Федеральное агентство по образованию

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

ТУСУР – 45 лет

КИБЭВС – 35 лет

НАУЧНАЯ СЕССИЯ ТУСУР-2007

Материалы докладов
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР-2007»
3–7 мая 2007 г.

В пяти частях

Часть 2

Тематический выпуск
«Системная интеграция и безопасность»

В-Спектр
Томск 2007

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

Научная сессия ТУСУР-2007: Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. **Тематический выпуск «Системная интеграция и безопасность»:** Томск, 3–7 мая 2007 г. – Томск: Изд-во «В-Спектр», 2007. Ч. 2. – 234 с.

Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых посвящены различным аспектам разработки, исследования и практического применения радиотехнических, телевизионных и телекоммуникационных систем и устройств, 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.

Конференция проводится при поддержке
ЦС РНТОРЭС им. А.С. Попова
Посвящается 45-летию ТУСУР

ISBN 5-91191-034-9978

ISBN 5-91191-036-5978 (Ч. 2)

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

Всероссийская научно-техническая конференция студентов и молодых ученых «Научная сессия ТУСУР-2007» 3–7 мая 2007 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 оптики 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

Ремпе 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.

Представители фонда Бортника (по согласованию), г. Москва

Конференция **«Научная сессия ТУСУР-2007»** вошла в число аккредитованных мероприятий по Программе «Участник молодежного научно-инновационного конкурса» (УМНИК) Фонда содействия развитию малых форм предприятий в научно-технической сфере (МП НТС) при поддержке Роснауки и Рособразования (Фонд Бортника)

(http://www.fasie.ru/index.php?rid=125).

Экспертным комитетом конференции при работе секции «УМНИК» 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 3 по 7 мая 2007 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 **3 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***

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. РАСПРЕДЕЛЕННЫЕ 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. АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ – *председатель* ***Раводин Олег Михайлович,*** *д.т.н., профессор каф. КИБЭВС; зам. председателя* ***Давыдова Елена Михайловна,*** *к.т.н., ст. преподаватель каф. КИБЭВС*

Секция 10. 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 10.1 ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ПРОЕКТИРОВАНИЯ ТЕХНИЧЕСКИХ УСТРОЙСТВ – *председатель* ***Черкашин Михаил Владимирович,*** *к.т.н., ст. преподаватель каф. КСУП*

Подсекция 10.2 АДАПТАЦИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ИМИТАЦИИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ – *председатель* ***Коцубинский Владислав Петрович,*** *зам. зав. каф. КСУП, к.т.н., доцент*

Подсекция 10.3 ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ПОДДЕРЖКИ СЛОЖНОГО ПРОЦЕССА – *председатель* ***Хабибуллина Надежда Юрьевна,*** *к.т.н., ст. преподаватель каф. КСУП*

Подсекция 10.4 МЕТОДЫ СТЕРЕОСКОПИЧЕСКОЙ ВИЗУАЛИЗАЦИИ – *председатель* ***Дорофеев Сергей Юрьевич,*** *студент каф. КСУП*

Подсекция 10.5 МЕТОДЫ ЛИДАРНОГО ЗОНДИРОВАНИЯ АТМОСФЕРЫ – *председатель* ***Ковшев А.А.,*** *аспирант ИОА СО РАН*

Секция 11. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – *председатель* ***Шелупанов Александр Александрович,*** *зав. каф. КИБЭВС, д.т.н., профессор; зам. председателя* ***Мещеряков Роман Валерьевич,*** *к.т.н., доцент каф. КИБЭВС*

Секция 12. 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 13. РАДИОТЕХНИКА – *председатель* ***Титов Анатолий Александрович,*** *д.т.н., профессор каф. РЗИ; зам. председателя* ***Семенов Эдуард Валерьевич,*** *к.т.н., доцент каф. РЗИ;*

Секция 14. 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 14.1 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 14.2 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 15. 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 15.1 МОДЕЛИРОВАНИЕ В ЕСТЕСТВЕННЫХ И ТЕХНИЧЕСКИХ НАУКАХ – *председатель* ***Зариковская Наталья Вячеславовна,*** *к.ф.-м.н., доцент каф. ФЭ*

Подсекция 15.2 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 15.3 ИНФОРМАЦИОННЫЕ СИСТЕМЫ МЕНЕДЖМЕНТА – *председатель* ***Сергеев Виктор Леонидович,*** *д.т.н., профессор каф. АСУ*

Секция 16. 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 17. АНТИКРИЗИСНОЕ УПРАВЛЕНИЕ – *председатель* ***Семиглазов Анатолий Михайлович,*** *д.т.н., профессор каф. ТУ; зам. председателя –* ***Бут Олеся Анатольевна,*** *ассистент каф. ТУ*

Секция 18. ЭКОЛОГИЯ И МОНИТОРИНГ ОКРУЖАЮЩЕЙ СРЕДЫ – *председатель* ***Карташев Александр Георгиевич,*** *д.б.н., профессор каф. РЭТЭМ*

Секция 19. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ – *председатель* ***Хорев Иван Ефимович,*** *д.т.н., профессор каф. РЭТЭМ; зам. председателя –* ***Полякова Светлана Анатольевна,*** *к.б.н., доцент каф. РЭТЭМ*

Секция 20. АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОЦИАЛЬНОЙ РАБОТЫ В СОВРЕМЕННОМ ОБЩЕСТВЕ – ***Грик Николай Антонович,*** *зав. каф. ИСР, д.ист.н., профессор; зам. председателя –* ***Казакевич Лариса Ивановна,*** *к.ист.н., доцент каф. ИСР*

Секция 21. 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 22. 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*)

Секция 23. 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 24. ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ ШКОЛЬНИКОВ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – *председатель* ***Дмитриев Игорь Вячеславович,*** *директор ОЦ «Школьный университет», к.т.н.; зам. председателя –* ***Шамина Ольга Борисовна,*** *начальник учебно-методического отдела ОЦ «Школьный университет», к.т.н., доцент*

Секция 25. 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,
предоставленные на конференцию, опубликованы в сборнике
«НАУЧНАЯ СЕССИЯ ТУСУР-2007»
в пяти частях

1 часть – доклады 1 – 8 секций;
2 часть – доклады 9, 11 секций;
3 часть – доклады 10 секции;
4 часть – доклады 12 – 16 секций;
5 часть – доклады 17 – 25 секций.

Адрес оргкомитета:

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

СЕКЦИЯ 9

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

*Председатель – **Раводин О.М.,** д.т.н., профессор каф. КИБЭВС;*
*зам. председателя – **Давыдова Е.М.**, к.т.н., ст. пр. каф. КИБЭВС*

В тематический выпуск «Системная интеграция и безопасность» включены доклады секций 9 и 11 «Научной сессии ТУСУР-2007», которые отражают научные интересы профессорско-преподаватель-ского состава, аспирантов и студентов кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) всех курсов очного обучения, а также студентов и аспирантов других специальностей и вузов России, работающих над вопросами автоматизации технологических процессов, информационной безопасностью и защитой информации, отражая различные аспекты научных направлений, которые интенсивно и традиционно развиваются на кафедре КИБЭВС. Такими научными направлениями являются 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 автоматизации, управления производства, образования, медицины, а также информационной безопасности автоматизированных систем, компьютерной безопасности. Ряд докладов посвящено 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 в рамках группового проектного обучения (ГПО). Система ГПО ралузуется на кафедре КИБЭВС согласно реализации ТУСУР инновационной образовательной программы «Разработка и внедрение в практику системы подготовки специалистов, обеспечивающей генерацию новой массовой волны предпринимателей наукоемкого бизнеса» национального проекта России «Образование».

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБРАБОТКИ ДАННЫХ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ МЕТАЛЛОВ

О.И. Абдалова, ассисентка; И.И. Абдалова, ст. 2 курса СГУПС;
М.И. Андреев, к.т.н., доц.
ТУСУР, г. Томск, т. 41-33-06, oltcde@yandex.ru

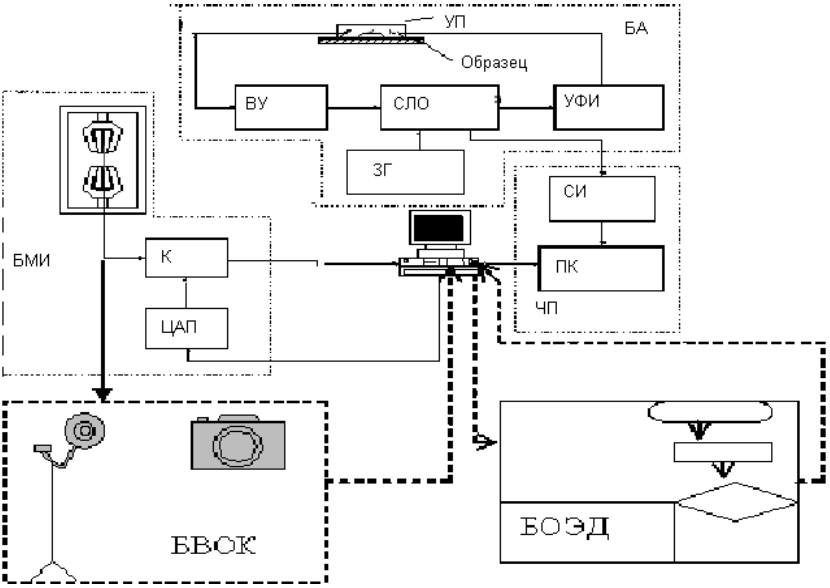
Введение. Накопление деформаций в элементах, которые находятся под воздействием механической нагрузки – это проблема, влекущая за собой негативные последствия. Результатами исследований в этой области являются определение срока эксплуатации строительных металлов для объектов, ресурса их долговечности; использование рекомендаций по условиям их эксплуатации, определение физических свойств металлов в целом. Не менее актуальным является вопрос обработки экспериментальных данных (ОЭД), необходимой для повышения их достоверности и точности, для поиска новых закономерностей в поведении физических характеристик металлов при различных внешних воздействиях (например, при механической циклической нагрузке) [1].

Использование автоматизированной системы ОЭД позволяет сократить временные и трудозатраты на получение зависимостей физических величин измерений от прочностных характеристик металла. Преимуществом также является получение достоверных результатов об оценке напряженно-деформированного состояния (НДС) металлов. Кроме того, появляется возможность сохранения результатов исследования и сравнения с полученными ранее. Важным является и наглядное представление результатов экспериментальных исследований, понятное не только экспертам рассматриваемой предметной области, но и рядовому пользователю.

Итак, целью данной работы являются разработка алгоритмов ОЭД исследований металлов и их программная реализация в виде автоматизированной системы. Для ее достижения необходимо рассмотреть следующие основные этапы: получение экспериментальных данных с использованием специальной экспериментальной установки, ОЭД (разработка и использование соответствующих алгоритмов и программ), получение и использование результатов о НДС исследованных металлов.

Описание экспериментальной установки. В работах [2,3] представлены характеристики основных методов контроля НДС металлов, а также необходимость использования их совокупности. В данной работе при выборе метода контроля учитывались: физические свойства металлов (сталь 09Г2С, сталь 10ХСНД, сталь Ст3), изменяющиеся под воздействием механической нагрузки; высокая чувствительность, разрешающая способность и глубина информативного слоя метода контроля;

простота его использования в эксперименте и на действующей металлоконструкции. Выбранным критериям удовлетворяют ультразвуковой [1, 2, 4] и визуально-оптический [3] методы контроля. На рисунке представлена структурная схема экспериментальной установки ультразвукового и визуально-оптического контроля НДС образцов металлов.



Структурная схема экспериментальной установки: БМИ– блок механических испытаний; К – компоратор; ЦАП – цифро-аналоговый преобразователь; БА – блок автоциркуляции; УП – ультразвуковой преобразователь; ВУ – входной усилитель; СЛО – схема логической обработки; УФИ – усилитель-формирователь импульсов; ЗГ – задающий генератор; ЧП – частотомер-преобразователь; СИ – счетчик импульсов; ПК – преобразователь кода; БВОК – блок визуально-оптического контроля; блок автоциркуляции – блок ультразвукового контроля; БОЭД – блок обработки экспериментальных данных

Здесь, БВОК – блок визуально-оптического контроля; блок автоциркуляции – блок ультразвукового контроля; БОЭД– блок обработки экспериментальных данных.

БОЭД включает алгоритмы ОЭД ультразвукового и визуально-оптического контроля, а также их программную реализацию.

Алгоритмы ОЭД и их программная реализация. При исследовании металлов в ПК передаются данные в результате ультразвукового и визу-

ально-оптического контроля. При ультразвуковом методе контроля исходными данными являются: марка стали, вид поставки, сечение, частота (измеренная с использованием блока автоциркуляции), текущее напряжение, предел упругости (справочный), предел прочности (справочный), коэффициент наклона, коэффициент смещения, частота автоциркуляции (справочная). Модель контроля и прогноза НДС металлов под воздействием механической нагрузки представлена в [4].

При визуально-оптическом методе контроля получены изображения поверхности исследуемого образца металла. Разработанные алгоритмы осуществляют поиск точек смещения на изображениях (области появления напряженно-деформированного состояния исследуемого металла); анализ обработанных изображений, сравнение и получение вектора сдвига; «сеточный» анализ обработанных изображений, включающий этапы формирования сетки на изображении, поиск первых приближений, сохранение полученных координат точек смещения и вывод их в отчет. Блок-схемы разработанных алгоритмов представлены в [5].

Средством реализации предложенных алгоритмов являются Borland C++ Builder, Delphi 7.0. Подробное описание, структурные схемы разработанных программ представлены в [4, 5]. Информационное обеспечение разработанных программ насыщено знаниями рассматриваемой предметной области. Автоматизированная система ОЭД в эксперименте позволяет решать поставленные задачи при исследовании металлов, а также при соответствующей доработке может быть использована на действующих металлокон-струкциях в различных областях промышленности. Результаты тестирования разработанных программ также представлены в работах [4, 5].

ЛИТЕРАТУРА

1. *Муравьев В.В., Зуев Л.Б., КомаровК.Л.* Скорость звука и структура сталей и сплавов. Новосибирск: Наука, 1996. 184 с.

2. *ВенгриновичВ.Л.* Принципы и практика диагностики напряженно-деформированного состояния конструкций, изделий и сварных соединений // В мире неразрушающего контроля. 2005. № 1 [27], март. С. 4–8.

3. *Гордиенко В.Е.* О факторах, влияющих на выбор методов неразрушающего контроля и надежность строительных металлоконструкций // Контроль. Диагностика. 2006. № 1. С. 52–56.

4. *Абдалова О.И.* Разработка программы для диагностики состояния трубопроводов нефтяной промышленности // Вестник компьютерных и информационных технологий. 2006. № 11. С. 19–24.

5. *Абдалова О.И.* Программная реализация алгоритмов обнаружения на изображениях изменений поверхности образцов стали под воздействием механической нагрузки // Контроль. Диагностика. 2006. № 12. С. 52–57.

К ВОПРОСУ ПОСТРОЕНИЯ СИСТЕМ УПРАВЛЕНИЯ БЫТОВЫМИ ПРИБОРАМИ

Е.А. Бакуров, руководитель; Л.А. Торгонский, к.т.н., доцент.
ТУСУР, г. Томск, т. 8-906-947-56-42, bakker@sibmail.com

Бытовая автоматика является одним из прогрессивных современных направлений автоматизации. Целями автоматизации в быту являются экономия энергетических ресурсов, предупреждение аварийных и кризисных состояний бытовой техники, охрана помещений от несанкционированного доступа, расширение спектра сервисных услуг в конечном счете, повышающих уровень комфортности среды обитания ее пользователя. В современных условиях средства бытовой автоматики кроме перечисленных предназначений, вместе с тем, стали привлекательными объектами для промышленности, развития инфраструктуры по продвижению средств автоматизации к их реальным и потенциальным пользователям.

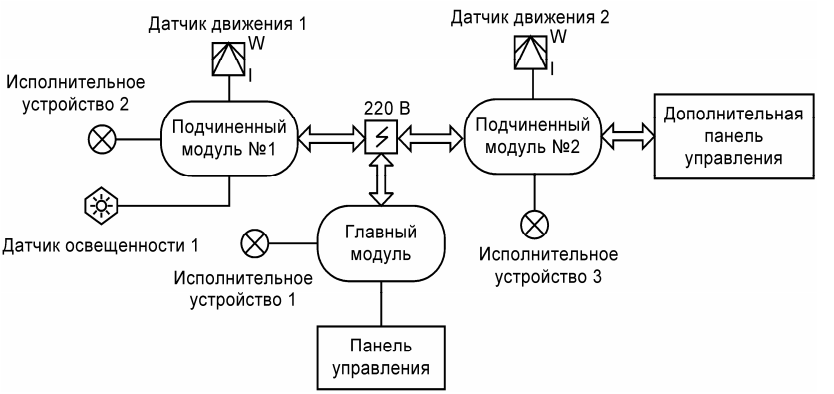
Анализ состояния этой сферы показывает, что наиболее привлекательными для производителей средств автоматизации являются автономные приборы с автоматическим или автоматизированным управлением. Этот сектор автоматизации представляется перспективным, благодаря доступности для неограниченного числа индивидуальных пользователей разного уровня технической подготовки, возраста и достатка.

Приборы индивидуального пользования, в свою очередь, могут объединяться в комплекс. Для выполнения общих задач по управлению распределенными приборами бытового назначения комплекс оснащается центральным контроллером с пультом управления, средствами связи. Развитие технических средств этого сектора средств автоматизации ведет к созданию универсальных и специализированных микропроцессорных систем с присущими им позитивными и негативными свойствами в части избыточности и повышения затрат. Типовая структура микропроцессорной системы управления бытовыми приборами, приведенная на рисунке, по составу объектов аналогична системам иных назначений. Тем не менее, для применения в быту определенные отличия построения систем управления присутствуют. К ним следует отнести:

– ограничение использования проводных соединений при сохранении возможности управления системой из разных помещений;

– привлекательные возможности расширения структурного состава системы по удобству подключения, материальным расходам;

– предоставление пользователю возможности активизации индивидуальных программ управления.



Структура системы управления

Весьма важным фактором успеха построения расширяемых модульных систем управления бытовыми приборами является выбор способов и средств информационного соединения объектов управления. В предлагаемом докладе приводятся краткие сведения об одном из представляющих интерес способов информационного соединения по проводам сетевого электроснабжения жилых помещений.

Передача информации по проводам сети электроснабжения применяется в отечественной и зарубежной практике электрической связи [1]. Ее применение согласуется с ГОСТ Р 51317.3.8 «Совместимость технических средств. Электромагнитная передача сигналов по низковольтным электрическим сетям. Уровни сигналов, полосы частот и нормы электромагнитных помех».

Для отработки приемов и накопления опыта передачи цифровых сообщений по сети переменного тока 110-380В автором доклада на основе специализированной микросхемы КР1446ХК1 [2], выпускаемой предприятием «Ангстрем», реализован модуль приемопередатчика. В микросхеме реализуются кодирование и частотная модуляция цифровых сигналов. Частотно-модулированный сигнал через развязывающий трансформатор передается в линию электросети 110–380 В.

Скорость обмена может принимать одно из 4-х возможных значений: 124, 248, 496, 992 бит/с и программно задается во время инициализации микросхемы КР1446ХК1. В микросхеме применено помехозащищенное кодирование для исправления одиночных и обнаружения двойных ошибок, которые могут возникать при передаче из-за помех в сети.

Приемник микросхемы анализирует данные, приходящие на вход в установленном спецификацией формате. Если приходят код слова синхронизации, последующий код адреса, назначенный адаптеру, то следующие за ними 2 байта информации предназначены данному приемопередатчику (ПП). Полученная информация сохраняется в буфере приема и может быть прочитана однократно или многократно.

Для передачи данных необходимо последовательно записать в буфер передачи адрес приемника и 2 байта данных. После этого информация в зависимости от выбора варианта выдается однократно или многократно в сеть по сигналу от микроконтроллера.

Для обеспечения опосредованного управления автором доклада выбран протокол информационного сообщения, соответствующий транспортному уровню OSI.

Начальные предположения к выбору приняты следующие:

– контроллер системы управления опрашивает подчиненные в порядке установленной очереди (т.е. подчиненный модуль не может самостоятельно начать передачу пакета в сеть, а контроллеру в исследуемом варианте присвоен адрес 01h);

– адреса всех модулей, подключенных к сети, контроллер по результатам опроса запоминает, перебирая их возможные адреса и регистрируя ответы на запрос;

– если по истечении одной секунды не приходит ответный пакет на пакет запроса главного модуля, то предусмотрена повторная посылка пакета запроса, а после трехкратного повтора подчиненный модуль считается неработающим;

– размер блока данных пакета сетевого уровня равен двум байтам, что обусловлено особенностями микросхемы КР14462ХК.

Испытания микропроцессорной системы управления освещением с использованием приемопередатчика по силовой электросети показали приемлемые результаты по проценту ошибок пересылки (не превышают 7%) на скорости обмена 992 бит/с. Однако проведение дальнейших исследований в части накопления статистики сбоев и оценки факторов влияния на их число представляется необходимым [1, 2].

ЛИТЕРАТУРА

1. http://www.brain-tech.ru – сайт, посвященный технологии «Умный дом».
2. http://www.angstrem.ru – сайт компании «Ангстрем».

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ДЛЯ ПРОВЕДЕНИЯ ПРИЕМНОЙ КОМИССИИ И УЧЕТА СВЕДЕНИЙ О СТУДЕНТАХ ФИЛИАЛА ТУСУР В г. СУРГУТЕ

А.А. Баранов, студент 5 курса каф. КИБЭВС;
Н.А. Новгородова, ассистент каф. КИБЭВС
ТУСУР, г.Томск, e-mail: Balex@sibmail.com

С каждым днем растет популярность автоматизированных систем обработки информации. И это правильно, потому что их применение во многих сферах деятельности позволяет добиться недостижимых ранее производительности и удобства в работе. Широкое распространение средств программирования вроде Delphi, C++ Builder и таких СУБД, как Paradox, InterBase, Oracle, MySQL и т.д. [1]. позволило относительно быстро создавать информационные системы для применения в конкретных случаях. При этом такие системы обладают удобным интерфейсом и максимально учитывают специфику работы в данной области, к тому же известно, что специализированный продукт в том виде деятельности, для которого он разрабатывался, обычно превосходит универсальный по удобству и функциональности. Поэтому во многих случаях логичной является замена старых способов хранения данных в виде электронных таблиц и уж тем более бумажных носителей (которые теперь можно использовать только в качестве архивов, не применяя в повседневной деятельности) на автоматизированные информационные системы.

