгоритма работы пакетного файла

ВЕРИФИКАЦИЯ ЗНАНИЙ С ИСПОЛЬЗОВАНИЕМ ПОЛИГРАФА

А.И. Юдин, студент 5-го курса КИБЭВС
ТУСУР, г. Томск, maddog_1@mail.ru

Весной 2006 г. специалисты компании ЗАО «Поликониус-Центр» начали очень интересное исследование, связанное с созданием интеллектуальной программы анализа психофизиологических реакций, регистрируемых в ходе проведения опросов с использованием полиграфа, с помощью нового подхода, основанного на применении современных нейросетевых технологий. Основные пути подхода к решению данной задачи были описаны в статье «Интеллектуальный полиграф». Исследования проводились совместно со специалистами ГУВД Пермского края и группой ученых из Пермского отделения Научного совета РАН по методологии искусственного интеллекта.

К сожалению, реализация алгоритма 3-й очереди потребовала от разработчиков несколько больше времени, чем предполагалось вначале. Алгоритм, обеспечивающий заявленную точность, может быть реализован только после проведения большого объема дополнительных исследований. Такие исследования пришлось временно приостановить, и вот по каким причинам.

На удивление быстро меняется отношение к полиграфу в нашей стране. За последнее время значительно участились обращения со стороны коммерческих компаний с просьбами организовать кадровые проверки сотрудников и кандидатов на работу с целью выявления так называемых факторов риска, наличие которых несовместимо с работой в данной компании, или для оказания помощи при проведении служебных разбирательств. По всей вероятности, в дальнейшем эта тенденция будет только расти.

Руководство фирм, использующих полиграфные проверки, уже давно убедилось в их эффективности, на таком предприятии повышается дисциплина и, как следствие, производительность труда, уменьшаются кражи и различные финансовые махинации, сотрудники, как ни странно, начинают с большим доверием относиться друг к другу.

По мере увеличения таких обращений, естественно, увеличивается и количество людей, которым приходится знакомиться с процедурой тестирования на полиграфе. А если исходить из постулата, что безгрешных людей просто не бывает, то каждая такая проверка для испытуемого, пусть даже самого лояльного по отношению к своей компании, является очень нежелательной.

В то же время следует заметить, что по мере возрастания объема доступной информации о методологии детекции лжи через возможности

Интернета или большое количество выпускаемых в настоящее время книг, возрастает и уровень подготовленности обследуемых. Все чаще в ходе тестирования на вопрос: «Вам известно что-нибудь о детекторах лжи?» – вспоминают не только актера Ножкина в роли Бекаса из известного фильма, а поясняют, что «такую проверку проходить уже приходилось ранее», или что «читал о методе и более менее представляю саму процедуру тестирования». А если при этом испытуемый читал о каких-нибудь методах противодействия и пытается их применить, а еще если ему действительно есть, что скрывать, у полиграфолога тут же начинаются проблемы с диагностикой полученных результатов.

Таким образом, на традиционных полиграфах проводить обследования, будь то скрининговые проверки или служебные разбирательства, становится все труднее. Отсюда вывод – по мере совершенствования испытуемыми приемов противодействия полиграфу необходимо совершенствовать как сам полиграф, так и методы выявления попыток противодействия, а также приемы т.н. контрпротиводействия, обеспечивающие пресечение попыток его применения.

Прежде всего, следует подчеркнуть, что проблема противодействия полиграфу является исключительно серьезной, так как представляет опасность не только точности и надежности результатов конкретных обследований, но и имиджу профессии в целом, что самым непосредственным образом может сказаться на ее будущем. По разным оценкам, до 70% лгущих обследуемых лиц, скрывающих свою вину или причастность к расследуемым событиям, в той или иной форме пытаются противодействовать.

О важности проблемы противодействия свидетельствует, например, и тот факт, что все основные члены Разведывательного сообщества США, наиболее активно использующие полиграф, такие как INSCOM (Intelligence and Security Command), AFOSI (Air Force Office of Special Investigation), NIS (Naval Investigative Service), а также Министерство обороны США, ФБР, Secret Service и многие другие, проводили и проводят закрытые исследования эффективности различных приемов противодействия полиграфу и способов контрпротиводействия им. Особенно важно подчеркнуть, что к этим исследованиям привлекались наиболее известные психофизиологи и специалисты в области использования полиграфа, такие как Дэвид Раскин, Давид Ликкен, Чарльз Хонтс (ведущий эксперт в США по проблеме противодействия полиграфу) и многие др.