В настоящее время в филиале ТУСУР в г.Сургуте для хранения информации о студентах и абитуриентах применяются таблицы Excel, также некоторые данные хранятся в виде текстовых файлов. Необходимо разработать систему, которая позволила бы обрабатывать все эти данные, максимально облегчила работу сотрудников и обеспечила печать всей необходимой документации. К системе предъявляются следующие требования:

– функциональность,
– надежность в работе,
– дружественный интерфейс,
– удобство и легкость в использовании,
– учет специфических требований для филиала,
– гибкость в настройке,
– возможность распечатки необходимой документации,
– поддержка импорта и экспорта данных в MS Excel.

При разработке нужно учесть основные бизнес-процессы, задачи и документооборот в филиале. Проектирование было начато с изучения предметной области и построения реляционной модели данных, необ-

ходимой для создания базы данных**.** Система должна обеспечивать редактирование всей информации о студентах, кафедре, попечителях студентов и сотрудниках, должна дать возможность генерировать документы: договор, личное дело и т.д. Создание такого программного продукта приведет к предупреждению возможных случайных ошибок и поможет избежать бумажную волокиту, увеличить мобильность работников.

Реляционная модель данных представляет собой общую структуру базы данных, пригодную для построения баз данных под управлением практически любых СУБД. Значит, остается только выбрать, какая СУБД будет использоваться. Приемом сведений об абитуриентах занимается несколько сотрудников одновременно, поэтому СУБД должна быть многопользовательская. Многопользовательский режим может предоставить клиент-серверная архитектура базы данных или архитектура с совместным использованием файлов. Выбор был остановлен на клиент-серверной архитектуре за счет ее большей устойчивости. Наиболее оптимальным решением представляется использование СУБД Interbase, обладающей следующими свойствами: легкость использования и управления, производительность, масштабируемость, переносимость, небольшое использование ресурсов и возможность восстановления после сбоя. К тому же в свете недавних событий роль играет наличие у кафедры лицензионной версии СУБД. Для разработки самой программы будет применена среда программирования Borland Delphi, ввиду ее широких возможностей, удобства в работе и быстроты создания продукта. Также Delphi поддерживает технологию InterBase Express, что позволит обращаться к серверу InterBase без использования таких средств доступа к данным, как BDE. Для вывода документации на печать скорее всего будет применяться генератор отчетов FastReport и MS Word [2, 3].

Проанализировав требования, предъявляемые к разрабатываемой системе, представим ее примерный компонентный состав.

1) «Список абитуриентов» – компонент, предназначенный для быстрой регистрации абитуриентов в приемной комиссии филиала.

2) «Форма регистрации» – форма для быстрого внесения в базу данных, содержащихся в заявлении студента;

3) «Личное дело» – компонент, содержащий информацию из личного дела студента, которое создается после поступления человека в вуз, должно поддерживать добавление сведений о переводе на другой курс, изменении статуса студента (обучается, отчислен, ушел в академ. отпуск и т.д.), достижениях и поощрениях студента и др.

4) «Анкета абитуриента» – компонент, выполненный в виде вкладки в личном деле студента, представляет собой полную карточку абитури-

ента, содержит исчерпывающие сведения о поступающем. Содержит следующую информацию об абитуриенте: «Специальности», «Льготы», «Личные данные», «Образование», «Испытания», «Родственники», «Сданные документы».

5) «Зачисление» – компонент, отображающий ход зачисления по группам.

6) «Сотрудники» – компонент содержит сведения о сотрудниках кафедры.

7) «Форма печати» производит распечатку документации.

8) «Настройки программы» предназначены для изменения собственно настроек программы.

ЛИТЕРАТУРА

1. *Фаронов В.* Программирование баз данных в Delphi 7. Учебный курс. СПб.: Питер, 2005. 459 с.

2. *Скляр А.Я.* Введение в InterBase. М.: Горячая линия–Телеком, 2002. 517 с.

3. *Кренке Д.* Теория и практика построения баз данных. 8-е издание. СПб.: Питер, 2003. 800 с.

ПРОЕКТИРОВАНИЕ БАЗЫ ДАННЫХ УЧЕТА СВЕДЕНИЙ О СТУДЕНТАХ ФИЛИАЛА ТУСУР В г. СУРГУТЕ

А.А. Баранов, студент 5 курса каф. КИБЭВС;
Н.А. Новгородова, ассистент каф. КИБЭВС
ТУСУР, г.Томск, e-mail: Balex@sibmail.com

Базы данных в настоящее время находят все большее применение практически во всех областях жизни и деятельности. Задача базы данных состоит в том, чтобы помочь людям в учете различного рода вещей [1–3]. При этом отличие от других способов хранения информации в виде списков и электронных таблиц заключается в том, что сведения в базе взаимосвязаны между собой, и это позволяет легко находить нужные данные и зависимости. Практически все современные СУБД относятся к реляционной модели, преимущество которой состоит в способе хранения данных, минимизирующем их дублирование и исключающем некоторые типы ошибок обработки, возникающие при других способах хранения. Данные хранятся в виде таблиц со столбцами и строками, связь между таблицами осуществляется с помощью ключей, содержащихся в столбцах.

На сегодняшний момент в филиале ТУСУР в г. Сургуте вся информация об абитуриентах и студентах хранится в виде электронных таблиц MS Excel. Использование MS Excel доставляет массу неудобств. Не

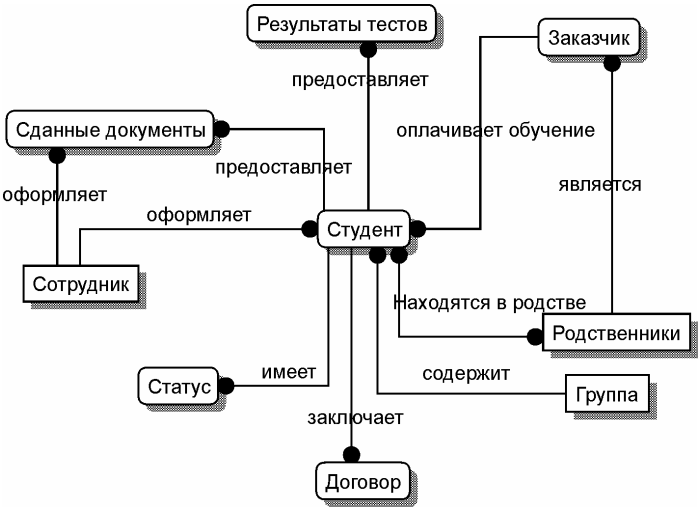
всегда можно сгенерировать новый документ из-за того, что информация в таблицах не связана. Нельзя быстро найти нужную информацию. Нельзя вести учет документации и проследить за наличием информации о студентах. Таблица имеет большие размеры, что затрудняет ввод данных, так как приходится искать нужные ячейки для внесения данных, из-за этого повышается вероятность ошибки при вводе. Поэтому замена электронных таблиц MS Excel на реляционную базу данных является правильной и своевременной политикой.

Наиболее распространенным методом проектирования баз данных является проектирование в рамках модели «сущность-связь». Сначала проводится анализ предметной области, в ней выделяются основные сущности и их атрибуты. На основе существующих между сущностями связей и зависимостей строится модель «сущность-связь», которая потом преобразуется в реляционные конструкции. Полученная реляционная модель подвергается нормализации с целью устранения аномалий модификации, дублирования данных или денормализации, чтобы упростить структуру базы данных, повысить ее быстродействие и т.д.

Рассмотрим предметную область. В филиале студенты обучаются по очной и заочной форме. Студенты очной формы после второго курса переводятся в Томск. При поступлении в филиал кафедры на абитуриента сотрудником приемной комиссии оформляется анкета абитуриента, содержащая личные сведения, результаты пройденных тестов (ЕГЭ, ЦТ и др.), имеющиеся награды (медали, грамоты и т.д.), информацию о родственниках. Также каждый абитуриент должен предоставить комплект документов – мед. справку, фотографии, аттестат об образовании и др. Абитуриент может подать заявку на поступление на несколько специальностей. Если суммарный балл, набранный по тестам, больше проходного на специальность, абитуриент зачисляется. Если нет, то может сдать экзамен. Большинство студентов в филиале обучаются платно, при поступлении заключается договор на оплату обучения, где указывается заказчик, это может быть родственник студента, предприятие или сам поступающий. Производится учет оплаты студентами обучения по семестрам, каждый год заключается дополнительное соглашение на оплату обучения. Стоимость обучения устанавливается на учебный год для специальности и курса. В базе должны храниться сведения об обучающихся студентах (сведения о переводе на другой курс, нахождении в академическом отпуске, отчислении и т.д.) и выпускниках. Также должен вестись учет происходящего документооборота.

Для данной предметной области выделим основные сущности и составим модель «сущность-связь». Эта модель, выполненная с использованием CASE-средства Erwin Platinum, представлена на рисунке. На ее

основе была создана подробная реляционная модель данных, используя которую можно разработать структуру базы данных.



Модель «сущность-связь»

ЛИТЕРАТУРА

1. *Кренке Д.* Теория и практика построения баз данных. 8-е издание. СПб.: Питер, 2003. 800 с.

2. *Кузнецов С.Д.* Основы современных баз данных.

3. *Карпова Т.С.* Базы данных: модели, разработка, реализация. М.: Питер, 2002, 304 с.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОИСКА, АНАЛИЗА ИНФОРМАЦИИ И ПРОГНОЗИРОВАНИЯ РЕЗУЛЬТАТОВ

А.В. Бяков, студент 5 курса каф. КИБЭВС

ТУСУР, г. Томск, e-mail: macintosh@sibmail.com

В эпоху электронного прогресса в сети Internet можно найти любую информацию, но как найти информацию, которая нам нужна? Провести несколько часов, изучая результаты поисковых систем? Возможно, но представим, что данная информация требуется фирме среднего размера ежедневно. Следует учесть, что информация должна быть самая «све-

жая», так как нужно знать, что делают конкуренты, а не что сделали год назад (хотя и это иногда бывает полезным).

Разрабатываемая система представляет собой автоматизированную систему поиска, анализа информации и прогнозирования результатов. Работа такой системы выполняется в несколько этапов.

1. Анализ существующих данных, позволяющий получить полную картину о том, что нам нужно.

2. Поиск и сбор информации. Объемы данных, на этом этапе, настолько внушительны, что человеку просто не по силам проанализировать их самостоятельно, хотя необходимость проведения такого анализа вполне очевидна, так как в этих «сырых данных» заключены знания, которые могут быть использованы при принятии решений. Для того чтобы провести автоматический анализ данных, используется Data Mining.

3. Предобработка и очистка данных.

4. Подготовка исходных данных. Методика анализа с использованием механизмов Data Mining-а базируется на различных алгоритмах извлечения закономерностей из исходных данных, результатом работы которых являются модели. Таких алгоритмов довольно много, но несмотря на их обилие, использование машинного обучения и т.п., они не способны гарантировать качественное решение. Никакой самый изощренный метод сам по себе не даст хороший результат, так как критически важным становится вопрос качества исходных данных.

5. Прогнозирование. Это одна из самых востребованных, но при этом и самых сложных задач анализа. Проблемы при ее решении обусловлены многими причинами – недостаточное качество и количество исходных данных, воздействие субъективных факторов. Но именно качественный прогноз является ключом к решению таких бизнес задач, как оптимизация финансовых потоков, бюджетирование, оценка инвестиционной привлекательности и многих других [1–3].

Ценность таких данных будет ощутима при наличии на рынке большого числа конкурентов. Зная, что хотят делать другие, можно сформировать свои действия, которые приведут к наилучшему результату.

На данном этапе идет разработка алгоритма поиска и сбора информации, с целью получения минимального времени поиска и максимально релевантного результата. Изучаются готовые поисковые системы с открытым исходным кодом, которые распространяются по лицензии GNU.

ЛИТЕРАТУРА

1. http://www.basegroup.ru
2. http://bestinform.com
3. http://www.intuit.ru

ЭЛЕКТРОННАЯ БИБЛИОТЕКА

Э. К. Данилин, студент 5 курса каф. КИБЭВС
Н.А. Новгородова, ассистент каф. КИБЭВС
ТУСУР, г. Томск, e-mail: Kain@ms.tusur.ru

Базы данных давно используются в различных отраслях, но в библиотеках используется редко, хотя библиотека сама по себе нуждается в структурированной системе. К примеру, затрачиваемое библиотекарем время на оформление одной-двух книг суммируется из поиска читательского билета, поиска книги, оформления книги, а если читательских не десятки, а сотни или тысячи, а сколько книг (!) – в этом количестве информации можно легко сделать ошибку. В таких случаях удобно использовать электронную базу данных [1, 2].

Преимущества использования специализированного программного приложения в отличие от приложений общего назначения простота использования оператору не придется искать нужные функции, они всегда под рукой, автоматизация различных процессов – генерирование отчетов, обработка данных, поиск, фильтры и многое другое, а также уменьшения ошибок оператора за счет предусмотренных заранее возможных ситуаций при работе с данными.

Целью работы являлась разработка базы данных и системы управления ею. Эта система рассчитана на оператора не являющегося специалистом в компьютерной области, т.е. на простого пользователя. Но такие приложения, как Microsoft Access, требуют знания баз данных и основ SQL, т.е. система должна удовлетворять следующие требования:

1) функциональность,
2) надежность,
3) практичность,
4) дружественный интерфейс,
5) легкость эксплуатации.

Для обеспечения этих условий, спроектирован интуитивно понятный интерфейс; для обеспечения практичности и легкости использования инструменты располагаются наиболее удобным образом. В данный момент «электронная библиотека» находится на стадии доработки.

ЛИТЕРАТУРА

1. *Баженова И.Ю.* Delphi 5. Самоучитель программиста. КУДИЦ-ОБРАЗ, 2000. 326 с.

2. *Глушаков С.В., Ломотько Д.В.* Базы данных. Фолио, 2002. 510 с.

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ SOLID WORKS ДЛЯ РАЗРАБОТКИ СЛОЖНОЙ ЭЛЕКТРОРАДИОАППАРАТУРЫ

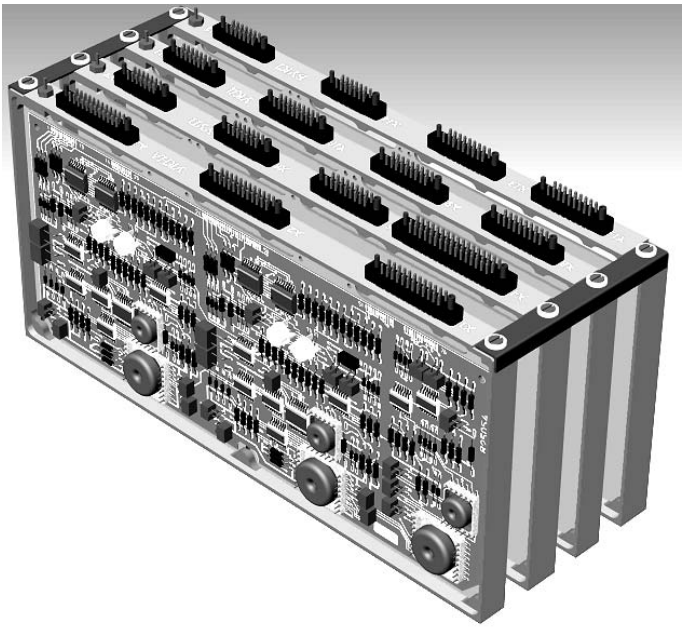
А. В. Долганов, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, e-mail: Lyohtya@ms.tusur.ru

Техническое развитие цивилизации привело к тому, что в настоящее время человечество практически не может обходиться без радиоэлектроники и радиоэлектронных приборов. В настоящее время электроника способна управлять такими процессами, где ранее требовались опыт и внимание не одного десятка человек. Более того, электронные приборы способны выполнять очень сложную работу даже при таких условиях внешней среды, при которых существует угроза не только здоровью человека, но и его жизни. К таким приборам предъявляются наиболее жесткие требования и обращается особое внимание к их надежности. Человек, ограниченный своими способностями, не может учитывать все действующие на прибор факторы и все более и более обращается за помощью к системам автоматизированного проектирования, которые в последнее время достигли небывалых высот.

В высокоточной и дорогостоящей аппаратуре уже на этапе разработки необходимо учитывать такие факторы, которые возможно оценить только на готовой аппаратуре либо путем достоверного физического моделирования. В данной статье о такой системе физического моделирования, как Solid Works, и пойдет речь [1–4]. Это легкое в освоении средство позволяет инженерам-проектировщикам быстро отображать свои идеи в эскизе, экспериментировать с элементами, размерами и формами, а также создавать модели и подробные чертежи. Solid Works позволяет не только создавать трехмерное изображение детали, но и придавать ему все физические свойства требуемого материала – массу, плотность, прочность. С его помощью можно получить реальную трехмерную, твердотельную модель детали, электрорадиоизделия и даже готового прибора любой сложности. В таких отраслях, как ракетостроение, большую роль играют массогабаритные показатели прибора, Solid Works дает возможность точного расчета объема и массы деталей сколь угодно сложной формы.

Такое моделирование удобно не только для производителя, но и для заказчика, так как уже на ранних этапах проектирования имеется возможность оценить всевозможные свойства изделия – его внешний вид и форму (рисунок), массу и объем.

В среде Solid Works реализована система, позволяющая досконально изучить прибор, например, путем разнесения его на отдельные детали либо путем создания всевозможных разрезов.



Трехмерная твердотельная модель изделия

Solid Works хорошо адаптирован для производства, в нем реализована функция создания чертежей по готовой трехмерной модели, причем в формате, доступном для других систем автоматизированного проектирования, таких как AutoCAD, P-Cad, CAM и т.д.

Созданные модели позволяют работать на автоматизированном производстве со станками с числовым программным управлением. Например, вырезание детали фрезой возможно при выполнении детали в той же последовательности, какая следует на реальном станке, т.е. вырезанием детали из цельного бруска, а не наращиванием материала, хотя это и проще.

Внедрение Solid Works в производство существенно облегчает работу инженерам-проектировщикам, улучшает взаимопонимание между заказчиком и исполнитель, и значительно повышает темпы производства.

ЛИТЕРАТУРА

1. Solid Works 2005 – Интерактивное руководство пользователя.
2. Знакомство с Solid Works 2005 – электронная книга, 2005. 102 с.
3. Solid Works для вузов – электронная книга. 2005. 351 с.
4. http://www.files.solidworks.com – информационный сайт.

НЕЙРОНЕЧЕТКАЯ ИДЕНТИФИКАЦИЯ ПАРАМЕТРОВ ЭЛЕКТРОТЕРМИЧЕСКИХ ПРОЦЕССОВ ПРИ АВТОМАТИЗАЦИИ УСТАНОВКИ ЭЛЕКТРОШЛАКОВОГО ПЕРЕПЛАВА

А.Ю. Дракин, аспирант

БГТУ, г. Брянск, т. 563602, ada108@yandex.ru

Процесс электрошлакового переплава (ЭШП) осуществляется на установке с неподвижным водоохлаждаемым кристаллизатором. Кристаллизатор является сложным техническим объектом [1–4], описываемым зависимостями, приведенными в [5], при наличии фактора неопределенности в оценке ряда характеристик, входящих в эти зависимости, в частности, к таковым (характеристикам) можно отнести:

а) количество флюса в шлаковой ванне (ШВ),

б) положение и размеры (глубина) ШВ в системе координат кристаллизатора,

в) положение и форму погруженных в ШВ частей электродов,

г) граничные условия и ряд других.

Применение классического аппарата структурной и параметрической идентификации данного блока представляется невозможным в силу нелинейности и многомерности математического описания протекающих процессов.

Структура модели для проведения нейронечеткой идентификации параметра «ток переплава», выполненной средствами системы MatLab 7.0/Simulink, представлена на рис. 1.

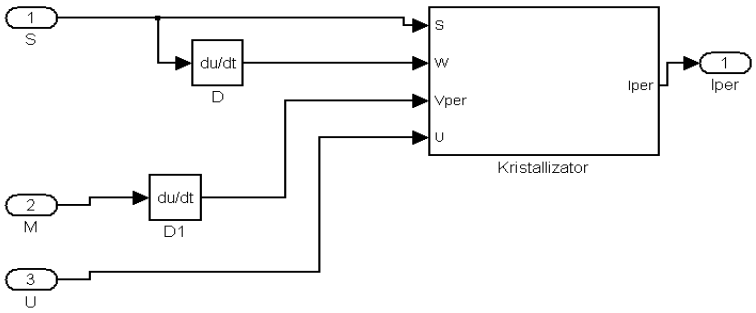


Рис. 1 ANFIS-модель кристаллизатора при ЭШП

Модель включает в себя сигналы: S – положение электродов; M – масса слитка; U – напряжение переплава; I_{per} – ток переплава. Дополнительно на входы подаются производные входных сигналов W – скорость подачи электродов; V_{per} – скорость переплава.

Для проведения нейронечеткой идентификации при создании системы автоматического управления установкой ЭШП использованы данные системы контроля (временные зависимости положения электродов, массы слитка, тока переплава, полученные непосредственно в процессе плавки). На их основании в процессе обучения нейронечеткой сети получена нечеткая нелинейная зависимость тока переплава от уровня наплавленного металла, скорости переплава и напряжения на расходуемых электродах [6].

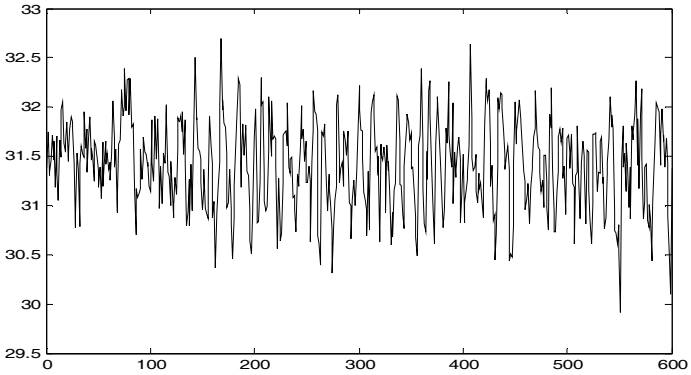


Рис. 2 Измеренные значения тока переплава

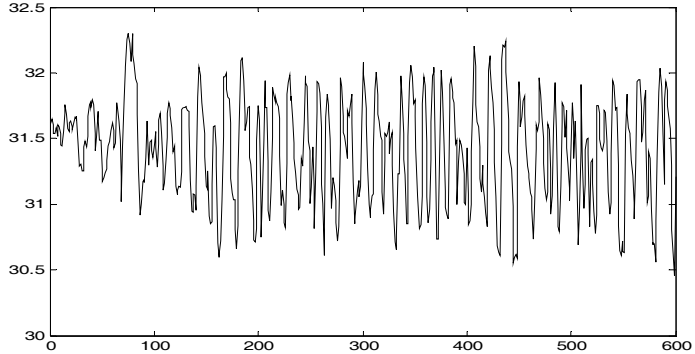


Рис. 3 Рассчитанные с использованием нейронечеткого контроллера значения тока переплава

Среднеквадратическая погрешность оценки значений тока переплава не превышает 3,5% относительно данных, не использовавшихся в обучающей выборке, что обусловлено наличием стохастической составляющей в данных, которые использовались для обучения нечеткой мо-

дели. Применение нормализации и сглаживания, очевидно, может повысить точность получаемых результатов.