Перечисленные проблемы, ставшие на сегодня особенно актуальными, породили необходимость разработки комплекса аппаратно-программных средств и методических приемов, которые позволили бы хотя бы отчасти решить поставленную задачу.

Что касается известных видов противодействия, то они наиболее подробно описаны в [2]. В зависимости от выбираемых способов воздействия на динамику физиологических показателей используемые приемы принято разделить на психические, физические, физиологические, фармакологические и прочие «экзотические».

К настоящему времени в компании завершена работа над созданием системы, обеспечивающей выявление большинства из указанных видов противодействия. Такая система включена в состав нового полиграфа «Диана-02», который наряду с другими дополнительными тактическими возможностями обеспечивает гораздо большую по сравнению с предыдущей моделью, эффективность работы полиграфолога, т.е. повышение надежности его заключений при снижении времени на подготовку к тестированию и анализ полученных данных.

После выпуска нового полиграфа исследования по созданию нейросетевой системы анализа данных будут продолжены.

Литература

1. *Забатова А.Н., Петров А.М., Сичинава З.И., Сошников А.П., Ясницкий Л.Н.* Российский полиграф № 1 // М. 2006. С. 76–83.

2. *Варламов В.А., Варламов Г.В.* Противодействия полиграфу и пути их нейтрализации. М.: ПЕР СЭ-Пресс, 2005. 192 с.

МЕЖСЕТЕВЫЕ ЭКРАНЫ В ТЕХНОЛОГИИ VipNet – КАК СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ

О.В. Жувагин, студент 5-го курса каф. КИБЭВС

ТУСУР, г. Томск, mave@security.tomsk.ru

В данной статье рассматриваются схемы включения межсетевых экранов в сеть, а также некоторые аспекты уязвимостей данного способа защиты информации.

Межсетевые экраны – наиболее защищенные устройства. Однако даже они не обладают абсолютной невосприимчивостью к атакам. Некоторые межсетевые экраны строятся поверх обычных операционных систем, таких как Windows или UNIX, и поэтому могут быть уязвимы для всех обычных атак уровня ОС. Даже если операционная система межсетевого экрана является собственной, в ней могут существовать уязвимости. Многие межсетевые экраны взаимодействуют с пользователями при помощи web-сервера, а значит, могут быть использованы дыры в web-интерфейсе. Обеспечение собственной безопасности этих средств передовой линии обороны критически важно и должно считаться одним из высших приоритетов.

Межсетевые экраны имеют также свойство обеспечивать безопасность, которая «тверда снаружи, мягка внутри». Это означает, что через них трудно проникнуть извне, но против атак изнутри сети почти никакой защиты не предусматривается. Нужно добиться, чтобы внутренние системы были по крайней мере минимально защищены, а безопасность не зависела целиком и полностью от межсетевых экранов.

Очень часто из уст многих отечественных разработчиков средств VPN можно услышать, что разработанное ими средство построения виртуальных частных сетей способно решить многие проблемы безопасности. Они упирают на то, что раз защищаемая сеть общается со своими оппонентами (удаленными офисами, партнерами, заказчиками и т.д.) только по VPN-соединению, то никакой вирус в нее не проникнет. Отчасти это так, но только при условии, что и оппоненты также ни с кем не общаются по незащищенным каналам. А это уже представить себе трудно. И поскольку большинство организаций используют шифрование для защиты внешних сетевых соединений, интерес злоумышленника будет направлен к тем местам в сети, где информация, представляющая для него интерес, вероятно, не является защищенной, т.е. к узлам или сетям, с которым установлены доверенные отношения. И даже в случае создания VPN-соединений между сетью, защищаемой при помощи МСЭ с функциями VPN, и доверенной сетью злоумышленник сможет с той же эффективностью реализовывать свои атаки. Мало того, эффективность его атак будет еще выше, поскольку зачастую требования по безопасности к доверенным узлам и сетям намного ниже всех остальных узлов. Злоумышленник сможет проникнуть в доверенную сеть, а уж затем из нее осуществлять свои несанкционированные действия по отношению к цели своей атаки.

Наиболее простым является решение, при котором межсетевой экран просто экранирует локальную сеть от глобальной. При этом почтовый сервер и другие сервера, оказываются также защищены межсетевым экраном (рис. 1).

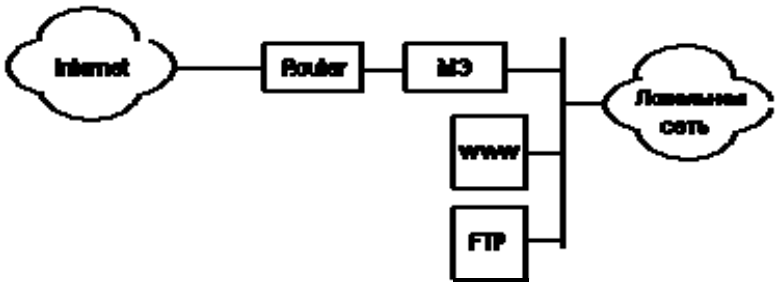


Рис. 1. Простое включение МЭ

Для предотвращения доступа в локальную сеть, используя ресурсы WWW-сервера, рекомендуется общедоступные серверы подключать перед межсетевым экраном (рис. 2).

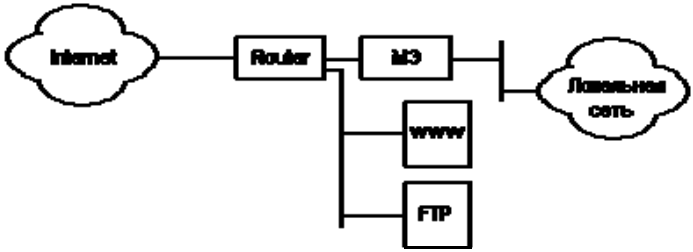


Рис. 2. Подключение МЭ с вынесением общедоступных серверов

Развитие глобальных сетей привело к увеличению количества пользователей и увеличению количества атак на компьютеры, подключенные к Сети. Многие из этих являются непреднамеренными, но нет никакой гарантии, что единственной угрозой для локальной сети организации являются потенциальные атаки из внешней сети. Поэтому необходимо помнить о том, что существует возможность воздействия на защищаемую информацию и внутри локальной сети. Оценки ежегодных потерь, связанных с недостаточным уровнем защищенности, достигают десятков миллионов долларов ежегодно, поэтому, планируя подключение локальной сети к мировым глобальным сетям, не стоит забывать о безопасности информации.

Литература

1. *Лукацкий А.В.* Способы обхода межсетевых экранов, Научно-инженерное предприятие «Информзащита» //
http://www.citforum.ru/internet/securities/obhod.shtml

2. *Осовецкий Л.* Построение средств межсетевой защиты информации, НТЦ «Критические Информационные Технологии» //
http://www.citforum.ru/internet/iinet97/6.shtml

3. Технология VipNet. http://www.infotecs.ru

ПРОСЛУШИВАНИЕ СЕТИ

О.В. Жувагин, студент 5-го курса каф. КИБЭВС
ТУСУР, г. Томск, mave@security.tomsk.ru

В данной статье приведены способы прослушивания сетевого трафика на программно-аппаратном уровне с кратким описанием каждого из них.

Прослушивание сетевого трафика может использоваться по разным причинам, но цель у него одна – отслеживать все происходящее на определенном участке в сети. Это может быть как мониторинг сети с целью выявления тех или иных нюансов в штатном режиме работы, так и обнаружение сетевых атак. Реализация прослушивания может быть осуществлена несколькими способами:

1. Программная реализация на одном из штатно используемых узлов. Например, можно запустить tcpdump, windump и далее наблюдать за выводимой ими информацией. Этот способ хорош отсутствием дополнительных затрат, но плох тем, что, во-первых, потребляются ресурсы процессора, во-вторых, прослушивание трафика можно отследить и обойти. В-третьих, на разных платформах используются разные программы, порой несовместимые между собой даже по формату.

2. Использование отдельного компьютера для перехвата трафика совместно с коммутаторами, имеющими порт для мониторинга или концентраторами.

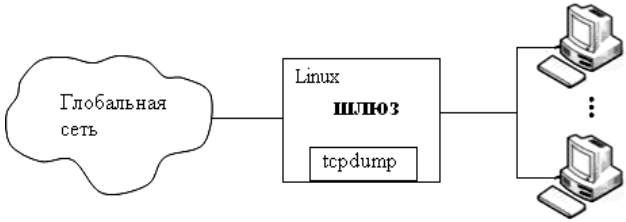


Рис. 1. Схема прослушивания сетевого трафика на базе шлюза

В разрыв исследуемого участка сети ставится коммутатор или концентратор, а уже к нему подключается отдельный компьютер, занимающийся анализом прошедшего трафика. Данный способ не зависит от других компьютеров в сети и используемого ими программного обеспечения.