Таким образом, все вышеизложенное позволяет сделать вывод об адекватности применения нейронечеткой методологии при создании систем управления сложными техническими объектами электрометаллургии с необходимостью косвенного контроля целевых переменных.

ЛИТЕРАТУРА

1. *Лукаш А. Г., Кудин Л.А. и др.* Принципы построения и алгоритмы функционирования АСУ ТП ЭШЛ на основе обучающихся моделей. М.: Проблемы спец. электрометаллургии, 1981. Вып. 14.

2. *Захаров В.Н., Ульянов С.В.* Нечеткие модели интеллектуальных промышленных регуляторов и систем управления. Методология проектирования // Известия академии наук. Техническая кибернетика. 1993. № 5.

3. *Митчелл А.* Механизм выделения и распространения тепла в процессе ЭШП // Электрошлаковый переплав. Киев. Наукова думка, 1971. С. 149–161.

4. *Троянский А.А.* Использование информационно-измерительной системы для диагностики и исследования процесса ЭШП // Металл и литье Украины. 2002. №7–8. С. 25–26.

5. *Петров А.И.* Автоматизация управления электрошлаковым переплавом. Устинов.: Удмуртия, 1985.

6. *Кудинов Ю.И., Дорохов И.Н., Пащенко Ф.Ф.* Нечеткие регуляторы и системы управления // РФФИ, отчет по гранту 04-01-00816, г. Москва, 2004.

КРИПТОСИСТЕМЫ КЛЕТОЧНЫХ АВТОМАТОВ

О.О. Евсютин, студент 3 курса

ТУСУР, г. Томск, т. 67-95-87, Levor@mail2000.ru

Идея клеточных автоматов была сформулирована независимо Дж. фон Нейманом и К. Цусе в конце 40-х гг. Оба рассматривали их как универсальную вычислительную среду для построения алгоритмов, эквивалентную по своим выразительным возможностям машине Тьюринга [1]. Эта идея породила волну многочисленных теоретических и прикладных исследований.

Клеточные автоматы являются дискретными динамическими системами, поведение которых полностью определяется в терминах локальных зависимостей, в значительной степени так же обстоит дело для большого класса непрерывных динамических систем, определенных уравнениями в частных производных. В этом смысле клеточные автоматы в информатике являются аналогом физического понятия «поля».

Клеточный автомат может мыслиться как стилизованный мир. Пространство представлено равномерной сеткой, каждая ячейка которой,

или клетка, содержит несколько битов данных; время идет вперед дискретными шагами, а законы мира выражаются единственным набором правил, скажем, небольшой справочной таблицей, по которой любая клетка на каждом шаге вычисляет свое новое состояние по состояниям ее близких соседей. Таким образом, законы системы являются локальными и повсюду одинаковыми.

Клеточные автоматы дают полезные модели для многих исследований в естественных и вычислительных науках, в комбинаторной математике; они, в частности, представляют естественный путь изучения эволюции больших физических систем.

Целью данной работы является разработка нового класса криптосистем на базе обратимых клеточных автоматов.

Некоторые основные черты физических законов, таких как однородность и локальность, присущи клеточным автоматам по построению; с другой стороны, обратимость не получается автоматически и должна быть представлена программно.

Можно конструировать нетривиальные клеточные автоматы, которые проявляют полную обратимость.

Система клеточных автоматов, детерминированная в обоих направлениях времени, называется обратимой, а правило, которое заставляет ее двигаться назад во времени, называется обратным по отношению к исходному, или прямому, правилу.

За исключением тривиальных случаев, обратное правило, когда оно существует как правило, отлично от прямого.

В специальных случаях, тем не менее, возможно достичь практически такого же эффекта «обратимости во времени» за счет выполнения того же прямого правила, что и при прямом направлении времени, но используя в качестве начального состояния для обратного движения состояние, полученное из конечного состояния при продвижении вперед предписанным преобразованием – процедурой «транслитерации».

Динамический закон, обладающий этим свойством, называется инвариантным к обращению времени относительно заданного преобразования состояний, или просто инвариантным к обращению времени, когда оператор преобразования известен. Таким образом, «инвариантность к обращению времени» более сильное свойство, чем просто «обратимость».

В работе используются два метода получения обратимых правил клеточных автоматов:

– метод второго порядка,

– метод разбиения (использование окрестности Марголуса).

ЛИТЕРАТУРА

1. *Тоффоли Т., Марголус Н.* Машины клеточных автоматов. Мир, 1991, 284 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ВЫЧИСЛЕНИЯ ДИСКРЕТНОГО ЛОГАРИФМА

М.В. Ильенко, ст. 3 курс ФВС; С.К. Росошек, доцент каф. КИБЭВС
г. Томск, ТУСУР, marishail@rambler.ru

При проектировании криптосистемы важно учитывать существующие методы взлома. Именно методы вычисления дискретного логарифма диктуют параметры криптосистем, стойкость которых основана на трудности их вычисления. Это системы Диффи-Хеллмана, шифры Шамира и Эль-Гамаля [1–4].

Указанные выше шифры основываются на односторонней функции:

$$y = a^x \bmod p\,. \qquad (1)$$

Известно, что, зная a и x, можем вычислить y, произведя не более $2\log x$ операций. Однако задача нахождения дискретного логарифма гораздо более сложна и состоит в отыскании x по известным a и y.

Наиболее очевидным и легким в реализации является алгоритм исчерпывающего поиска (прямого перебора). Он состоит в последовательной подстановке дискретного логарифма x в формулу (1) вплоть до того, когда вычисленное значение y совпадет с начальным. Однако этот метод является и самым трудоемким. Среднее время, затрачиваемое на его реализацию для возведения в степень по простому модулю p, составляет

$$t_{п.п.} \approx \frac{p}{2}\,. \qquad (2)$$

Как видим, алгоритм абсолютно неэффективен в реальных условиях при больших p, которые используются в криптографии.

Более быстрый метод нахождения дискретного логарифма впервые был предложен Шенксом в 1973 г. Этот алгоритм носит название «малый шаг – большой шаг». Пусть $m = \sqrt{p}$, где p есть порядок α. Этот алгоритм основан на следующем замечании. Если $\beta = \alpha x$, то запишем $x = im + j$, где $0 \le i, j < m$, следовательно, $\alpha x = \alpha im \cdot \alpha j$, откуда следует $\beta(\alpha - m)i = \alpha j$. В описанном выше методе «малый шаг – большой шаг» время отыскания x гораздо меньше, чем в алгоритме исчерпывающего поиска и составляет

$$t_{м.ш.б.ш.} \approx 2\sqrt{p}\,. \qquad (3)$$

Однако при больших p время вычислений по данному методу возрастет и составит

$$t_{м.ш.б.ш.} \le const\sqrt{p}\log^2 p\,. \qquad (4)$$

Еще одним, более совершенным по сравнению с предыдущим, является ρ-алгоритм Полларда вычисления дискретного логарифма. Основные идеи этого алгоритма известны в теории чисел довольно долгое время, однако только в 1979 г. американским ученым Адлеманом был предложен данный алгоритм как метод решения задачи нахождения дискретного логарифма. В реальных условиях реализации данного алгоритма (в том числе и его усовершенствованных вариантов) дает довольно быстрое решение задачи нахождения дискретного логарифма. При этом среднее время решения задачи с использованием данного метода составляет:

$$t_{\rho\text{-а.П.}} \approx \text{const1} \cdot 2^{\text{const2} \cdot \sqrt{\log p \log\log p}}. \qquad (5)$$

Самым быстрым на данное время считается алгоритм Полига-Хеллмана. Этот алгоритм используется в случае известной факторизации порядка p группы G. Алгоритм Полига-Хеллмана является наиболее сложным в реализации, так как требует реализации других теоретико-числовых алгоритмов, таких как китайская теорема об остатках. Трудоемкость данного метода следующая:

$$t_{\text{П-Х}} \approx \text{const1} \cdot 2^{(\text{const2}+o(1)) \cdot \sqrt[3]{\log p (\log\log p)^2}}. \qquad (6)$$

В рамках данного исследования была написана программа, реализующая работу данных методов. Ее работа будет продемонстрирована в процессе защиты публикации.

При проектировании систем защиты считается, что противник силен. При проектировании криптосистем, основанных на использовании уравнения (1), следует считать, что противник будет использовать наиболее быстрый алгоритм для решения задачи нахождения диск-ретного логарифма. По данным на 2005 г., рекомендуемая длина модуля для достижения криптостойкости таких систем составляет 1024 бит.

ЛИТЕРАТУРА

1. *Росошек С.К.* Специальные главы математики: Учебное пособие. Часть 2. Томск, 2006.

2. *Рябко Б.Я., Фионов А.Н.* Криптографические методы защиты информации: Учебное пособие. М.: Телеком, 2005.

3. *Брюс Шнайер*. Прикладная криптография.

4. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. МЦНМО. 2003.

РАСЧЕТ ПОМЕХ (ПАРАЗИТНЫХ НАВОДОК) В ЦЕПЯХ ЭЛЕКТРОПИТАНИЯ

И.Р. Исмагилов, студент гр. 572-2;
ТУСУР, г. Томск т. 8-923-411-57-90, iir@list.ru

При работе электронных устройств имеют место *паразитные связи.* Паразитная связь обусловлена конструкцией изделия и физическими процессами в схеме.

Паразитными называют элементы, появившиеся в результате неидеальности практической реализации электрической схемы из-за невозможности создания проводников и линий связи, не обладающих сопротивлением, индуктивностью и емкостью.

Канал связи может являться как источником, так и приемником помех. Если два канала связи имеют взаимную паразитную связь, то и наводки, а следовательно, и утечка информационных сигналов возникают в обоих каналах взаимно. Уровень наводок и их влияние на работу канала связи зависят от относительного уровня сигналов в каналах.

В электронных устройствах чаще других имеет место внешняя параллельная емкостная паразитная связь.

Причиной появления последовательной помехи (наводки) на высоких частотах является паразитная связь из-за взаимной индуктивности между проводами. В этом случае отсутствие общих проводов не гарантирует отсутствие токовой наводки [1, 2].

На рис. 1 приведен механизм возникновения наведенных информативных сигналов в цепях электропитания, заземления, линиях коммутационных устройств. Рассмотрим подробнее одну из паразитных емкостных связей в схеме, приведенной на рис. 1.

В нашем случае будем проводить расчет наводки в цепи электропитания из информативного канала –1, канал в неинформативный канал – 2, канал-сеть электропитания, по которому возможен съем информации, и между этими каналами существует паразитная емкостная связь. Эквивалентная схема внешней параллельной емкостной паразитной связи в цепи электропитания показана на рис. 2.

Для нахождения величины помехи, наводимой из второго информативного канала в первый, нужно отыскать величину тока, который проходит через внутреннее сопротивление первого канала – R_1. Величину помехи находим по формуле

$$U_{\text{П}} = \dot{I}_{11} * R_1 . \qquad (1)$$

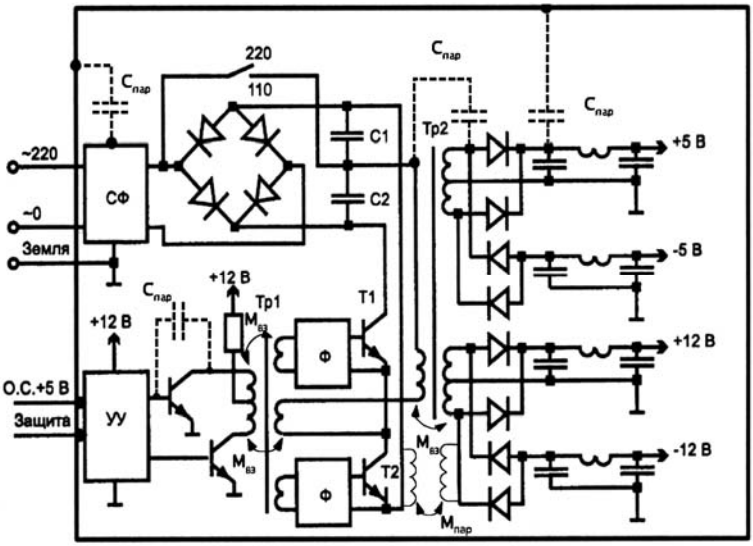


Рис. 1 Двухтактный блок питания РС: СФ – сетевой фильтр; УУ – устройство управления; Ф – формирователи импульсов; Тр1 – трансформатор развязки цепей управления; Тр2 – силовой трансформатор; $C_{ПАР}$ – паразитная емкость электронного элемента; $M_{ПАР}$ – паразитная взаимоиндукция между проводниками, выводами электронных элементов в области высоких частот; $M_{ВЗ}$ – взаимная индукция обмоток трансформатора в области высоких частот

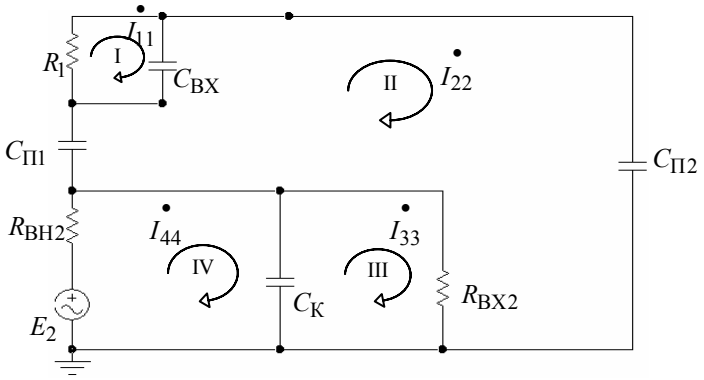


Рис. 2. Эквивалентная схема внешней параллельной емкостной паразитной связи

Зададимся исходными данными для расчета: $R_1 = 50$ Ом $C_{п1} = 50 \cdot 10^{-9}$ Ф; $C_{п2} = 50 \cdot 10^{-9}$ Ф; $C_{вх} = 100 \cdot 10^{-9}$ Ф; $C_к = 100 \cdot 10^{-9}$ Ф; $E_2 = 60$ В; $f = 5000$ Гц.

Для нахождения величин токов в схеме (рис. 2) воспользуемся методом контурных токов, который базируется на втором законе Кирхгофа. После составления системы уравнений и решения ее при помощи программы COMCAL получаем величину тока наведенного сигнала:

$$\dot{I}_{11} = 3{,}65 \cdot 10^{-2}\ \text{А}\ .$$

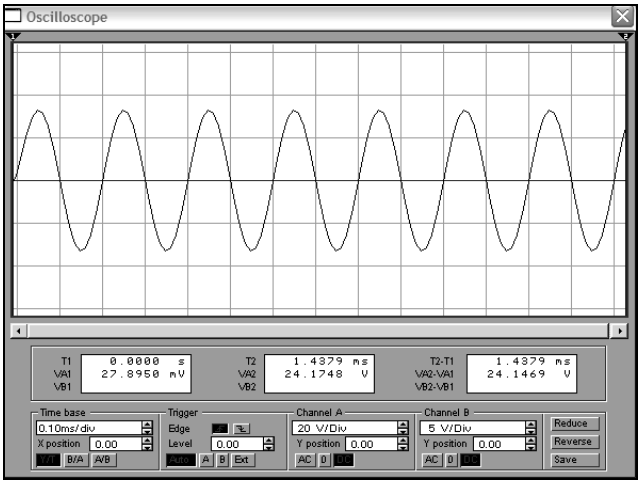
Подставляя данные в (1), получаем, что величина помехи наведенного сигнала из второго канала в первый равна

$$U_{\text{П}} = 1{,}825\ \text{В}.$$

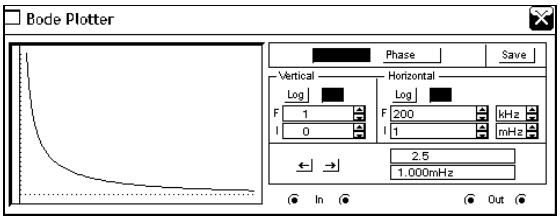
Для проверки полученного результата воспользуемся средой программной моделирующей системы версии EWB 5.12. Расчетное и экспериментальное значения примерно равны, следовательно, расчеты проведены верно:

$$U_{\text{П}}^{\text{расч}} = 1{,}825\,\text{В} \approx U_{\text{П}}^{\text{эксп}} = 1{,}848\ \text{В}.$$

Для снятия осциллограммы и АЧХ наведенного сигнала также воспользуемся моделирующей системой EWB 5.12. Результаты моделирования приведены на рис. 3



а



б

Рис. 3 Результаты моделирования в моделирующей системе EWB: *а* – осциллограмма сигнала наводки; *б* – АЧХ сигнала наводки

Вывод. При наличии паразитных емкостных связей в цепях электропитания в ВИП компьютера возможна утечка информации через паразитные связи информативных каналов с неинформативными, и дальнейший съем информативного сигнала через питающую сеть ВИП [3, 4].

ЛИТЕРАТУРА

1. *Сазонов А.А., Лукичев А.Ю.* Микроэлектронные устройства автоматики: Учебное пособие для вузов. М.: Энергоатомиздат, 1991. 384 с.

2. *Волин М.Л.* Паразитные процессы в радиоэлектронной аппаратуре. М.: Радио и связь, 1981. 296 с.

3. *Зайцев А.П., Шелупанов А.А.* Технические средства защиты информации. Учебное пособие. Томск: Изд-во Томск. гос. ун-та систем управления и радиоэлектроники, 2005.

4. *Зайцев А.П., Шелупанов А.А*. Практические занятия по техническим средствам и методам защиты информации. Томск: Изд-во Томск. гос. ун-та систем управления и радиоэлектроники, 2005.

СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОДУКЦИИ CPU КОРПОРАЦИИ APPLE

К.В. Климентьев, ст. гр. 574-1

ТУСУР, г. Томск, KLIM42rus@mail.ru

В соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2006 г.) произведен анализ современного состояния продукции CPU компании (корпорации) Apple. Компания Apple является производителем персональных компьютеров, предлагает на рынке не только аппаратную часть, но и операционную систему Mac OS с разнообразным программным обеспечением как профессиональным, так и нацеленным на широкий круг пользователей. Для сравнения, например, операционная система Windows разрабатывается компанией Microsoft, а для платформы Wintel разные компоненты аппаратной части проектируются, разрабатываются и производятся различными компаниями. В результате этого не исключены несостыковки и необходимость доработки операционной системы, а также установка дополнительных драйверов. Пользователю Apple эти проблемы незнакомы. Конфликтов между аппаратной частью и операционной системой Mac OS X не возникает [1, 2]. Производство комплексного решения также позволяет Apple обеспечить загрузку и использование аппаратного обеспечения на полную мощность. Все компоненты компьютера работают с операционной системой со 100%-й эффективностью, потому что говорят «на одном

языке». Например, когда портативный компьютер производства Apple находится в режиме энергосбережения, то для того, чтобы активизироваться, ему нужна только одна секунда, в то время как компьютеру на платформе Wintel для выхода из режима энергосбережения требуется около 15 с с восстановлением памяти.

Преимущества процессора PowerPC G4, которым оснащено большинство современных компьютеров Apple, начинается с конвейера обработки данных. Благодаря эффективной 7-шаговой архитектуре (против 20 шагов у процессора Pentium 4), процессор G4 способен во многих случаях выполнять задачу. Высокая производительность процессора PowerPC G4 объясняется во многом и использованием модуля Velocity Engine, который обрабатывает данные 128-битными блоками, в отличие от традиционных процессоров, где применяются 32-битные и 64-битные блоки. Процессор PowerPC G4 способен выполнять четыре (а в некоторых случаях восемь) 32-битных операции с плавающей точкой за один цикл, что от двух до четырех раз быстрее показателей процессоров, применяемых в PC-совместимых компьютерах. Другая ключевая особенность процессора G4 – функция векторной перегруппировки данных. Преимущества PowerPC G4 в области векторной обработки данных делают этот процессор незаменимым в задачах, связанных с визуализацией данных. В старших моделях Power Mac G4 применяется трехуровневая организация кэш-памяти процессора. Кэш-память третьего уровня использует 2 Мб высокоскоростной Double Data Rate (DDR) SDRAM памяти, что позволяет значительно ускорить работу процессора, обеспечивая доступ к данным и программному коду на скорости до 4 гигабит в секунду. Благодаря использованию L3-кэш памяти для хранения большой части обрабатываемых данных, объем информации, передаваемой между процессором и основной оперативной памятью в каждый момент времени, становится минимальным. Это приводит к уменьшению объема данных, передаваемых через системный контроллер и снижению до минимума вероятности возникновения узких мест из-за появления нескольких одновременных потоков данных, передаваемых по системной шине. Оптимальная производительность компьютеров Apple достигается за счет эффективной работы всех уровней системной архитектуры. Основными особенностями такой архитектуры являются интегрированные интерфейсы ввода-вывода и быстрая шина PCI. Симметричная многопроцессорность позволяет достичь беспрецедентных показателей производительности при работе на двухпроцессорных системах Apple. Операционная система Mac OS X рассчитана на использование всего потенциала, заложенного в компьютере Power Mac G4. Mac OS X автоматически распределяет нагрузку между двумя процессорами,

позволяя всем приложениям достичь максимальной производительности. Mac OS X интеллектуально распределяет задачи приложений между процессорами, например, нагружая первый процессор сложным обсчетом трансформации изображения, а второй – созданием аудиофайла, значит, время выполнения обеих задач может быть уменьшено почти вдвое.

В отличие от других производителей Apple предлагает различные варианты, позволяющие свободно обмениваться информацией с системой Wintel, Atari и другими платформами. Возможно не только переносить файлы с одной платформы на другую, но и работать с ними. Сейчас Apple остается лидером в индустрии по применению новых технологий в своих продуктах. Пользователи могут быть уверены, что современные модели компьютеров Macintosh предлагают новейшие решения, существующие на данный момент на рынке. Компания дает пользователю те технологи, которые станут общедоступными на других платформах только через несколько лет [3].