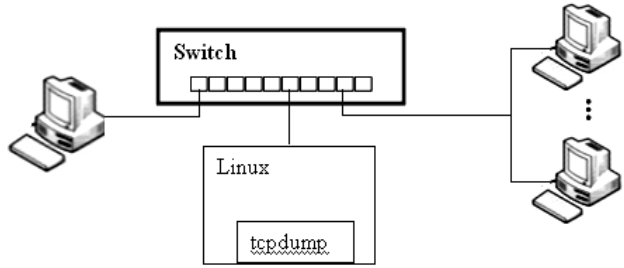


Рис. 2. Схема с использованием отдельного компьютера

3. Использование отдельного компьютера в мостовом включении на исследуемом участке. Этот способ несколько лучше предыдущего тем, что при желании можно организовать не только пассивный просмотр трафика, но и фильтрацию и подмену, т.е. влиять на проходящий трафик.

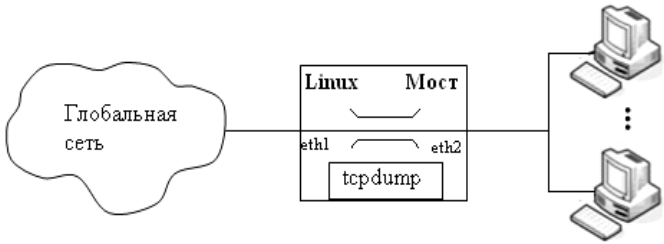


Рис. 3. Схема использования моста

Отличие от первого способа состоит в том, что работа с трафиком ведется на более низком уровне (на канальном, против сетевого в случае шлюза). Как следствие, стандартными средствами вроде traceroute удаленно обнаружить факт подключения (прослушивания и фильтрации) невозможно.

4. Использование пассивного подключения к кабелю без его разрыва на физическом уровне.

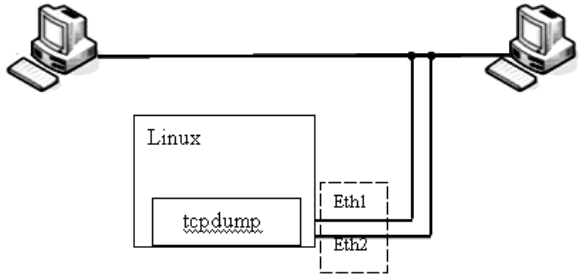


Рис. 4. Схема пассивного подключения

Используется совместно с компьютером для обработки перехваченных данных. Так как физический уровень самый низкий из всех, то обнаружить такое подключение на канальном уровне и выше практически невозможно. Правильнее будет сказать, что программно такое подключение обнаружить нельзя.

С точки зрения скрытного перехвата первый способ однозначно не подходит, так как программу, осуществляющую просмотр трафика можно обнаружить и отключить. Даже если она хорошо спрятана и обнаружить ее не получается, можно отформатировать винчестер и установить систему заново.

Второй способ, как и третий, легко обнаружить физически. Лишний бесхозный концентратор и/или компьютер быстро найдутся и привлекут к себе внимание, если их не спрятать в отдельной комнате. Оборудование «посередине» может зависнуть. В случае использования разных по скорости сетевых карт или разных режимов работы может оказаться, что

одна карта работает в режиме 100 Мбит/с в полном дуплексе, а составляющая ей пару на другом конце провода умудряется работать со скоростью 10 Мбит/с без дуплекса. Отключив кабель с одной стороны, можно долго удивляться тому, как на другой стороне индикатор «link» почему-то светится и не гаснет, и наоборот. Подозрение сразу перейдет на кабель, а простое подергивание его с любой стороны от загадочного места внутри стены рано или поздно приведет к «секретной комнате» и перехват будет обнаружен.

Четвертый способ пассивного перехвата при правильной реализации обнаружить довольно сложно, но возможно, например, измерив нагрузку на проводе и сделав соответствующие выводы.

Литература

1. Системный администратор. 2004. Ноябрь.

2. *Мамаев М., Петренко С.* Технологии защиты информации в Интернете. Специальный справочник.

СОДЕРЖАНИЕ

СЕКЦИЯ 10
АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

СЕКЦИЯ 12
МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Научное издание

Научная сессия ТУСУР-2008

Материалы
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
5–8 мая 2008 г., Томск, Россия
В пяти частях

Часть 3

Тематический выпуск
«Системная интеграция и безопасность»

Корректор – **А.И. Корчуганова**
Верстка **В.М. Бочкаревой**
Дизайн обложки **В. Глушко**

Издательство «В-Спектр»
Сдано на верстку 01.04.2008. Подписано к печати 25.04.2008.
Формат $60\times84^{1}/_{16}$. Печать трафаретная.
Печ. л. 15,5. Усл. печ. 14,6.
Тираж 150 экз. Заказ 19.

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