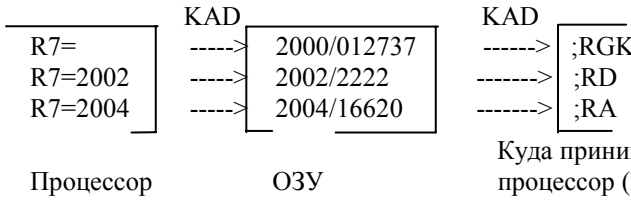
ЛИТЕРАТУРА

1. http://www.macwest.ru
2. http://www.apple.ru
3. http://www.3dnews.ru

ОРГАНИЗАЦИЯ ПОРТА ВЫВОДА ИЗ РЕГИСТРОВОГО АЛУ

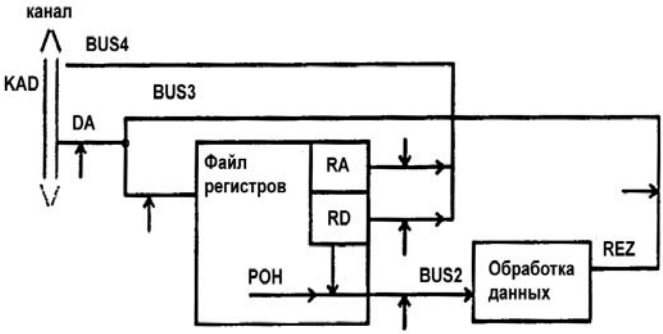
К.В. Климентьев, Е.В. Узбеков, А.А. Шило, судены гр. 574-1
ТУСУР, г. Томск, KLIM42rus@mail.ru

В соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2000г.) произведен анализ процесса ввода трех слов команды MOV #D,@#A.



Расширение формата команд CPU возможно с применением методов адресации [1].

Закончив прием первого(RGK), второго(RD1) и третьего(RA) слов команды MOV #D,@#A, процессор приступает к собственно исполнению команды MOV: вывод данных из RD1 по адресу, хранимому в RA(рисунок).



Фрагмент конфигурации РАЛУ

Системный канал представлен шиной адресов-данных (KAD).

Это происходит следующим образом:

1. BUS4:=RA ;Пересылка содержимого RA на BUS4
2. KAD:=BUS4 ;Загрузка канала адресом из RA
3. Чтение ОЗУ адреса, помещенного на шину KAD (синхронизация по сигналу – СИА)
4. BUS4:=RD1 ;Загрузка BUS4 содержимым RD1
5. KAD:=BUS4 ;Загрузка канала данными из RD1
6. Чтение ОЗУ данных KAD. Подтверждение от ОЗУ, что данные приняты (СИП).

На этом цикл ВЫВОД завершен.

Таким образом, для организации порта ввода-вывода при исполнении команды MOV #D,@#A группы R-M(регистр-память) необходимо иметь в составе регистрового АЛУ регистр команд, регистр данных и регистр адреса.

Дополнительно в файл рабочих регистров введен RD2 для возможности осуществлять работу с двумя операндами. Например,

RD1:=RD1+RD2.

Соответственно RD2 также должен быть включен в порт ввода данных.

Заметим, что в порт ввода данных могут быть включены и POH из-за связи BUS3:=DA, POH:=BUS3.

ЛИТЕРАТУРА

1. *Прищепа Л.С.* Проектирование центральных и периферийных устройств ЭВС. Ч. 1: Учеб. пособ. В 2-х разд. Томск ТМЦДО, 2004. Разд. 2. 214 с.

ПРОЕКТИРОВАНИЕ МОДЕЛИ ГИБКОЙ АВТОМАТИЗИРОВАННОЙ ЛИНИИ

К.В. Клюкин, студент гр. 572-1;
ТУСУР, г. Томск, т. 8-923-401-13-94, svarog@sibmail.com

Все большее значение в усовершенствовании учебного процесса занимает персональный компьютер. Известно, что применение средств программного обучения позволяет повысить успеваемость и ускорить процесс освоения материала в среднем на 25–30% при существенном облегчении труда преподавателя.

Современный уровень развития вычислительной техники и ее программного обеспечения открывает широкие возможности проектирования виртуальных тренажеров и установок.

Одним из практических применений компьютерной трехмерной графики является визуализация работы робототехнических систем.

В учебном процессе не всегда возможно использование реальных технологических объектов, так как это связано с высокой стоимостью оборудования, сложностью организации лабораторных установок. Кроме того, на нашей кафедре основное внимание уделяется проблемам управления системами, проблемам программирования систем автоматизации технологических процессов. Поэтому возникает необходимость создания виртуальной модели гибкой автоматизированной линии (ГАЛ).

Необходимо создать модель ГАЛ на основе виртуальных моделей сборочного робота, сварочного робота, копировально-фрезерного станка, технологического конвейера, склада. На разработанной модели ГАЛ представится возможность ознакомиться с принципами работы роботов, научиться управлять технологическим процессом обработки детали при последовательной и дискретной подаче деталей.

Прежде чем приступить к созданию модели сформулируем, что же такое ГАЛ. Гибкая автоматизированная линия – гибкая производственная система, в которой технологическое оборудование расположено в принятой последовательности технологических операций.

Все модели, входящие в ГАЛ, расположены в последовательности изображенной на рисунке.

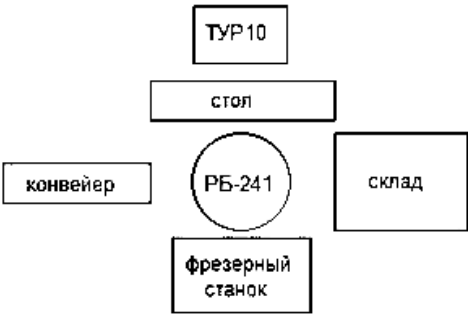


Схема расположения моделей на сцене

Модель сварочного робота создана на основе реального сварочного робота «ТУР-10». Основная область применения промышленных роботов «ТУР-10» – это автоматизация точечной и дуговой сварки, зачистка заусенцев после штамповочных операций, сортировка и отбраковка продукции, загрузка буферных межоперационных накопителей. Эти роботы имеют антропоморфный манипулятор с пятью или шестью звеньями в зависимости от модификации. Модель выполняет только необходимые нам функции реального робота, а именно проведение сварки.

Модель обеспечивает перемещение манипулятора робота по трем координатам в сферической системе координат; перемещение рабочего органа робота в автоматическом режиме согласно загруженной технологической программе; процесс сварки нескольких деталей; возможность изменять угловую скорость манипулятора в ручном и автоматическом режимах (группа скорости может принимать значения от 0 до 7).

Модель сборочного робота построена на основе робота РБ-241. Робот РБ-241 предназначен для автоматизации таких вспомогательных производственных операций, как загрузка станка заготовками обрабатываемых деталей; смена рабочих инструментов; транспортирование обрабатываемых деталей при помощи цепного транспортера; удаление стружек из зоны инструмента при помощи воздушной струи; подсчет обработанных деталей. Модель робота выполняет функцию загрузки станка заготовками обрабатываемых деталей. Модель обеспечивает движение рабочего органа робота в трехмерной декартовой системе координат по осям x, y и z; транспортировку детали при помощи схвата; возможность изменять линейную скорость манипулятора в ручном и автоматическом режимах (группа скорости может принимать значения от 0 до 7). Для обеспечения более удобного управления схват модели поворачивается на 360, а не на 180º как у предыдущей модели.

Модель копировально-фрезерного станка построена на основе станка 6Т12Ф-1. Станок выполняет функцию фрезерования детали сложной пространственной конфигурации. Модель обеспечивает следующие функции реального оборудования: перемещение стола в трехмерной декартовой системе координат по осям x, y и z; перемещение стола в автоматическом режиме согласно загруженной технологической программе; возможность задавать отклонение задаваемых значений. В столе фрезерного станка предусмотрен зазор, чтобы робот РБ-241 мог брать деталь не только при горизонтальном положении схвата, но и при вертикальном.

Детали подаются на конвейер автоматически через дискретные интервалы времени. Имеется возможность задавать интервалы времени, через которые деталь будет поступать на конвейер.

Предполагается, что объем склада не ограничен и изделия он может принимать в заданные дискретные моменты времени.

Управление всеми элементами ГАЛ производится с помощью технологических программ, адекватным реальным системам программирования соответствующих объектов управления.

При управлении сценой предусмотрено переключение между моделями. При этом изменяются фокусировка камеры и панель управления моделями.

На данной модели имеется возможность обучаться технологическому программированию как отдельных производственных единиц, так и взаимосвязанному программированию всей гибкой производственной линии.

Система находится на стадии разработки, и в дальнейшем планируется предусмотреть различные технологические программы для управления моделями, будет предусмотрена возможность наблюдения за работой всех моделей одновременно. Будет реализована обработка возможных ошибок, возникающих во время работы ГАЛ. Для более удобного обращения с программой будет разработан функциональный интерфейс.

ДИНАМИЧЕСКОЕ МОДЕЛИРОВАНИЕ ГИБКОЙ ПРОИЗВОДСТВЕЕНОЙ ЛИНИИ В СЕТЯХ ПЕТРИ

Н.Ю. Комарова, студентка гр. 572-1;
ТУСУР, г. Томск, т. 8-923-409-04-27, kisa2005@pochta.ru

Для проведения лабораторных работ по дисциплине «Гибкие производственные системы и робототехнические комплексы» были разработаны модели сборочного робота РБ241, покрасочного робота, сварочного робота ТУР-10 и модель фрезерного станка.

Известно, что металлорежущие станки и роботы, снабженные системой ЧПУ, являются основным видом заводского оборудования экономически развитых стран и предназначены для производства современных машин, приборов, инструментов и других изделий. Изучение принципов построения и программирования таких систем студентам технического университета необходимо изучать. Однако открытым остался вопрос о построении не отдельных элементов автоматизированной производственной системы, а о моделировании комплекса взаимодействующих технологических объектов.

Любая исследовательская, проектная, управленческая деятельность в определенной мере связана с моделированием. Чертеж детали, проект

станка или производственного участка, макет самолета или здания, системы уравнений, описывающих технологический процесс или движение кинематического механизма, – все это модели объектов изготовления, строительства и управления.

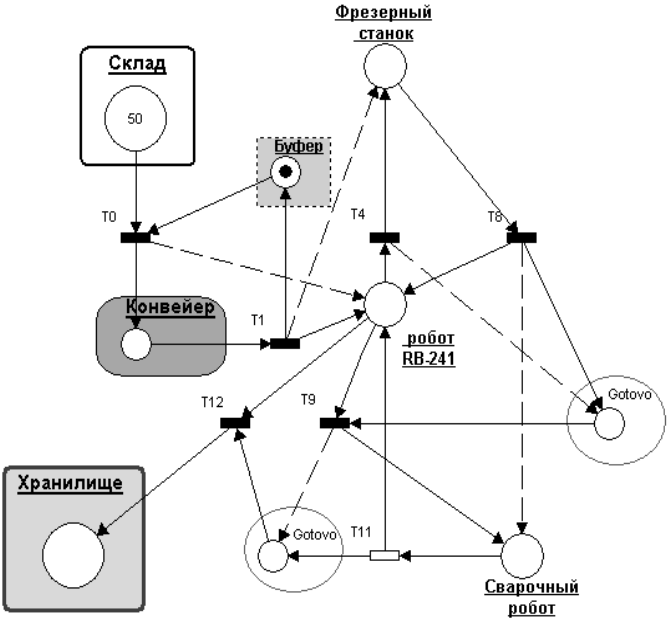
Многообразие объектов, целей и задач моделирования породило множество различных типов моделей.

Модель – это представление, как правило, в математических терминах того, что считается наиболее характерным в изучаемом объекте или системе. Ожидается, что, манипулируя представлением, можно получить новые знания о моделируемом явлении, избегая опасности, дороговизну или неудобства манипулирования самим реальным явлением.

Сети Петри представляют собой графическое и математическое средства моделирования, применимое к системам самых различных типов. Они представляют собой перспективный инструмент описания и исследования мультипрограммных, асинхронных, распределенных, параллельных, недетерминированных и/или стохастических систем обработки информации. В качестве графического средства сети Петри могут использоваться для наглядного представления моделируемой системы, подобно блок-схемам, структурным схемам и сетевым графикам. Вводимое в этих сетях понятие фишек (ресурсов) позволяет моделировать динамику функционирования систем и параллельные процессы. В качестве математического средства аналитическое представление сети Петри позволяет составлять уравнения состояния, алгебраические уравнения и другие математические соотношения, описывающие динамику систем. Сети Петри могут с успехом использоваться и теоретиками, и практиками, а, следовательно, становятся эффективным средством их взаимного общения: практики могут перенять у теоретиков более совершенную методологию построения моделей, а теоретики – научиться у практиков, как приблизить свои модели к реальности.

В проекте решается задача моделирования сетями Петри гибкой производственной линии (ГПЛ), состоящей из состоящую из модели сборочного робота, модели сварочного робота, модели копировально-фрезерного станка, модели технологического конвейера, модели склада, модели хранилища. Моделирование необходимо для исследования в динамике взаимодействия элементов ГПЛ, определения необходимых размеров накопителей для неравномерного поступления заготовок на входе ГПЛ, выявления необходимых синхронизаций и «узких» мест в работе системы.

Для моделирования пользуемся разработанной программой HPSim 1.1. Все модели входящие в ГПЛ изображены на рисунке.



Модель сети Петри

Описание модели

При старте симуляции сети необходимо поместить определенное количество необработанных деталей в «Склад», – склад необработанных деталей.

Запускаем эмулятор. Первым действием деталь поступает на «Конвейер» – это действие осуществимо в случае отсутствия на «Конвейере» другой детали. Выставлен знак готовности, т.е. конвейер свободен (фишка в «Буфере»).

Одновременно, когда деталь поступает на конвейер, идет проверка, свободен ли робот РБ-241 и в случае отсутствия у него детали, робот РБ-241 берет деталь с конвейера.

Одновременно с поднятием детали идет проверка, свободен ли фрезерный станок, чтобы ему передать деталь на обработку. И на буфер поступает фишка, показывающая, что конвейер свободен. Робот РБ-241 передает деталь. Фрезерный станок принимает деталь, и в то же время идет проверка, передана ли деталь на обработку.

Далее робот РБ-241 забирает обработанную деталь у фрезерного станка, и идет проверка, свободен ли сварочный робот, поступает другая необработанная деталь со склада на конвейер.

Робот РБ-241 передает деталь сварочному роботу, и в то же время идет проверка, передана ли деталь на обработку.

В то время пока сварочный робот обрабатывал деталь, с конвейера робот РБ-241 передал деталь на обработку фрезерному станку и следом на конвейер подается следующая необработанная деталь со склада.

Когда сварочный робот обработал деталь, ее берет РБ-241 и отправляет в *Хранилище*.

Робот РБ-241 передал деталь в хранилище. Затем последовательность повторяется до тех пор, пока не закончатся все детали.

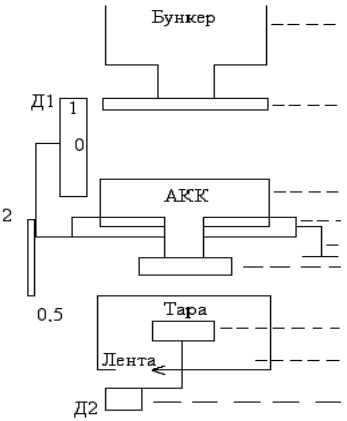
В модели предусмотрены не все возможные варианты работы системы, возникающие при решении данной задачи. Так, например, возникает вопрос, что делать, если одновременно пришел сигнал, что деталь изготовлена и на конвейере появилась очередная заготовка? Что должны делать роботы, если обработка на станке занимает длительное время? Что делать, если заготовки поступают с частотой, больше чем их в состоянии обработать данная система?

В дальнейшем разработка модели будет усложняться, а значит, можно воплотить такую систему, которая сможет работать заданный интервал времени в полностью автономном режиме без участия человека.

ВИЗУАЛИЗАЦИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ ИНТЕРФЕЙСНОГО МОДУЛЯ СОПРЯЖЕНИЯ

С.Л. Крыловский, М.Г. Власова – студенты 4 курса;
А.А. Шилов, студент 3 курса
ТУСУР, г. Томск, т. 8-903-951-1825

В данной работе была решена проблема ГПО по визуализации процесса проектирования интерфейсного модуля сопряжения в режиме запроса от объекта. Для решения использовалась теория, представленная в [1, 2]. Целью данной научно-исследовательской работы является создание простой и наглядной обучающей презентации, которая объединяет в себе все необходимые этапы модификации модуля сопряжения. Модификация касается подключения к базовой схеме узлов формирования запросов, сброса запросов и чтения флагов F5 и F6 состояния объекта дозирования сыпучих материалов. На этапе проектирования модуля сопряжения необходима визуализация метода «сверху вниз», а также визуализация модификации структурной схемы модуля сопряжения для работы в цикле ВВОД и ВЫВОД. После всех этапов модификации необходимо визуализировать электрическую функциональную схему модуля, правильность подключения к схеме узлов формирования запросов, сброса запросов и чтения флагов F5 и F6 с использованием общей шины.



Для решения проблемы была использована среда разработки MS Power Point. Была реализована визуализация технологического процесса на объекте автоматизации (рис. 1). В частности, реализованы основные этапы дозирования сыпучих материалов – поиск тары, дозирование, затаривание.

Рис. 1. Дозирующая установка (условно)

Также решена проблема модификации структурной схемы модуля сопряжения. Для более простого понимания был использован метод визуального запоминания, т.е. из начальной схемы сначала вырезаются ненужные узлы, а затем на их место устанавливаются необходимые части для решения заданной по варианту задания проблемы (рис. 2).

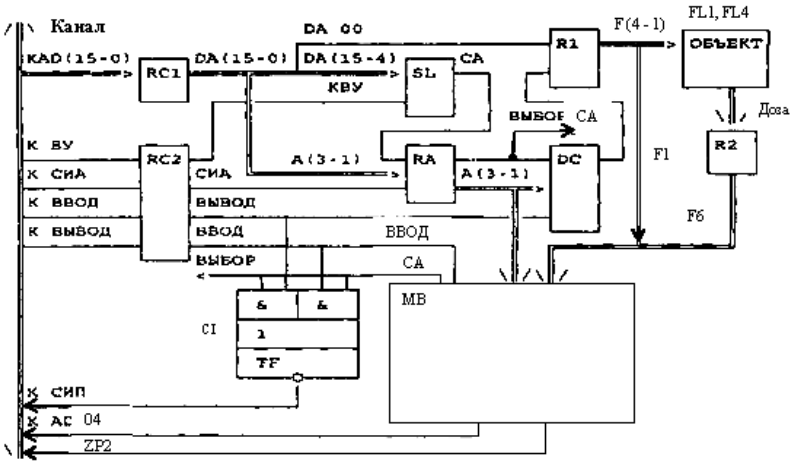


Рис. 2. Структурная схема модуля сопряжения

В результате был визуализирован процесс модификации модуля сопряжения, подключение основных узлов по варианту задания. Разработанный учебно-программный комплекс доступно и понятно помогает

студентам выполнить задание курсового проектирования в соответствии с вариантом, а именно произвести модификацию модуля сопряжения в режиме запроса от объекта.

ЛИТЕРАТУРА

1. *Прищепа Л.С.* Компьютерные средства в системах автоматизации и управления. Системотехника, вычислительные комплексы и сети ЭВС: Учебное методическое пособие к курсовому проектированию. Томск: ТМЦДО, 2003. 144 с.

2. Вестник Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. Спец. вып. Системная интеграция и безопасность. Томск: В-Спектр, 2006. 154 с.

АДАПТИВНАЯ ОБУЧАЮЩАЯ СИСТЕМА ПО КУРСУ «МЕТОДЫ ОПТИМИЗАЦИИ»

Г.И. Курманалиева, О.М. Раводин – научный руководитель
ТУСУР, 634034, Томск, пр. Ленина 50

Необходимость принятия наилучших решений так же стара, как само человечество. Испокон веку люди, приступая к осуществлению своих мероприятий, раздумывали над их возможными последствиями и принимали решения, выбирая тем или другим образом зависящие от них параметры – способы организации мероприятий. Одни решения человек принимает без специальных расчетов, просто опираясь на имеющийся у него опыт и на здравый смысл. Другие решения являются гораздо более ответственными. Для того, чтобы представить себе последствия, нужно провести расчеты. Выбранные решения должны по возможности гарантировать нас от ошибок, связанных с неточным прогнозированием, и быть достаточно эффективными для широкого круга условий. Для обоснования таких решений приводится в действие сложная система математических расчетов.

Методы управления сложными системами изучаются в ряде дисциплин учебного плана специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».

Мы считаем, что основой для изучения дисциплины должно являться учебное пособие, а автоматизированные обучающие системы (АОС) служат средством, позволяющим преподавателю избавиться от рутинной работы, интенсифицировать работу студентов, управлять процессом обучения при использовании дистанционных технологий, заставляющим преподавателя четко сформулировать основные положения дисциплины, детально продумать технологию проведения лабораторных и практических занятий.

Целью работы явилась разработка учебно-методического материала, тестовых вопросов и заданий в среде адаптивной обучающей системы «LirAOS» (разработанной и используемой в ТУСУР) по дисциплине «Методы оптимизации». Пользователям (студентам) начинающим работу с АОС «LirAOS», предлагается ознакомиться с теоретическими знаниями, ответить на вопросы, выполнить задания.

Пользователями данной АОС являются преподаватель, студент, а также методист-оператор. Методистом-оператором системы может быть преподаватель. Данный учебно-методический комплекс должен являться звеном взаимодействия между студентом и преподавателем.

Работа преподавателя с АОС заключается в следующих аспектах.

- Работа с методическим материалом: подбор текстовой информации по выбранной теме, формирование заданий на лабораторные и практические работы составление тестовых заданий.
- Формирование адаптивной «траектории» обучения, автоматически изменяющейся в зависимости от уровня знаний студента.
- Проведение статистической обработки результатов тестирования, выполнения заданий и экзаменов: определение качества усвоения и коррекция методических материалов, выставление итоговой оценки.
- Консультирование учащихся по проблемным вопросам.

Работа студентов с АОС заключается в следующих режимах.

1) Режим обучения: возможность изучения необходимой темы путем прочтения методического материала.

2) Режим тестирования: возможность прохождения тестирующих заданий по необходимой теме.

3) Режим получения и выполнения задания: получение задания по изучаемой теме, вход в моделирующую систему, позволяющую выполнить задание.

Работа методиста-оператора заключается в добавлении либо удалеении методического материала и тестовых заданий, предоставленных преподавателем.

Адаптивная система состоит из следующих модулей:

– редактор – программа, предназначенная для создания и редактирования файлов обучения или тестов;

– программа-сервер – программа для организации работы по локальной сети или сети Интернет;

– контрольно-обучающий модуль, предназначенный непосредственно для обучения студента и контроля уровня его знаний;

– проверочный модуль – программа для проверки целостности отчета, созданного контрольно-обучающим модулем.

Студенты работают только с обучающей программой.

Разработка методического материала велась в специальном редакторе АОС.

Учебно-методический материал составлен используя возможность «LirAOS» – правила перехода (АОС с использованием нелинейных алгоритмов). Это возможность изменять последовательность предъявления слайдов в зависимости от того или иного отклика учащегося на информационное воздействие, т.е. повторного возврата к слайдам, отражающим темы, которые учащийся недостаточно усвоил.

Также широко используется другая возможность «LirAOS» – вызывать исполняемые модули. Конкретное применение для демонстрации примеров и выполнения заданий.

Контрольные вопросы реализованы в виде тестов. В основном использованы тесты простого выбора:

– выбор одного варианта ответа из нескольких предлагаемых;

– выбор нескольких правильных ответов из предлагаемого списка.

Учебно-методический материал составлен таким образом, что охватывает тот минимум, необходимый для полного представления основ теории оптимизации.

АОС по «Методам оптимизации» содержит следующие главы:

– Процесс управления.
– Оптимизация процесса управления.
– Математическое описание объекта управления.
– Классификация задач оптимального управления.
– Основные понятия теории оптимизации.
– Линейное и нелинейное программирование.
– Итеративные методы поиска оптимума.
– Динамическое программирование.

СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОДУКЦИИ CPU КОРПОРАЦИИ «IBM»

А.Е. Леонов студент гр. 574-1

ТУСУР, г. Томск, KLIM42rus@mail.ru

В соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2006 г.) произведен анализ современного (на 2006 г) состояния продукции CPU компании (корпорации) IBM.

Основным и практически единственным конкурентом 54-разрядных микропроцессоров пост-RISC архитектуры Intel IA-64 с точки зрения производительности остается IBM Power 4.

Первоначальные утверждения разработчиков IA-64, что после появления микропроцессоров данной архитектуры RISC-архитектура будет побеждена и наступит эпоха «пост-RISC», пока не реализовалось. Рынку представлено уже второе поколение микропроцессоров IA-64, а лидером по производительности с плавающей запятой на тестах SPECfp2000 и Linpack (n = 100 и т = 1000) является RISC-процессор IBM Power 4. По целочисленной производительности (SPECint2000) лидирует 32-разрядные процессоры AMD Opteron и Intel Pentium 4, чуть опережая Power 4.

С появлением Madison (Третье поколение IA-64) производительность вырастет на 30–50%, но подрастет и производительность конкурентов (хотя, возможно, и не в такой степени). Основными соперниками IA-64 должны остаться 64-разрядные RISC-процессоры. Микропроцессоры Pentium 4 подошли к ситуации, когда они будут в не состоянии поддерживать характерные для современного развития информационных систем объемы оперативной памяти (имеется в виду емкость, доступная одному приложению) даже в ПК-серверах, а производительность этих микропроцессоров возрастет в этом году, скорее всего, не очень сильно. Появились 64-разрядные AMD Opteron, но они вряд ли будут существенно быстрее Pentium 4/Xeon, по крайней мере, в 2003 г.

В условиях, когда будущее семейства Sun UltraSPARC как возможного лидера производительности вызывает определенный скепсис, флагманом RISC-архитектуры могут оказаться микропроцессоры Power 4, а в будущем– Power 5. Если проанализировать характеристики быстродействия Power 4, то обнаружится, что он имеет наиболее сбалансированную производительность: у Alpha и Itanium 2-«провалы» с целочисленной производительностью, у Pentium 4 – отставания по плавающей запятой.

Корпорация IBM представила два сервера из серии eServer iSeries, ставших первыми компьютерами на основе ее нового 64-разрядного RISC-процессора Power 5, а 13 июля анонсировала использующие этот процессор три модели Unix – серверов pSeries. Появление Power 5 способно серьезно изменить расстановку в мире коммерческих Unix платформ в пользу их корпораций. После выхода в конце 2001 г. предшественника этого процессора, Power 4, в котором впервые была реализована архитектура «два процессорных ядра на одном кристалле», «Голубому гиганту» удалось значительно увеличить свою долю на рынке Unix-систем и свести к минимуму отставания от занимающих здесь первое и второе место компаний HP и Sun.

Учитывая огромные ресурсы, которые IBM выделила на продвижение архитектуры Power, а также отказ HP от дальнейшего развития своих RISC-серверов, которые постепенно заменяются на платформе Itanium, и вынужденно пересмотренные Sun планы выпуска UltraSPARC (в частности, с 2006 г. ее серверах старшего класса будет использоваться процессор SPARC 64 VI), многие наблюдатели рассматривают Power 5 как главную надежду сторонников RISC-технологий и наиболее сильного конкурента Intel в сфере 64-разрядных вычислений.

Идея массового параллелизма, на основе которой работает Cell, была заложена в «клеточную структуру», в которой используется множество однотипных процессоров (от 10 тыс. до 1 млн.), каждый из которых оснащен собственным контроллером RAM и определенным объемом оперативной памяти. Благодаря встроенной возможности объединения чипов Cell, микропроцессоры, являющиеся сегодня «индивидуальными островками», будут связаны между собой более тесно, благодаря чему сеть на основе таких процессоров превратится в одну унифицированную «суперсистему» [1–3].

ЛИТЕРАТУРА

1. www.osp.ru
2. www.butemag.ru
3. www.3dnews.ru

ПОРТ ВВОДА-ВЫВОДА РЕГИСТРОВОГО АЛУ ДЛЯ ВВОДА ТРЕТЬЕГО СЛОВА КОМАНДЫ

А.Е. Леонов, А.А. Шилов студенты гр. 574-1
ТУСУР, г. Томск, opk@ms.tusur.ru

В системе (рис. 1) на базе процессора, включающего регистровое АЛУ, обмен с периферией (ОЗУ, ВУ) осуществляется с помощью команд группы R-M (регистр-память).

Например, команда MOV #D,@#A имеет формат три слова:

	KAD		KAD	
R7=2000	----->	2000/012737	------>	;RGK
R7=2002	----->	2002/2222	------->	;RD
R7=2004	----->	2004/16620	------->	;RA
процессор		ОЗУ	куда принимает процессор (ВВОД)	

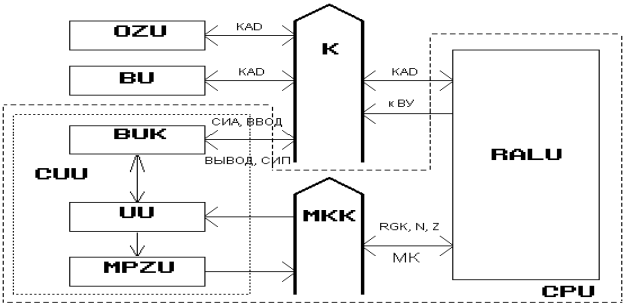


Рис. 1. Система

Аппаратные средства поддержки обмена процессора с периферией включены в РАЛУ. Здесь возможны следующие соглашения.

Каждый регистр подключен к каналу и каждый регистр связан с каждым (рис. 2).

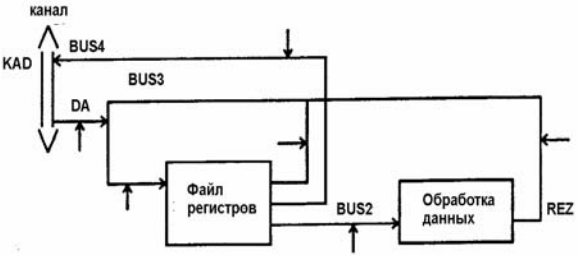


Рис. 2. Фрагмент обсуждаемой конфигурации РАЛУ. Управление шиной обозначено стрелкой

При анализе требований предложенного выше СОГЛАШЕНИЯ приходим к следующим результатам (рис. 3).

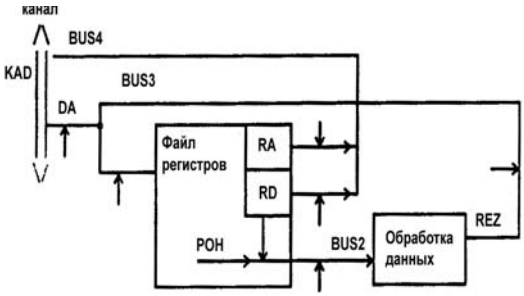


Рис. 3. Фрагмент принятой конфигурации РАЛУ. Системный канал представлен шиной адресов-данных (KAD)

Только регистры RA и RD подключены к каналу, а остальные регистры РАЛУ имеют возможность передать данные через шины BUS2, REZ и BUS3 на RA и RD. Это, конечно, удлиняет цепи передачи дан-

ных, снижает быстродействие РАЛУ, но исключает аппаратные затраты, необходимые для подключения регистров непосредственно к шине BUS4.

Аппаратные средства поддержки приема из ОЗУ третьего слова интерпретируемой команды показаны на рис. 4.

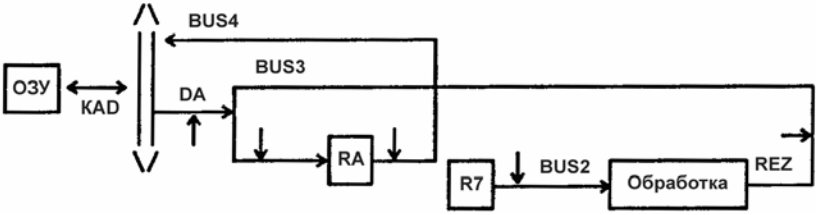


Рис. 4. Прием третьего слова команды.

Обработка состоит в пересылке содержимого R7 с шины BUS2 на шину REZ; МКК – канал микрокоманд

Пусть R7 = 2004. Тогда: последовательность пересылок.

1. BUS2:=R7 ;Пересылка содержимого R7 на BUS2
2. REZ:=BUS2 ;Пересылка содержимого R7 из BUS2 на REZ
3. BUS3:=REZ ;Загрузка шины BUS3 с шины REZ
4. RA:=BUS3 ;Запись адреса в RA с шины BUS3
5. BUS4:=RA ;Загрузка шины BUS4 адресом из RA
6. KAD:=BUS4 ;Загрузка канала адресом 3-го слова с BUS4
7. Чтение ОЗУ адреса, помещенного на шину KAD (синхронизация по сигналу – СИА)
8. Загрузка шины KAD содержимым адреса (третье слово команды). (СИА), (ВВОД). Подтверждение от ОЗУ, что третьего слово в канале (СИП), (СИА), (ВВОД)
9. DA:=KAD ;Чтение канала KAD на шину DA
10. BUS3:=DA ;Загрузка BUS3 с шины DA
11. RA:=BUS3 ;Содержимое с шины BUS3 загружается в RA

Таким образом, в соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2000 г.) произведен анализ процесса ввода третьего слова команды MOV #D,@#A в регистровом АЛУ системы.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЛЯ ЛАБОРАТОРНОГО ПРАКТИКУМА ПО UML

И.В. Мельникова, студентка 5 курса каф. КИБЭВС;
Н.А. Новгородова, ассистент каф. КИБЭВС
ТУСУР, г. Томск, e-mail: gammi@sibmail.com

Данная система ориентирована на изучение унифицированного языка моделирования UML. Язык UML предназначен для описания, визуализации и документирования системы на базе объектно-ориентированного подхода с целью последующего использования моделей процессов для реализации их в виде программного обеспечения.

Поддержка нотации UML есть во многих CASE-средствах. Наиболее распространенными из них являются MS Visio и Rational Rose. В отличие от MS Visio, который предназначен больше для визуализации данных, Rational Rose подходит для проектирования программных систем любой сложности. Можно сказать, что Rational Rose является графическим редактором UML диаграмм.

При использовании разрабатываемого практикума приобретаются практические навыки по построению моделей системы, а также глубокие знания CASE-средства Rational Rose, которая позволяет детально описывать, что система содержит и как функционирует. Одно из его главных достоинств – это доступное визуальное представление создаваемой сложной информационной системы [1].

Автоматизированная система для лабораторного практикума по UML должна быть удобна и легка в использовании, интерфейс должен быть понятен всем пользователям, но в то же время быть достаточно функциональной.

В данную систему входят следующие основные модули:

– теоретический материал по UML,
– лабораторные работы и задания к ним,
– методические указания к лабораторным работам,
– проверка приобретенных знаний.

Теоретический материал изложен очень доступно с множеством примеров, а практическая часть представляет собой ряд лабораторных работ, выполнение которых заканчивается контрольным тестированием. Контрольное тестирование дает возможность перейти к выполнению следующей лабораторной работы [2, 3].

Так как в рамках UML все представления о модели сложной системы фиксируются в виде специальных графических конструкций, которые называются диаграммами, то, чтобы описать одну сложную модель, необходимо построить некоторое количество диаграмм, отражающих

аспекты поведения или структуру системы. Таким образом, для построения каждой диаграммы имеется отдельная лабораторная работа, которая представляет собой подробное пошаговое описание.

Необходимо отметить функциональность системы, которая содержит поиск и вспомогательные разделы для изучения и выполнения лабораторных работ.

Рабочий материал системы написан на HTML. Проведение лабораторных работ осуществляется с помощью CASE-средства Rational Rose.

ЛИТЕРАТУРА

1. *Леоненков А.В.* Объектно-ориентированный анализ и проектирование с использованием UML и Rational Rose. БИНОМ. 2006. 320 с.

2. http://www.intuit.ru

3. *Буч Г., Рамбо Д., Джекобсон А*. Язык UML. Руководство пользователя.

УНИВЕРСАЛЬНОЕ УСТРОЙСТВО УДАЛЕННОГО УПРАВЛЕНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ BLUETOOTH®

А.Н. Мертвецов, студент 5 курса; Л.А. Торгонский, к.т.н., доцент

ТУСУР, г. Томск, т. 56-17-66, axid@ms.tusur.ru

Технология Bluetooth® с большой скоростью проникает в новые области промышленности, появляются устройства, где она ранее никогда не использовалась. Технология Bluetooth® нашла свое применение и во многих бытовых приборах – микроволновые печи, холодильники, телевизоры и т.д. Многие современные компьютеры имеют Bluetooth® интерфейс [1].

Bluetooth – это технология передачи данных по радиоканалу на короткую дистанцию, позволяющая осуществлять связь беспроводных телефонов, компьютеров и различной периферии при отсутствии прямой видимости.

Технология Bluetooth® предполагает объединение всех устройств находящихся в доме, производственном помещении на расстоянии до 100 м в одну или несколько сетей.

Устройство удаленного управления позволит управлять любым прибором, поддерживающим соответствующие профили, определенные в спецификации Bluetooth®. Функциональные возможности устройства удаленного управления определены следующим образом [2, 3].

- управление перемещением,
- действие над доступной информацией,
- прием и передача звуковой информации от телефона,

– изменение громкости проигрывания, телефонного разговора,

– управление телефонным разговором,

– возможность программирования дополнительных функций управления пользователем.

Пульт управления может быть использован как беспроводная телефонная трубка. Для управления перемещением необходимо изменять положение устройства управления в пространстве в соответствующем направлении. Информацию о направлении перемещения получаем от датчика ускорения (акселерометра).

Устройство работает со следующими профилями Bluetooth®: HID Keyboard и Headset.

Human Interface Device Profile (HID) – обеспечивает поддержку устройств с HID (Human Interface Device), таких как мышки, джойстики, клавиатуры и др. Использует медленный канал, работает на пониженной мощности.

Headset Profile (HSP) – профиль используется для соединения беспроводной гарнитуры и телефона, который поддерживает минимальный набор AT-команд спецификации GSM 07.07 для обеспечения возможности совершать звонки, отвечать на звонки, завершать звонок, настраивать громкость [4, 5].

Для индикации работы служат два светодиода:

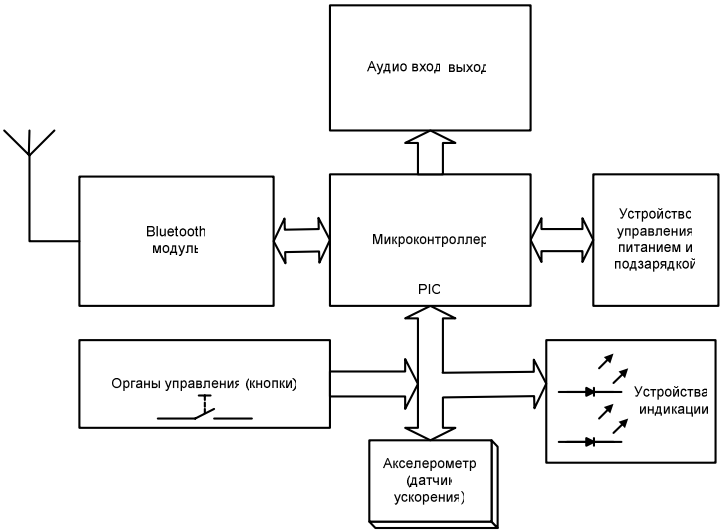
– индикация состояния соединения,

– индикация разряда элементов питания (заряда).

Устройство управления работает от встроенных литий-полимерных аккумуляторов, заряд которых осуществляется посредством подключения пульта к интерфейсу USB. Также через интерфейс USB возможны обновление программного обеспечения и обмен данными.

На рисунке показана структурная схема пульта дистанционного управления. Структура реализуется на базе множества готовых Bluetooth®-модулей. Микросхема BC31A223A фирмы CRS для приведенной структуры содержит: Bluetooth®-модуль, микроконтроллер, аудиовход и выход (с усилителями), модуль управления питанием и подзарядкой, параллельный интерфейс ввода-вывода.

Из названного состава отдельными конструктивными объектами являются кнопки, элементы индикации и датчик пространственных движений по двум координатам с четырьмя степенями свободы (акселерометр). Акселерометр выпускается в виде микросхемы MMA7260QT (фирма Freescale Semiconductor). Микросхема имеет выбираемую чувствительность. Подключение акселерометра к модулю BC31A223A предполагает применение микросхемы ADG811 фирмы Analog Devices для преобразования сигналов датчика в сигналы уровней логической 1 и 0.



Структура устройства удаленного управления

Кнопки, элементы индикации, сигналы с микросхемы ADG811 подключены на входы-выходы параллельного порта микросхемы BC31A223A.

Программой работ предусматриваются отработка принципиальной схемы устройства, проектирование конструкции и программирование дистанционного пульта. Для программирования устройства имеется фирменная интегрированная среда проектирования BlueLab®, в которой используется синтаксис языка С.

ЛИТЕРАТУРА

1. *Семенов Ю.А., Bluetooth.* http://book.itep.ru/4/41/bluetooth.htm.

2. *Кессених В., Иванов Е., Кондрашов З.* Bluetooth: Принципы построения и функционирования. http://www.chipinfo.ru/literature/chipnews/200107/8.html

3. *Specification* of the Bluetooth System., 4 November 2004. 1230 с.

4. *Headset* profile, 22 February 2001. 30 с.

5. *Craig Ranta, Steve McGowan.* Human interface device (HID) profile, 2003. 123 с.

6. © CSR plc, BlueCore3-Audio Flash Data Sheet, April 2006, 99 с.

7. © *Analog* Devices, ADG811/ADG812/ADG813. 2004, 16 с.

8. © *Freescale* Semiconductor, ±1g – 6g Three Axis Low-g Micromachined Accelerometer. 2006, 11 с.

ЭНЕРГОСБЕРЕГАЮЩИЙ СПОСОБ РЕГУЛИРОВАНИЯ ПРОЦЕССА СУШКИ ЗЕРНА

А.В. Муравьев, аспирант

ТУСУР, г. Томск, т. 8-906-949-37-22, e-mail: mawww@mail2000.ru

Требования, предъявляемые к автоматическим подсистемам регулирования влажности зерна, сводятся к следующему. Диапазон регулирования, исходя из нормированный значений кондиционной влажности основных зерновых культур для различных зон страны, можно принять от 13 до 18%. Погрешность регулирования при сушке зерна различных культур, учитывая влияние многих факторов на показания поточных влагомеров, не должна превышать 1,5% [1].

Возмущения по заданию не характерны для данной подсистемы, так как регулятор влажности должен работать в конкретных зональных условиях на одной уставке датчика, соответствующей кондиционной (по зоне) влажности зерна. К типовым возмущениям в данном случае относят ступенчатое изменение начальной влажности зерна, наблюдаемое при смене партий зерна, и возмущения в виде стационарной случайной функции, характеризующей совокупное действие внутренних и внешних возмущений. В первом случае, поскольку длительные отклонения конечной влажности зерна от кондиционного значения недопустимы, желательный характер переходного процесса при действии ступенчатого возмущения возможно обеспечить при условии минимума интегрального квадратического критерия качества:

$$I = \int_0^\infty \left[\Delta\omega(t)\right]^2 dt, \qquad (1)$$

где $\Delta\omega(t)$ – отклонение регулируемой величины от заданного значения в переходном процессе. Однако использование этого критерия может привести к сильным колебательным процессам в подсистеме, что недопустимо. Поэтому к рассматриваемому критерию целесообразно ввести ограничения на заданную степень затухания, выбираемую обычно в пределах $\psi = 0{,}85 \ldots 0{,}9$, что соответствует показателю колебательности $M_к = 1{,}7$.

При действии типовых возмущений, имеющих характер случайной функции времени $[\omega_{сн}(t)]$, подсистема должна обеспечить минимальное значение среднеквадратической погрешности регулирования (при доверительной вероятности 0,95), что не должно превышать заданного значения.

Объект регулирования влажности зерна в шахтных сушилках – это сушильная камера. Выходным параметром объекта (регулируемым) яв-

ляется влажность зерна $\omega_{ск}$, выходящего из сушильной камеры, а входным параметром (по каналу управления) – регулирующее воздействие, приводящее к изменению производительности сушилки $Q_{ск}$. Основное внешнее возмущение, действующее на объект, – изменение влажности поступающего на сушку зерна $\omega_{сн}$.

Передаточные функции по каналу управления и по каналу возмущения описываются следующими выражениями:

$$W_{qw}(p)=\frac{k_{qw}\,\mathrm{e}^{-p\tau_{qw}}}{T_{qw}p+1}, \tag{2}$$

$$W_{fw}(p)=k_{ww}\,\mathrm{e}^{-p\tau_{ww}}\ . \tag{3}$$

Для рассматриваемого объекта регулирования с передаточной функцией, описываемой выражением (2), применим типовой ПИ-регулятор.

Следующий этап синтеза подсистемы состоит в определении коэффициента передачи $k_{р}$ и постоянной времени $T_{и}$ регулятора. Однако в данном случае возникают существенные трудности, заключающиеся в следующем. Как показали исследования, параметры передаточных функций $W_{qw}(p)$ и $W_{fw}(p)$ объекта T_{qw}, τ_{qw}, k_{qw} и k_{ww}, τ_{ww} существенно непостоянны и изменяются в широких пределах в зависимости от производительности сушилки. Поэтому зерносушилка как объект регулирования влажности зерна относится к объектам с переменными параметрами, которые необходимо рассматривать как нелинейные объекты.

Параметры передаточной функции по каналу возмущения зависят от производительности зерносушилки $Q_{ск}$ и изменяются в широких пределах, поэтому создание комбинированной системы постоянной структуры, в которую вводится корректирующий контур по внешнему возмущению, является нецелесообразным. В качестве повышения качества регулирования влажности зерна можно использовать систему регулирования влажности с переменной структурой. Одним из вариантов такой системы может быть система с ПИ-регулятором, в котором коэффициент передачи $k_{р}$ и постоянная интегрирования $T_{и}$ автоматически изменяются по определенной зависимости от производительности сушилки.

ЛИТЕРАТУРА

1. *Е.В. Картин.* Автоматизация технологических процессов пищевых производств. 2-е изд., перераб. и доп. М.: Агропромиздат, 1985. 536 с.

2. *Гуляев Г.А.* Оптимизация управления шахтной зерносушилкой // НТБ / ВИМ. 1986. Вып. 63.

ПРИМЕНЕНИЕ СИСТЕМНОГО АНАЛИЗА ПРИ РАЗРАБОТКЕ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Н.А. Новгородова, ассистент; Е.Ю. Ерлыков, А.Ю. Журавлева, С.Ю. Исхаков, С.С. Карпачев, Н.В. Хорошев, студенты 4 курса

ТУСУР, г. Томск, т. 52-79-42, pna@keva.tusur.ru

При разработке сложных систем различного назначения практикуется применение системного анализа. Разрабатываемая система нацелена на упрощение документооборота кафедры и вуза в целом. Для решения столь многогранной задачи необходимо вначале структурировать ее и выделить основные цели.

В разработке было решено использовать системный подход, т.е. подход к исследованию объекта как к системе, в которой выделены элементы, внутренние и внешние связи, наиболее существенным образом влияющие на исследуемые результаты его функционирования, а цели каждого из элементов, – исходя из общего предназначения объекта. Основными чертами системного подхода являются целостность, иерархия и структуризация целей и задач [1].

Вся система состоит из множества документов, из которых основными являются государственные стандарты, учебные планы, рабочие планы занятий, извещения поручений по кафедрам и журнал распределения нагрузки преподавателей. Построив электронные версии этих документов и связав их в целостную рабочую систему, можно добиться основной цели – введения электронных журналов для каждого преподавателя.

Системный подход также называют методом математической дедукции, т.е. переход от общего к частному. Федеральным агентством по образованию разрабатываются ГОС на различные специальности, на основе которых формируются учебные планы занятий [2].

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 указанно 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.

В результате глубокого изучения предметной области задачи и применения системного подхода были выделены следующие цели и задачи.

1. Создание электронного документа ГОС с целью контроля учебных планов на соответствие государственным стандартам. Для этого необходимо:

– для каждого компонента разных разделов указать набор дисциплин и минимальное количество часов;

– определить квалификации выпускника;

– определить срок освоения программы;

– определить области, объектов и вида профессиональной деятельности.

2. Создание конструктора учебных планов с целью быстрой и гибкой разработки новых учебных планов и введение их в действие. Для этого требуется:

– вести базу учебных планов;

– для каждой дисциплины в учебном плане указывать общее количество часов, часов в неделю и вид отчетности в каждом семестре;

– составлять график учебного процесса с распределением видов занятий по курсам и неделям;

– обеспечить проверку всех указанных значений на соответствие ГОСТ;

– обеспечить гибкое и быстрое создание и модификацию различных вариантов учебных планов.

3. Создание конструктора рабочих планов занятий для распределения по неделям общего количества часов дисциплин, изучаемых группой в семестре. Для этого нужно:

– определить группы, совместно изучающие дисциплины в семестре;

– составить рабочий план занятий для каждой группы, обучающейся на кафедре на данный семестр;

– обеспечить проверку количества часов в соответствии с учебным планом.

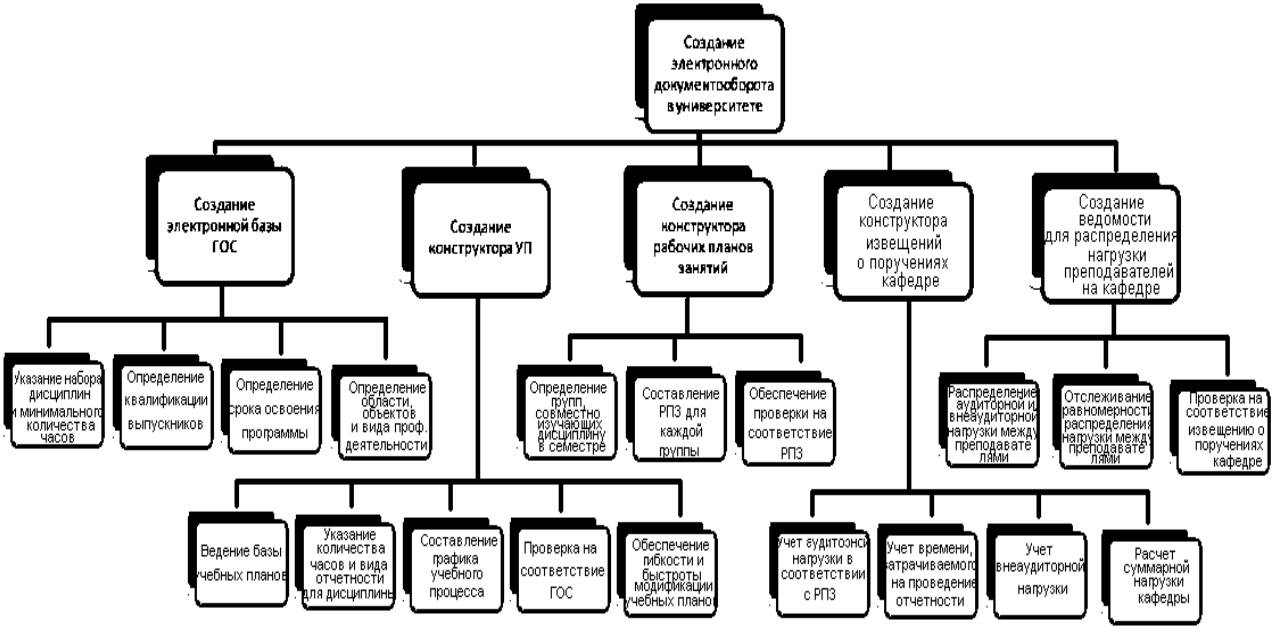
4. Создание конструктора извещений о поручениях кафедре с целью информирования других кафедр о количестве часов по каждой дисциплине, преподаваемой информируемой кафедрой. Следовательно, при составлении данного документа необходимо:

– учесть аудиторную нагрузку кафедры в соответствии с РПЗ;

– учесть нагрузку кафедры, связанную с соответствующими видами отчетности (экзамен, зачет, курсовая работа и т.д.), основанную на соответствующих приказах ректора;

– учесть внеаудиторную нагрузку кафедры, связанную с дипломными проектами, УНИР, преддипломными и другими видами практик и т.д.;

– рассчитать общую суммарную нагрузку кафедры.



Дерево целей и задач создания систем электронного документооборота вуза

5. Создание ведомости для распределения нагрузки преподавателей на кафедре. Для этого требуется:

– распределить аудиторную и внеаудиторную нагрузку всех преподавателей кафедры в соответствии с ведомостью о поручениях кафедре;

– отслеживать равномерность распределения нагрузки между преподавателями;

– рассчитать суммарную нагрузку преподавателя и общую кафедральную нагрузку и проверка на соответствие с нагрузкой, указанной в извещении о поручениях кафедре.

Схематично результат нашего анализа задачи представлен на рисунке.

ЛИТЕРАТУРА

1. *Блауберг И.В.* Проблема целостности и системный подход. М.: Эдиториал УРСС, 1977. 450 с.

2. *Дружинин В.В., Конторов Д.С.* Системотехника. М.: Радио и связь, 1985. 200 с.

OPENGL ГРАФИКА КАК ИНСТРУМЕНТ СОЗДАНИЯ МОДЕЛИ ГИБКОЙ АВТОМАТИЗИРОВАННОЙ ЛИНИИ (ГАЛ)

А.В. Пестеха, студент гр. 572-1;

ТУСУР, г. Томск, т. 8-960-973-39-82, stout@sibmail.com

Компьютерная графика в настоящее время уже вполне сформировалась как наука. Существует аппаратное и программное обеспечение для получения разнообразных изображений – от простых чертежей до реалистичных образов естественных объектов. Компьютерная графика используется практически во всех научных и инженерных дисциплинах для наглядности восприятия и передачи информации.

Целью нашего проекта является визуализация работы гибкой автоматизированной линии (ГАЛ), основанной на совместной работе сварочного робота «ТУР-10», сборочного робота «РБ-241» и копировально-фрезерного станка. На разработанной модели ГАЛ студенты смогут научиться программировать технологические процессы в гибких производственных системах.

Проект реализован в интегрированной среде визуального программирования Delphi 7.0 с использованием стандартной графической библиотеки OpenGL.

Система OpenGL – это графический стандарт, который предоставляет широкие возможности, несмотря на то, что поддерживает простейшую модель программирования. Ее процедурный интерфейс позво-

ляет программистам легко и эффективно описывать как простые, так и комплексные задачи воспроизведения. Поскольку OpenGL применяется только для воспроизведения, то она может включаться в состав любой не только графической (Windows 95 и Windows NT), но и консольной операционной системы.

Приведем основные достоинства OpenGL.

– Стабильность. OpenGL – устоявшийся стандарт, действующий уже более шести лет. Все вносимые в него изменения предварительно анонсируются и реализуются таким образом, чтобы гарантировать нормальную работу уже написанного программного обеспечения.

– Надежность. Все приложения, использующие OpenGL, гарантируют одинаковый визуальный результат вне зависимости от используемого оборудования и операционной системы.

– Переносимость. Приложения, использующие OpenGL, могут запускаться на персональных компьютерах, рабочих станциях или суперкомпьютерах.

– Простота использования. OpenGL хорошо структурирована. Ее драйверы включают информацию об основном оборудовании, освобождая разработчика от необходимости проектирования для специфических особенностей графических устройств.

Перечислим основные возможности, которые OpenGL предоставляет разработчикам:

– геометрические примитивы (точки, линии и многоугольники);

– растровые примитивы (битовые массивы и прямоугольники пикселов);

– работа с цветом в RGBA и индексном режимах;

– видовые и модельные преобразования;

– удаление невидимых линий и поверхностей;

– прозрачность;

– использование B-сплайнов для рисования линий и поверхностей;

– наложение текстуры;

– применение освещения;

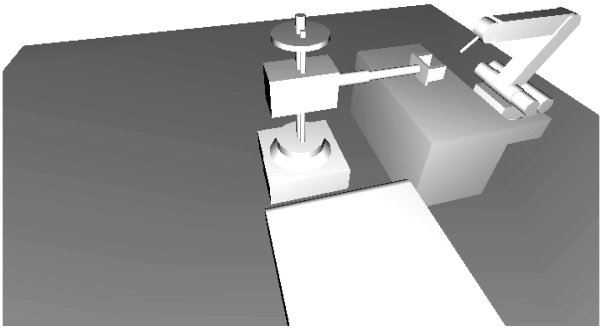
– использование плавного сопряжения цветов, устранения ступенчатости, «тумана» и других эффектов;

– использование списков изображений.

Возможности этой графической системы очень широки и достаточны для решения задачи визуализации работы робота.

В настоящее время существует графическая библиотека GLScene, которая позволяет значительно упростить работу с 3D-графикой в OpenGL. GLScene – это объектная надстройка над OpenGL для Borland Delphi. Работа в GLScene настолько проста, что даже для создания

сложных 3D-объектов не требуется каких-либо навыков работы в OpenGL. В связи с этим данная библиотека активно использовалась при создании виртуальной модели ГАЛ. Стоит заметить, что упрощается не только процесс создания моделей, но и процесс работы с ними, так как каждый элемент модели является объектом, а следовательно, имеет свойства и события, с помощью которых мы можем, например, без особых сложностей привести роботов в движение: чтобы, например, повернуть робота вокруг своей оси, нужно повернуть лишь основание робота, остальные его части повернуться автоматически, так как «привязаны» к основанию. Сцена с моделями роботов представлена на рисунке.



Модели роботов, входящих в гибкую автоматизированную линию

На рисунке представлены роботы РБ-241 – сборочный робот, ТУР-10 – сварочный робот и конвейер. Сборочный робот перемещает детали с конвейера на рабочий стол сварочного робота для дальнейшей обработки, после обработки перемещает деталь на склад и так далее.

ПОРТ ВВОДА-ВЫВОДА РЕГИСТРОВОГО АЛУ ДЛЯ ВВОДА ВТОРОГО И ТРЕТЬЕГО СЛОВ КОМАНДЫ

Е.Р. Плотникова студенка гр. 71-з; А.Е. Леонов, А.А. Шилов, Е.В. Узбеков, К.В. Климентьев, К.В. Ван-Пин – студенты гр. 574-1
ТУСУР, г. Томск; KLIM42rus@mail.ru

В соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2000 г.) произведен анализ процесса ввода первого слова команды MOV #D,@#A в регистровом АЛУ (РАЛУ) системы.

В системе (рис. 1) на базе процессора, включающего регистровое АЛУ, обмен с периферией (ОЗУ, ВУ) осуществляется с помощью команд группы R-M (регистр-память).

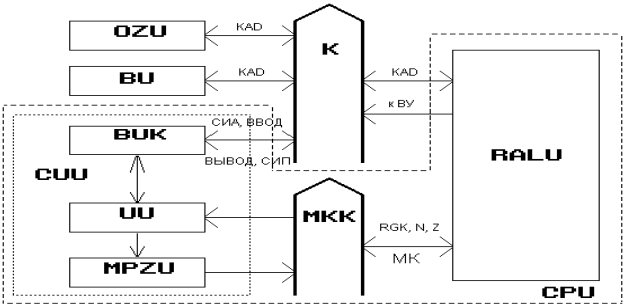
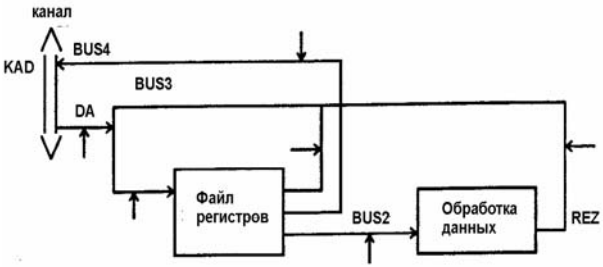


Рис. 1. Система

Например, команда MOV #D,@#A имеет формат три слова:

	KAD		KAD	
R7=2000	----->	2000/012737	------>	;RGK
R7=2002	----->	2002/2222	------->	;RD
R7=2004	----->	2004/16620	------->	;RA
процессор		ОЗУ	куда принимает процессор (ВВОД)	

Аппаратные средства поддержки обмена процессора с периферией включены в РАЛУ. Здесь возможны следующие соглашения:



Каждый регистр подключен к каналу и все регистры связаны между собой (рис. 2).

Рис. 2. Фрагмент обсуждаемой конфигурации РАЛУ. Управление шиной обозначено стрелкой

При анализе требований предложенного выше СОГЛАШЕНИЯ приходим к следующим результатам (рис. 3).

Только регистры RA и RD подключены к каналу, а остальные регистры РАЛУ имеют возможность передать данные через шины BUS2, REZ и BUS3 на RA и RD. Это, конечно, удлиняет цепи передачи дан-

ных, снижает быстродействие РАЛУ, но исключает аппаратные затраты, необходимые для подключения регистров непосредственно к шине BUS4.

Аппаратные средства поддержки приема из ОЗУ первого слова интерпретируемой команды показаны на рис. 4.

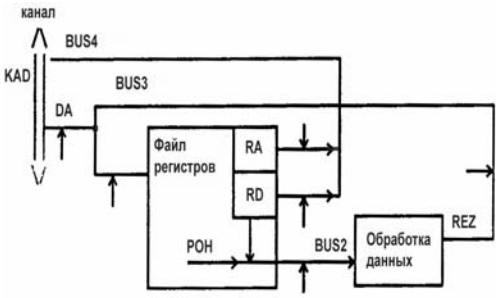


Рис. 3. Фрагмент принятой конфигурации РАЛУ. Системный канал представлен шиной адресов-данных (KAD)

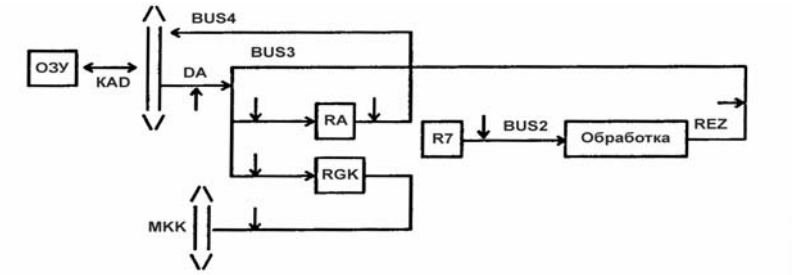


Рис. 4. Прием первого слова команды. Обработка состоит в пересылке содержимого R7 с шины BUS2 на шину REZ; МКК – канал микрокоманд

Пусть R7=2000. Тогда: последовательность пересылок.

1. BUS2:=R7 ;Пересылка содержимого R7 на BUS2
2. REZ:=BUS2 ;Пересылка содержимого R7 из BUS2 на REZ
3. BUS3:=REZ ;Загрузка шины BUS3 с шины REZ
4. RA:=BUS3 ;Запись адреса в RA с шины BUS3
5. BUS4:=RA ;Загрузка шины BUS4 адресом из RA
6. KAD:=BUS4 ;Загрузка канала адресом 1-го слова с BUS4
7. Чтение ОЗУ адреса, помещенного на шину KAD (синхронизация по сигналу – СИА)
8. Загрузка шины KAD содержимым адреса (первое слово команды). (СИА), (ВВОД). Подтверждение от ОЗУ, что первое слово в канале (СИП), (СИА), (ВВОД)
9. DA:=KAD ;Чтение канала KAD на шину DA первого слова
10. BUS3:=DA ;Загрузка BUS3 с шины DA первым словом
11. RGK:=BUS3 ;Содержимое с шины BUS3 загружается в RD1
12. MKK:=RGK ;Передача первого слова через микроканал MKK

ДОСТУП К БАЗАМ ДАННЫМ ИЗ WEB-ПРИЛОЖЕНИЯ

А.Г. Полянский, студент гр. 572-1.; Н.А. Новгородова, ассистент
ТУСУР, г. Томск, т. 8-906-947-37-42, icarus@rambler.ru

Возможности современных баз данных не ограничиваются банальным хранением информации. С развитием сетей базы данных становятся сетевыми и многопользовательскими. В последнее время наблюдается тенденция удаленного администрирования баз данных посредством развития глобальной сети Интернет.

Работа с базой данных включает в себя определенное ПО для просмотра информации, поэтому очень важно, чтобы доступную информацию просмотрел любой желающий, не имея специализированного ПО. Реализация WEB-приложения позволяет обходить эту проблему так как средства для просмотра WEB-страниц есть практически на всех современных компьютерах. В качестве средства разработки Web-приложения хорошо подходит PHP. Это широко распространенный открытый ресурс – язык скриптинга (сценариев) общего назначения, который создан специально для Web и который можно внедрять в HTML [1, 2].

PHP отличается от других подобных языков, типа клиентского JavaScript тем, что код выполняется на сервере. Если вы имеете скрипт, на сервере, то клиент получит результат работы этого скрипта, не имея возможности определить, каков был исходный код. Также можете сконфигурировать web-сервер таким образом, чтобы он обрабатывал все HTML-файлы с помощью PHP, и реально пользователь не будет иметь способа определить, какой скрипт использовался для создания Интернет-страницы.

Наилучшим качеством PHP является то, что он предельно прост для новичка в программировании, но предлагает много продвинутых возможностей для программиста-профессионала.

PHP может использоваться на всех крупных операционных системах (ОС), включая Linux, многие варианты Unix (HP-UX, Solaris и OpenBSD), Microsoft Windows, Mac OS X, RISC OS и, возможно, другие. PHP имеет поддержку для большинства существующих web-серверов. Это Apache, Microsoft Internet Information Server, Personal Web Server, Netscape и iPlanet-серверы, Oreilly Website Pro, Caudium, Xitami, OmniHTTPd и многие другие.

С самого начала целью работы являлась разработка WEB-приложения, позволяющего получать доступ на чтение базы данных, и отображение результата при помощи обозревателя Интернет. По задумке, система должна удовлетворять таким требованиям, как:

1) функциональность,

2) надежность в работе,

3). дружественный интерфейс,
4) удобство и легкость в использовании,
5) работать с 3 СУБД: InterBase, MSSQL и Oracle,
6) поддержка максимального количество Интернет-обозревателей
7) обеспечение безопасности БД,
8) обеспечение авторизации пользователей.

ЛИТЕРАТУРА

1. *Ульман Л.* Основы программирования на PHP: Пер. с англ. М.: ДМК Пресс, 2001. 288 с.

2. *Ковязин А., Востриков С.* Мир InterBase. Архитектура, администрирование и разработка приложений баз данных в InterBase. 2-е изд. дополненное. М.: КУДИЦ-ОБРАЗ, 2002. 496 с.

РЕШЕНИЕ ПРЯМОЙ ЗАДАЧИ КИНЕМАТИКИ

А.А. Рыжов, студент гр. 572 –2;
ТУСУР, г. Томск, т. 8-923-402-87-71, sashar@sibmail.com

Разрабатываемая система состоит из нарисованных моделей: фрезерного станка (осуществляет свои движения в трехмерной декартовой системе координат), сборочного (производит свои движения в цилиндрической системе координат) и сварочного роботов (производит свои манипуляции в ангулярно-сферической системе координат). Чтобы привести данные роботы в движение, необходимо разобраться с задачей кинематики [1].

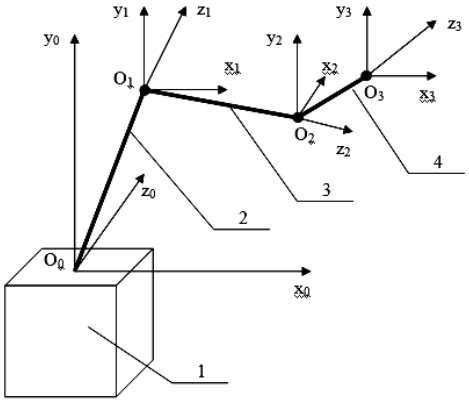
Прямая задача кинематики заключается в определении положения и ориентации схвата в выбранной системе координат по заданным значениям обобщенных координат манипулятора, однозначно определяющим его положение как механической системы. Решение прямой задачи всегда однозначно и может быть получено для любого числа звеньев, составляющих манипулятор.

В качестве обобщенных координат выступают поворот основания робота и поворот каждого звена манипулятора, а прямая задача состоит в определении координат конца электрода при каждом значении обобщенных координат.

Для описания трехзвенного манипулятора, имеющего вращательные кинематические пары V класса, имеются следующие системы координат: $O_0x_0y_0z_0$ – базовая система координат, связанная с основанием манипулятора; $O_1x_1y_1z_1$ – подвижная система координат, неизменно связанная с первым звеном манипулятора; $O_2x_2y_2z_2$ – подвижная система

координат, связанная со вторым звено манипулятора; $O_3x_3y_3z_3$ – подвижная система координат, связанная с кистью манипулятора (для удобства примем систему координат $O_3x_3y_3z_3$ на конце электрода). Рассмотренная схема приведена на рисунке.

Ось z_i совпадает с осью кинематической пары, имеющей тот же номер i, ось x_i определяется как перпендикуляр к плоскости, образуемой осями z_{i-1} и z_i, и направлена в ту сторону, откуда мысленный поворот оси z_{i-1} к z_i через меньший угол виден против часовой стрелки, ось y выбирается таким образом, чтобы система координат $O_ix_iy_iz_i$ была правой. Начало полученной ортогональной системы координат O_i совмещено с центром i-й кинематической пары.



Системы координат трехзвенного манипулятора: 1 – основание робота; 2 – первое звено манипулятора; 3 – второе звено манипулятора; 4 – кисть манипулятора

Теперь вектор обобщенных координат, описывающих состояние трехзвенного манипулятора в сферической системе координат, запишется в виде:

$$\boldsymbol{\varphi} = \left[\varphi_1, \varphi_2, \varphi_3, \varphi_4\right]^T, \qquad (1)$$

где φ_1 – поворот основания робота относительно базовой системы координат; φ_2 – поворот первого звена манипулятора относительно базовой системы координат; φ_3 – поворот второго звена манипулятора относительно базовой системы координат; φ_4 – поворот кисти робота относительно базовой системы координат.

Если известны начальное положение механизма и абсолютные значения углов поворота, тогда для нахождения нового положения мани-

пулятора необходимо последовательно, начиная с кисти манипулятора, выполнять повороты звеньев вокруг осей z_{i-1} на величину $\Delta\varphi_i$.

Найдем координаты конца электрода в трехмерной системе координат $O_0x_0y_0z_0$. Поворот основания робота осуществляется вокруг оси y, поэтому изменяются координаты z и x. Поскольку основание робота так же, как и звенья манипулятора, двигается в сферической системе координат, то здесь также можно применить уравнение параметрически заданной окружности. Тогда получим уравнение движения рабочего органа в трехмерной сферической системе координат:

$$\begin{aligned} x_3 &= (x_2 + l_3 \cdot \cos\varphi_4) \cdot \cos\varphi_1 = (l_1 \cdot \cos\varphi_2 + l_2 \cdot \cos\varphi_3 + l_3 \cdot \cos\varphi_4) \cdot \cos\varphi_1 \\ y_3 &= y_2 + l_3 \cdot \sin\varphi_4 = l_1 \cdot \sin\varphi_2 + l_2 \cdot \sin\varphi_3 + l_3 \cdot \sin\varphi_4 \\ z_3 &= (x_2 + l_3 \cdot \cos\varphi_4) \cdot \sin\varphi_1 = (l_1 \cdot \cos\varphi_2 + l_2 \cdot \cos\varphi_3 + l_3 \cdot \cos\varphi_4) \cdot \sin\varphi_1 \end{aligned} \quad (2)$$

где φ_1 – угол поворота основания робота вокруг оси y.

В разработанных моделях роботов полученные формулы используются для нахождения координат рабочего органа робота при движении звеньев манипулятора на заданные углы, а также для проверки аварийных ситуаций [2].

ЛИТЕРАТУРА

1. *Черноусько Ф.Л., Болотник Н.Н., Градецкий В.Г.* Манипуляционные роботы: динамика, управление, оптимизация. М.: Наука, 1992. 368 .

2. *Коровин Б.Г.* Системы программного управления промышленными установками и робототехническими комплексами: Учебное пособие для вузов. Л.: Энергоатомиздат. Ленинградское отделение, 1990. 352.

СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОДУКЦИИ CPU КОРПОРАЦИИ «Sun Microsystems»

А.А. Шилов, студент гр. 574

ТУСУР, г. Томск, opk@ms.tusur.ru

В соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2006 г.) произведен анализ современного (на 2006 г) состояния продукции CPU компании (корпорации) Sun Microsystems [1].

Корпорация Sun Microsystems является лидером инноваций в области процессоров x64 и UltraSPARC и поставляет высокопроизводительные и масштабируемые системы, которые позволяют эффективнее использовать физическое пространство вычислительных центров.

Архитектура SPARC (Scalable Processor Architecture) разрабатывалась компанией Sun Microsystems в период между 1984 и 1987 гг. и бра-

ла свое начало в Университете Беркли (шт. Калифорния), где с 1980 по 1982 гг. разрабатывался компьютер с сокращенным набором инструкций (Reduced Instruction Set Computer – RISC). Архитектура RISC позволяла значительно увеличить скорость работы процессора и делала его проектирование более простым. Появление архитектуры SPARC сделало возможным достижение более высоких уровней производительности процессоров, удешевило и ускорило их проектирование, производство и продвижение на рынок.

В настоящее время Sun выпускает серверы, которые отвечают самым высоким в отрасли показателями быстродействия, масштабируемости и эффективности, в основе которых лежат процессоры собственной разработки корпорации – UltraSparc IV, UltraSparc IV+ и UltraSparc T1.

UltraSparc IV – первый процессор Sun, который может одновременно выполнять более одного потока инструкций одновременно. Достигается это за счет размещения на одном чипе сразу двух ядер. Оба процессорных ядра основаны на дизайне UltraSparc III и имеют тактовую частоту 1,2 ГГц. В дальнейшем планируется перейти на 0,09-микронную технологию производства чипов, что, предположительно, позволит увеличить рабочую частоту процессора вдвое. UltraSparc IV основан на архитектуре Sparc V9, построен на двух ядрах UltraSparc III (64 битная Sparc-архитектура, набор инструкций VIS), поддерживает технологии Chip Multithreading (CMT) – многопоточность на кристалле, по потоку на процессор. Процессор производится по 0,13-микронному техпроцессу (КМОП), содержит 66 млн. транзисторов и работает на тактовой частоте 1,05–1,35 ГГц. Кэш-память данных первого уровня 64 КБ, кэш-память инструкций первого уровня 32 КБ, внешняя кэш-память второго уровня 16 МБ (по 8 МБ на ядро). Контроллер кэш памяти встроен в кристалл, контроллер памяти также встроен в кристалл до 16 ГБ ОЗУ на процессор, 2,4 ГБ/с. Энергопотребление: до 108 Вт на частоте 1,2 ГГц и напряжении 1,35 В.

Процессор UltraSparc IV+ разработан на базе 90-нанометровой производственной технологии корпорации Texas Instruments. По сравнению с процессором UltraSparc IV он позволяет удвоить производительность приложений благодаря увеличению объема кэш-памяти и буферов, улучшенному механизму прогнозирования ветвления, расширен-ным возможностям упреждающей выборки из памяти и новым вычислительным возможностям. Кроме того, в UltraSparc IV+ применяется новая трехуровневая иерархия кэш-памяти, включающая интегрированную на кристалле кэш-память второго уровня объемом 2 Мбайт и внешнюю кэш-память третьего уровня объемом 32 Мбайт. Кроме новых функций увели-

чения производительности процессор UltraSparc IV+ имеет значительно более высокую тактовую частоту (первоначально 1,8 ГГц). По сравнению с процессором UltraSparc IV производительность каждого потока выросла примерно вдвое. В то же время наличие целого ряда средств для повышения надежности, работоспособности и удобства обслуживания позволяет назвать этот процессор самым надежным среди всех моделей процессоров UltraSparc. Так же, как и процессор UltraSparc IV, новый процессор UltraSparc IV+ совместим на уровне двоичных кодов с предыдущими поколениями процессоров архитуктуры Sparc. Это позволяет пользователям сохранить инвестиции в средства разработки и в прикладное программное обеспечение. Кроме того, пользователи смогут легко модернизировать существующие системы, чтобы повысить их производительность и надежность – новые процессоры могут устанавливаться в существующие системы семейства Sun Fire и работать вместе с уже ранее установленными в системе процессорами UltraSparc IV и UltraSparc III. Может потребоваться только замена блока питания или системы охлаждения.

14 ноября 2005 г. компания представила новый многоядерный процессор UltraSparc T1, ранее известный под кодовым названием Niagara. Процессор UltraSparc T1 с технологией CoolThreads представляет собой высокопроизводительный процессор, отвечающий самым строгим экологическим требованиям. Процессор T1, выполненный по технологии 90 нм, доступен в версиях с четырьмя, шестью или восемью ядрами, работающими на частоте 1 или 1,2 ГГц. Причем каждое из ядер позволяет обрабатывать одновременно до четырех потоков. Таким образом, самый мощный процессор UltraSparc T1 в состоянии одновременно обрабатывать до 32 отдельных потоков, т.е. больше, чем могут предложить сегодня чипы Intel Xeon или AMD Opteron. Взаимодействие между ядрами обеспечивает шина (crossbar) с пропускной способностью 136 Гб/с. Также на кристалле расположен кэш второго уровня размером 3 Мб, разделяемый между ядрами. Новый процессор Sun имеет четыре встроенных контроллера памяти, которые обеспечивают работу с памятью DDR2 (до 32 Гб) на частоте 333 МГц, общая пропускная способность памяти составляет 23 Гб/с. Отметим, что блок выполнения операций с плавающей точкой вынесен за пределы кристалла, поэтому T1 не силен в выполнении интенсивных вычислений и в целом не предназначен для «непотоковых» задач. Важной отличительной чертой процессора является его сверхнизкий показатель максимального энергопотребления, который составляет всего 70 Вт. Это дает возможность исполь-зовать данный T1 в системах со сверхплотным монтажом компонентов, которые чаще всего используются в центрах обработки данных и телекоммуникационных компаниях.

В конце мая 2006 г. корпорацией Sun Microsystems были представлены первые образцы процессора Niagara 2, где идея многопоточности получила дальнейшее развитие. Как и Niagara, Niagara 2 содержит восемь ядер, но каждое из них может работать с восемью потоками. Таким образом, общее число обрабатываемых потоков удваивается и составляет 64. Удвоение числа потоков увеличивает площадь кристалла менее чем на 20%. Так как Niagara 2 производится по 65-нм технологии, а не 90-нм, как первая версия Niagara, Sun смогла также увеличить емкость кэш-памяти с 3 до 4 Мбайт и добавить дополнительные механизмы шифрования. Процессор содержит также порт PCI Express, четыре контроллера FB-DIMM (fully buffered dual inline memory modules) и два порта Ethernet 10 Гбит/с. Sun приняла меры и для повышения быстродействия при выполнении каждого отдельного потока. Например, каждое ядро Niagara 2 снабжено собственным арифметическим устройством с плавающей запятой. У Niagara было только одно такое устройство, обслуживающее все ядра. К тому же у каждого ядра есть механизм stream processing unit, повышающий быстродействие при решении разнообразных задач шифрования-дешифрования [2–6].

ЛИТЕРАТУРА

1. http://ru.sun.com
2. http://www.opensparc.net
3. http://www.terralab.ru/system/239348/
4. http://www.asutp.ru/?p=204423
5. http://www.netlib.org/utk/papers/advanced-computers/sparcIV.html
6. http://zdnet.ru/?ID=615039

АВТОМАТИЗИРОВАННАЯ ОБУЧАЮЩАЯ СИСТЕМА ПО ДИСЦИПЛИНЕ «ГИБКИЕ ПРОИЗВОДСТВЕННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА»

Т.В. Степанова, студентка гр. 572-2;

ТУСУР, г. Томск, т. 8-923-406-44-10, s_tania@mail.ru

Данная работа посвящена подготовке учебных и программных материалов для проведения лабораторных и практических занятий по дисциплине «Гибкие производственные системы и робототехника». Требовалось разработать обучающую систему для дисциплин, связанных с технологическим программированием гибкой производственной линии, включающей в себя сварочный и сборочный роботы, модель копировально-фрезерного станка, модель технологического конвейера и модель склада [1].

В дальнейшем на основе спроектированных роботов, поставленных на конвейер, будет разработан ряд лабораторных работ и тестов. На основе представленного теоретического материала в тестах, а также предложенных вопросов студент может вкратце ознакомиться с большим объемом литературы, необходимым для выполнения лабораторных работ. Сами лабораторные работы будут состоять из нескольких кадров, например: 1 кадр «Оглавление», в котором описано задание к данной лабораторной работе. Во 2-м кадре «Теоретический материал» описана краткая теория по этой лабораторной работе. Оставшиеся кадры – это контрольные вопросы. И так в каждой работе.

Это будет выглядеть приблизительно так:

1) изучить основные характеристики каждой модели робота;

2) изучить принцип работы конвейера;

3) написать программу по каждому технологическому объекту, не забывая, что они находятся во взаимосвязи по времени, т.е.:

- загрузить брус на модель копировально-фрезерного станка;
- на модели копировально-фрезерного станка из ранее загруженного бруса вырезается определенная форма детали (форма зависит от написанной программы);
- далее модель сборочного робота берет изготовленную деталь, переносит и ставит поверх уже готовой детали;
- после чего модель сварочного робота «ТУР-10» производит сварку по линии, где детали соприкасаются друг с другом;
- получившаяся деталь с помощью сборочного робота отправляется на склад;

4) Написать технологические программы для управления совместно всеми объектами;

5) Написать отчет по проделанной работе.

Составление лабораторных работ и тестов будет происходить в ранее созданной обучающей программе LirAOS. На рис. 1, представлена наиболее важная часть автоматизированной обучающей системы для набора учебных материалов – окно редактора.

По данным моделям робота в дальнейшем будет представлен контрольный тест, в котором будут использованы операторы перехода между кадрами, такие как:

- GOTO (переводится как «иди к»), позволяет изменять траекторию обучения, не переставляя кадры в файле с учебным материалом;

<оператор> = GOTO <имя кадра>

Результатом данного выражения будет запуск кадра указанного за ключевым словом GOTO.

- IF (переводится как «если»), с помощью этого оператора также можно изменять траекторию, но он включает в себя другие операторы,

которые выполняются или не выполняются в зависимости от какого-то условия:

<оператор> = IF <(выражение)> GOTO <имя кадра> ELSE <имя кадра>.

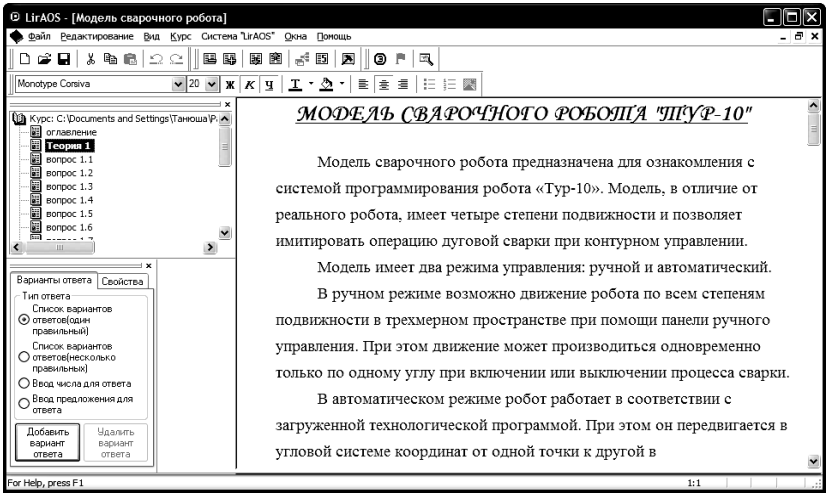


Рис. 1. Окно редактора программ

Если результатом выражения является истинное значение (True), то программа после этого кадра запускает кадр, указанный за ключевым словом GOTO. Если результатом выражения является значение False, то выполняется переход к кадру, указаному за ключевым словом ELSE (переводится как «иначе»), в противном случае выполняется следующий оператор.

- RANDOM, данный оператор позволяет формировать билеты с нужным количеством вопросов по каждой выбранной теме:

<оператор> = RANDOM (<выражение>, <имя кадра>, …, <имя кадра>).

Оператор команды random выбирает случайное количество кадров, указанное в выражении, из всех кадров, указанных далее. Это очень удобно для организации экзаменов или тестов, например, когда достаточно задать только 15 вопросов из 100.

Указание переходов осуществляется с помощью окна, показанного на рис. 2.

Итак, данные переходы позволяют студенту, не набравшему необходимое количество баллов для прохождения к теоретическому материалу следующего раздела, снова ознакомиться с теорией этого же раздела.

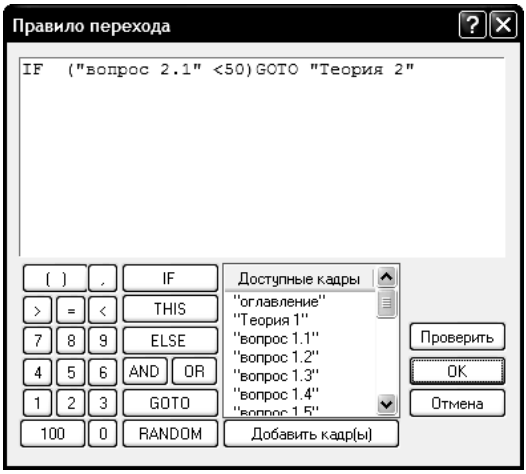


Рис. 2. Правило перехода

Так как данная система находится на стадии разработки, в дальнейшем с помощью обучающей системы LirAOS будет составлен полный курс обучающих тестов и лабораторных работ по дисциплине «Гибкие производственные системы» [2].

ЛИТЕРАТУРА

1. *Раводин О.М., Абдрахманова Э.О., Раводина О.В.* Гибкие производственные системы и робототехника: Сборник лабораторных работ. Томск, 2003. 84 с.

2. *Мельников А.В., Цытович П.Л.* Принципы построения обучающих систем и их классификация. http://cdo.susu.ac.ru/journal/numero4/pedag/tsit3.html

КРИПТОГРАФИЧЕСКОЕ АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО (КРИПТОАРМ)

А.М. Терзи, студент 5 курса, гр. 522-2 ФВС
ТУСУР, г. Томск, amt2001@inbox.ru

В настоящее время в различных организациях остро стоит вопрос о безопасном документообороте между его участниками. С развитием техники и технологии все более часто такие документы представлены в электронном виде, а сам участник не отходит от своего рабочего места, используя для передачи и обмена документами электронные каналы связи. Основными угрозами подобного электронного взаимодействия являются:

1) нарушение целостности электронного документа (ЭД),

2) нарушение неотказуемости ЭД,

3) нарушение адекватности отображения ЭД,

4) несанкционированный доступ ЭД.

Реализация угроз может привести к ряду конфликтов между участниками электронного документооборота, таких как:

– отказ от факта приема (получения) или передачи (отправки) ЭД;

– опротестование содержания и/или времени приема или передачи ЭД;

– отказ от авторства ЭД.

С учетом специфики формата документов, а также среды передачи и обработки такой информации для успешного противодействия вышеописанным угрозам необходимо использовать криптографические методы защиты информации. К таким методам в первую очередь необходимо отнести:

1) выработку и проверку электронно-цифровой подписи (ЭЦП) ЭД,

2) шифрование и расшифрование ЭД,

3) выработку хэш-значения для ЭД.

В соответствии с законодательством РФ и рекомендациями стандартов в качестве таких криптографических алгоритмов необходимо использовать для шифрования – ГОСТ 28147-89; для выработки и проверки ЭЦП – ГОСТ Р 34.10-2001 (ГОСТ Р 34.10-94); для выработки хэш-значений – ГОСТ 34.11.

Основной проблемой на рынке средств, предназначенных для криптографической защиты ЭД, является их обособленность и не соответствие криптографических форматов, произведенных различными производителями. В первую очередь это накладывает отпечаток на конечного пользователя – участника системы ЭД, который тратит силы, средства и время на установку различных программных средств для защиты ЭД. Для решения данной проблемы предлагается использовать криптографические методы защиты информации, основанные на инфраструктуре открытых ключей PKI (public key infrastructure) [1]. Главной особенностью данной системы является наличие третьей стороны – удостоверяющего центра (УЦ), главной задачей которого является гарантия соответствия сертификата (открытого ключа) конкретному пользователю в системе, собственно выдача этих сертификатов и отслеживание просроченных сертификатов. Сертификат необходим каждому участнику для осущест-вления документооборота. Информация из сертификата используется при формировании ЭЦП, ключей при шифровании. Сертификат пред-ставляет собой файл формата CER или DER в соответствии со стандартом X.509. Помимо этого, в структуре PKI применяются стандарт-ные форматы криптографических сообщений PKCS

(Public Key Cryptography Standarts), роль которых заключается в приведение уже зашифрованных сообщений к одному и тому же виду. Таким образом, единственное несоответствие, которое может возникнуть между участниками системы, – это использование различных алгоритмов криптопре-образований.

Компания Microsoft (MS) успешно интегрировала в свои продукты – ремейки Windows криптографический интерфейс MS CAPI (Cryptographic Application Programming Interface), который позволяет внедрять в программное обеспечение криптографические алгоритмы посредством подключения так называемых криптопровайдеров CSP (Cryptographic Service Provider), содержащих конкретные криптографические алгоритмы. Основной особенностью данного интерфейса являются его широкая распространенность, наличие двух уровней набора функций, использование одинакового синтаксиса при написании схем криптографического взаимодействия, использование в системе PKI, хорошая техническая поддержка со стороны разработчика.

В качестве CSP при реализации криптографического АРМ выбран продукт компании «КриптоПро» CryptoPro CSP 2.0. Его основными чертами являются использование российских криптографических алгоритмов, описанных выше, возможность хранения ключевой информации в контейнерах различного типа (диск 3,5", системный реестр, eToken и т.д.), возможность расширения [2–4].

В результате был создан программный продукт, позволяющий участникам системы обмениваться ЭД по незащищенным каналам связи путем постановки ЭЦП ЭД и шифрования. Главным достоинствами программы является возможность массовой отправки сообщения, включение штампа времени в подпись, работа со списком сертификатов пользователей, дружественный интерфейс, прозрачность шифрования для пользователя и минимальные усилия при работе. Впоследствии планируется включить в программу возможность работы со списком отозванных сертификатов, «журналирование» и другие возможности.

ЛИТЕРАТУРА

1. *Щербаков А.Ю., Домашев А.В.* Прикладная криптография. Использование и синтез криптографических интерфейсов. М.: Русская редакция, 2003. 416 с.

2. http://www.itsecurity.ru – Учебный центр «Информзащита».

3. http://www.cryptopro.ru – компания «КриптоПро».

4. http://www.msnd.microsoft.com – Microsoft Developer Network.

КОМПЬЮТЕРНЫЕ ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ

П.И. Трофимов, студент 5-го курса
ТУСУР, Томск, т. 89234033653, trofim@ms.tusur.ru

Измерение физических параметров предполагает точную оценку аналоговых величин. Компьютер же работает исключительно с дискретными величинами. Следовательно, процесс превращения ПК в виртуальный измерительный прибор предполагает подключение таких устройств, как микроконтроллер с аналого-цифровым (АЦП) и цифро-аналоговым (ЦАП) преобразователем. С помощью компьютера можно управлять микроконтроллером через последовательный интерфейс.

Область применения виртуального прибора практически полностью определяется характеристиками программного обеспечения, в то время как характеристики интерфейсных устройств в большинстве случаев вполне понятны пользователю.

Помимо выполнения программ сбора данных, пользователь виртуального измерительного прибора сможет часто экспортировать результаты измерений в более развитые приложения, например, электронные таблицы или программы построения диаграмм.

В программной среде была разработана виртуальная панель комплекса приборов, реализующая функции осциллографа и генератора. Основной задачей комплекса является формирование синусоидальных сигналов, получение и вывод сигналов, полученных с устройства, на экран монитора, а также функции масштабирования сигналов по уровню и по времени на экране монитора, сохранение их на жестком диске для дальнейшего анализа. Построение компьютерных измерительных приборов производится на базе имеющегося оборудования (ПЭВМ тип IBM PC и учебного микропроцессорного стенда SDK1.1).

Согласно заданию необходимо организовать защиту входа АЦП и выхода ЦАП от перенапряжения и короткого замыкания. Для этого разрабатывается адаптер внешнего подключения к объектам.

Учебный микропроцессорный стенд SDK1.1 необходимо запрограммировать на ввод и вывод непрерывных сигналов, а также на управление и обмен с ПЭВМ через последовательный интерфейс и COM-порт компьютера. Для соединения стенда SDK1.1 с ПЭВМ разрабатывается кабель с разъемным соединением. Для управления стендом необходимо написать программу, которая будет управлять ЦАП, АЦП и портом передачи данных RS232.

Роль адаптера выполнит повторитель напряжения. Адаптер подключения к объектам должен иметь внутренний двухполярный источник питания, адаптер необходимо выполнить на отдельной плате, по-

местить в корпус. На корпусе разместить входы и выходы адаптера для внешнего подключения. Адаптер подключается к стенду SDK1.1 через соединительный кабель с разъемными контактами.

Необходимо выбрать кросс-ассемблер на ПЭВМ с целью трансляции программ стенда и с помощью программы загрузчика стенда загрузить программу в стенд.

В итоге состав измерительных приборов должен включать ПЭВМ, стенд SDK1.1, адаптер подключения к объектам, соединительные провода, и программное обеспечение: виртуальная панель измерительных приборов, программа – драйвер стенда SDK1.1 [1–3].

При сравнении реальных и виртуальных приборов, помимо предоставляемых возможностей и режимов работы, надо также принимать во внимание и их основные характеристики – точность и быстродействие.

Точность виртуального прибора определяется не только количеством цифр после запятой. Одним из основных критериев является разрядность аналого-цифрового преобразователя. Этот параметр определяет степень разрешения при измерениях, т.е. ту наименьшую разницу между двумя соседними значениями, которую «чувствует» измерительный прибор. Поэтому 12-разрядный АЦП с возможностью формирования на выходе 4096 различных значений выходного кода сможет измерить напряжение 2,5 В с точностью около 0,61мВ. Разумеется, эти расчеты верны при условии, что все электронные компоненты в АЦП имеют допуски, соответствующие указанным величинам. Что касается быстродействия, следует указать, что большинство виртуальных приборов, имеет относительно узкую полосу рабочих частот. Это вызвано, с одной стороны, затратами времени, необходимыми АЦП для выполнения каждого преобразования «аналог-цифра», а с другой стороны – затратами времени, необходимыми для программной обработки результатов.

ЛИТЕРАТУРА

1. *Ключев А.О.* Учебный стенд SDK-1.1: Руководство пользователя. М.: ООО ЛМТ, 2001. 84 с.

2. *Каган Б.М., Сташин В.В.* Основы программирования микропроцессорных устройств автоматики. М.: Энергоатомиздат, 1987. 304 с.

3. *Калабеков Б.А.* Микропроцессоры и их применение в системах передачи и обработки сигналов: Учеб. пособие для вузов. М.: Радио и связь, 1988. 368 с.

СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОДУКЦИИ CPU КОРПОРАЦИИ «AMD»

Е.В. Узбеков студент гр. 574-1
ТУСУР, г. Томск.

В соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2006 г.) произведен анализ современного (на 2006 г.) состояния продукции CPU компании (корпорации) AMD.

AMD – мировой поставщик интегральных микросхем для рынка персональных и сетевых компьютеров и коммуникаций, чьи производственные мощности расположены в Соединенных Штатах Америки, Европе, Японии и Азии. AMD производит микропроцессоры, устройства флэш-памяти и вспомогательные микросхемы для коммуникационных и сетевых приложений.

Технология AMD разрушает барьеры на пути к новому и усовершенствованному ПО, которое предполагает наличие 64-битной технологии и превосходной работы процессора. Энтузиасты, желающие получать больше от своих систем, и просто геймеры могут открыть целый потенциал технологии AMD64, одновременно наслаждаясь выдающейся производительностью ПО на компьютере нового поколения. В процессорах AMD Athlon™ 64 FX реализованы передовые технологические решения, обеспечивающие высочайшую производительность. Пользователям ПК станут доступны реалистичные графические изображения кинематографического качества также и в компьютерных играх. Сегодня уже анонсирован выпуск современных 64-разрядных операционных систем Microsoft®, Red Hat, SuSE и TurboLinux для платформы AMD64 – эти системы работают только на процессорах на базе технологии AMD64. Улучшенная защита от вирусов – одна из возможностей технологии AMD64. Эта функция поддерживается такими ОС, как Windows XP SP2 и Windows XP 64-bit Edition для 64-разрядных систем, и разработана для перехвата определенного типа злонамеренных действий, известных как «переполнение буфера» («buffer overrun» или «buffer overflow»). Улучшенная защита от вирусов при поддержке указанных ОС призвана предотвратить распространение некоторых вирусов, таких как MSBlaster и Slammer._Процессор AMD Athlon 64 FX является не только единственным Windows®-совместимым 64-разрядным процессором для ПК, но и самым экстремальным процессором для игр в мире. Благодаря многочисленным техническим новшествам, этот процессор позволит испытать самые захватывающие ощущения от работы на компьютере. Процессоры на базе архитектуры AMD64 имеют удвоенное

число регистров общего назначения и регистров SSE/SSE2, что повышает производительность и расширяет возможности обработки мультимедийных данных с использованием средств технологий 3DNow!™ Professional и SSE2. Технология HyperTransport™ позволяет увеличить общую производительность системы за счет сокращения узких мест в подсистеме ввода-вывода, повысить скорость обработки данных и уменьшить время отклика [1–3].

Технология HyperTransport представляет собой высокопроизводительный интерфейс типа «точка-точка» с малым временем задержки, повышающий скорость обмена данными между электронными компонентами персональных компьютеров, серверов, сетевого и коммуникационного оборудования до 48 раз по сравнению с существующими технологиями. Применение HyperTransport сокращает количество шин в системе, что способствует устранению узких мест и позволяет современным высокопроизводительным процессорам более эффективно использовать системную память в компьютерах высшего класса. Отличительные особенности технологии HyperTransport.

○ Существенно превосходит другие технологии по пропускной способности.

○ Обеспечивает доступ с малыми задержками и использует небольшое количество сигнальных проводников.

○ Обеспечивает совместимость с наследуемыми устройствами PCI и поддерживает возможность перехода на новые шины на основе архитектуры Systems Network Architecture (SNA).

○ Полностью прозрачна для операционной системы и мало влияет на драйверы периферийных устройств.

Технология HyperTransport разработана корпорацией AMD при участии отраслевых партнеров. В настоящее время сопровождение и лицензирование этой технологии осуществляются консорциумом Hyper Transport Technology Consortium – некоммерческой корпораций со штаб-квартирой в шт. Техас, США.

До недавнего времени увеличение производительности процессора часто приводило к росту потребляемой мощности и повышению уровня шума. Технология Cool «*n*» Quiet™ от компании AMD представляет собой инновационное решение, доступное в системах на базе процессора AMD Athlon™ 64. Это решение обеспечивает эффективное снижение потребляемой мощности и позволяет тем самым создавать более тихие вычислительные системы. В то же время оно поддерживает функцию «производительность по требованию» (Performance on demand), обеспечивающую максимальные вычислительные возможности. Совместно со своими технологическими партнерами корпорация AMD реализовала

технологию Cool «*n*» Quiet в виде функциональной подсистемы, объединяющей процессор с активированной технологией Cool «*n*» Quiet, системную плату, BIOS с поддержкой указанной технологии, программный драйвер и процессорный вентилятор. Процессор AMD Athlon™ 64 является наиболее современным процессором для мобильных систем на базе ПК, обладающим потрясающей производительностью, необходимой для требовательных к вычислительным ресурсам программ. Процессор AMD Athlon 64 разработан с учетом высоких требований к мобильности; поддержка технологии AMD PowerNow!™ обеспечивает необходимую вычислительную мощность системы, увеличивая время автономной работы мобильных систем. Разработка процессора AMD Athlon 64 велась с учетом как текущих, так и будущих потребностей пользователей в вычислительных ресурсах. Ноутбуки с процессором AMD Athlon 64 демонстрируют производительность настольных систем при работе с самыми требовательными к ресурсам приложениями. Процессор AMD Athlon 64 обеспечивает высочайшую производительность программного обеспечения, написанного для платформы ПК, включая офисные приложения, программы для развлечений и компьютерные игры [4–7].

Процессор AMD Athlon 64, являясь первым процессором для портативных компьютеров на базе платформы AMD64, гарантирует высочайшую производительность в современных приложениях и обеспечивает полную готовность к переходу на 64-разрядные вычисления. Преимуществами новой архитектуры смогут воспользоваться в первую очередь приложения, требовательные к скорости обработки больших массивов данных: высокопроизводительные серверы, САПР, системы управления базами данных, мощные вычислительные комплексы.

ЛИТЕРАТУРА

1. http://www.citforum.tomsk.ru
2. http://www.ixbt.com
3. http://www.amd.ru
4. http://www.microprocessor.sscc.ru
5. http://npksv.ru
6. http://www.bytemag.ru
7. http://www.osp.ru

СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОДУКЦИИ CPU КОРПОРАЦИИ «INTEL»

К.В. Ван-Пин студент гр. 574-1
ТУСУР, г. Томск, KLIM42rus@mail.ru

В соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2006 г.) произведен анализ современного (на 2006 г) состояния продукции CPU компании (корпорации) Intel.

Intel выпустила девять давным-давно обещанных двухъядерных процессоров Itanium 2 (ранее известных под кодовым наименованием Montecito), предназначенных для сегмента Hi-End. Флагманская модель семейства Itanium 2 9050 имеет два ядра с поддержкой Hyper-Threading (может одновременно выполнять четыре потока команд), а размер кэш-памяти третьего уровня составляет внушительные 24 Мбайта [1].

В начале 2007 г. Intel демонстрирует сэмплы изготовленных по 45-нм технологическому процессу модулей SRAM, продает полный спектр 65-нм процессоров и сворачивает «устаревшее» 90-нм производство.

Новый технологический процесс получил вполне привычное название – P1264, привычные производственные материалы и привычное производственное оборудование – ультрафиолетовые литографические инструменты на основе 193-нм лазеров. Даже в 90-нм P1262 разнообразных технологических новшеств было больше, однако в P1264 удалось обойтись без особых ухищрений, ограничившись лишь небольшими улучшениями и усовершенствованными фазосдвигающими масками. Среди улучшений – переход к использованию в качестве электропроводящего материала силицида никеля (NiSi) и слегка доработанная технология «напряженного кремния», позволяющие снизить тепловыделение кристалла. А вот толщину изолирующего оксидного слоя в новом техпроцессе изменять не стали, сохранив ее на уровне 1,2 нм. Кроме того, в кристалл, ранее насчитывавший семь слоев, добавлен восьмой слой, позволяющий повысить плотность электрических контактов, скорость распространения электрических сигналов и снизить «межконтактную» емкость. Собрав эти «мелочи» вместе, технологам удалось совершить маленькое чудо: сохранив все преимущества «тонкого» технологического процесса, уменьшить токи утечки кристалла почти вчетверо! И это еще не все: рабочий ток затвора возрос на 10–15%, а электрическая емкость уменьшилась на 20%, что, по словам представителей Intel, обеспечивает почти 30–40-процентный прирост тактовых частот! Заодно всюду, где только можно, внедрили технологию «спящих транзисторов», отключающихся от питания, когда они не используются.

Тем не менее, заполучив в свое распоряжение прогрессивный технологический процесс, изменять ядро Pentium 4 Prescott в связи с «похоронами» NetBurst разработчики не стали. Новые ядра (кодовое название CedarMill) «официально» получили кэш-память объемом 2 Мбайт, технологию виртуализации Intel Virtualization Technology (VT-x, aka Vanderpool) и сниженный с 14 до 12 минимальный множитель.Тактовые частоты поднимать не стали: для одноядерных CedarMill верхним пределом сегодня стала частота 3,6 ГГц (понижена с прежних 3,8 ГГц Prescott), а для двухъядерных Presler – 3,55 ГГц (повышена с 3,20 ГГц Smithfield). По сути, почти весь созданный новым технологическим процессом задел для повышения тактовой частоты (а если слова о 40% увеличения быстродействия транзисторов правдивы, то новые Pentium 4 могли бы постепенно достичь 5 ГГц) так и остался неиспользованным. Intel улучшила лишь результаты откровенно провального Pentium D 3,20 ГГц. Отчасти это вызвано желанием снизить тепловыделение, а отчасти «политическими» мотивами: все-таки NetBurst при всех своих недостатках, была невероятно прогрессивной архитектурой, и грядущий «суперпроцессор» Conroe мог бы и не догнать «второй Northwood», неожиданно преодолевший технологические проблемы. Увеличенный до 4 Мбайт (2+2) кэш двухъядерников сыграл все-таки негативную роль, поскольку снижения TDP для двухъядерных процессоров так и не произошло: оно по-прежнему составляет 130 Вт у старших моделей. Правда, измерения показывают, что новый 955-й Pentium Extreme Edition значительно экономичней прежнего лидера – 840-го, хотя и рассеивает тепла раза в полтора больше, чем сопоставимое по производительности решение конкурента [2].

Еще один немаловажный момент, связанный с новым технологическим процессом, – это заметно возросшая производительность (в смысле – количественные возможности по выпуску процессоров с одной пластины) и пропорционально снизившаяся себестоимость производства. Площадь одноядерного CedarMill (с двухмегабайтным кэшем) уменьшилась до скромнейших 81 кв. мм, мало того – новые двухъядерники, в отличие от ядра Smithfield, «собираются» из двух независимых ядер CedarMill в одном корпусе. В принципе, Smithfield и так был не более чем объединением двух ядер Prescott, но их приходилось делать в виде единого кристалла. Ну а теперь нашелся удобный способ независимой упаковки двух кристаллов в один процессор. Кстати, Presler (это не отдельное ядро, а два CedarMill) станет не единственным процессором, использующим эту технологию: ближе к 2007 г. похожим образом Intel собирается выпускать четырехъядерные процессоры, упаковывая по два двухъядерных кристалла. «Двойная упаковка» очень технологична и, в

принципе, позволяет Intel легко перевести в 2006 г. бóльшую часть своих процессоров на использование двух ядер.

В мобильном секторе все гораздо сложнее. Новые 65-нм процессоры (кодовое название Yonah) – впервые в мире мобильных CPU – являются двухядерными, причем построенными на основе прогрессивной технологии, общей для двух ядер кэш-памяти второго уровня. Правда, два ядра – это удвоенное тепловыделение, которое трудно компенсировать даже более тонким технологическим процессом, поэтому при работе ноутбука от батарей процессор незаметно «превращается» в одноядерный, если мощность второго ядра не требуется. Добавили в процессор и поддержку технологии виртуализации Intel VT-x. Правда, кэш-память второго уровня увеличивать по сравнению с предыдущим поколением Dothan не стали – она так и осталась равной 2 Мбайт и для одноядерных и для двух-ядерных вариантов.

ЛИТЕРАТУРА

1. *Процессоры* Intel Itanium 2 серии 9000. Компьютерра. 12 сентября 2006 г. №33. С. 25.

2. http://www.dvgu.ru

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ПРОЕКТИРОВАНИЮ БЛОКА ОБРАБОТКИ ДАННЫХ

К.В. Ван-Пин, К.В. Климентьев студенты гр. 574-1

ТУСУР, г. Томск, KLIM42rus@mail.ru

В соответствии с инновационной стратегией группового проектного обучения по проблеме «Устройство цифрового управления объектом» (ГОС СД.05 от 2000 г.) произведен анализ блока обработки данных.

Модифицировать содержимое РОН требуется каждый раз, когда в команде указан регистровый автоинкрементный или декрементный метод адресации, соответственно, или РОН+2, или РОН – 2, а также для аналогичных косвенных методов.

По умолчанию R7 всегда при выборке слов формата команды модифицируется: R7+2.

Процесс модификации поддерживают аппаратные средства, показанные на рис. 1.

Решение этой ситуации – включение в схему модификации регистра результата (RGR), запись на который управляемая (У:С) и не зависимая от у:W, у:R, как это показано на рис. 1.

При модификации R7+2 организуется такая последовательность микроопераций:

у:D) PA:=MKK, PMS:=MKK; у:R) и уR:7) BUS2:A:=R7, и

yR:14) BUS2:B:=2, PMS) REZ:=AL(A+B), y:C) RGR:=REZ;
y:L) BUS3:=RGR, y:w) и yw:7) R7:=BUS3.

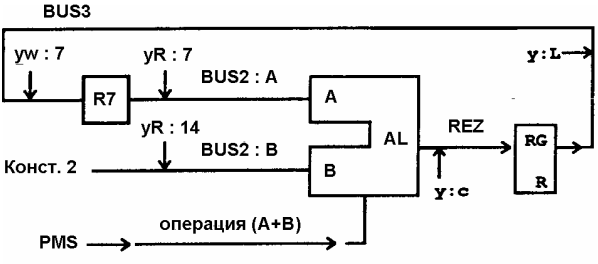


Рис. 1. Вариант схемы модификации РОН

В соответствии с микрооперацией y:D производится прием части формата микрокоманды МКК(21-00) на регистры РА и PMS (адресный и типа операции АЛУ). Возникает требование, чтобы эти поля формата микрокоманды не пересекались.

Пусть РА(3-0):=МКК(3-0), а PMS(4-0):=МКК(8-4).

Приведенная выше последовательность микроопераций позволяет некоторые из них выполнять одновременно, т.е. управляющие биты могут быть включены в одну микрокоманду [1].

Рассмотрим команду: ADD R1,R2. Вариант аппаратной поддержки команды ADD (сложение) показан на рис. 2.

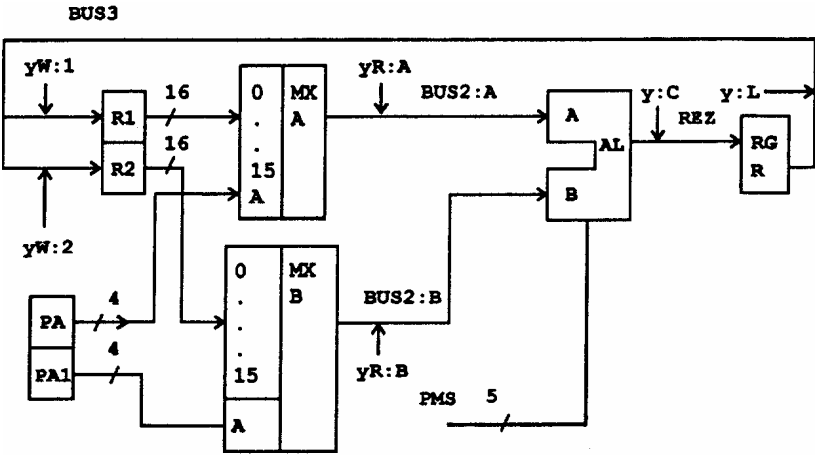


Рис. 2. Обработка данных (вариант)

Заметим, что для подготовки операндов потребуются два адресных регистра (РА и РА1), два управляющих сигнала y:D и y:D1, записи этих

адресов (или расширение формата микрокоманды на два поля адреса регистра), кроме того, два мультиплексора MX:A и MX:B для шин.

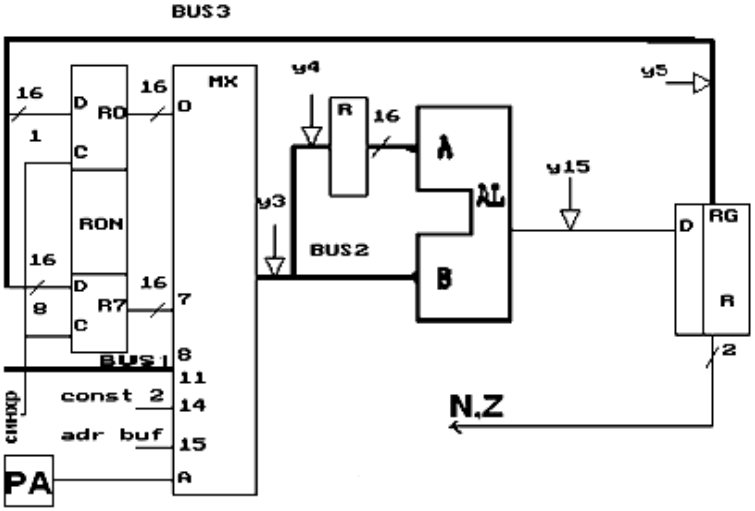


Рис. 3. Блок обработки данных

Окончательное решение схемы чтения регистров РАЛУ, показанное на функциональном уровне, представлено одним мультиплексором (на разряд) и дополнительным регистром R, подключенным по входу к шине BUS2, а выход R подключен ко входу АЛЛУ. При этом шина BUS2 не расширяется (см. рис. 3), а вход регистра R является управляемым (бит микрокоманды) [1].

ЛИТЕРАТУРА

1. *Прищепа Л.С.* Аппаратные средства вычислительной техники: В 5 разделах. Раздел 2. Базовые модели учебных ЭВМ: Учебное пособие. Томск: В-Спектр, 2006. 164 с.

СОПРЯЖЕНИЕ ПРОЦЕССОРА С ОБЪЕКТОМ В РЕЖИМЕ ЗАПРОСОВ

М.Г. Власова, С.Л. Крыловский, студенты 4 курса;
А.Е. Леонов, студент 3 курса
ТУСУР, г. Томск, т. 8-913-851-3569

В рамках проблемы ГПО рассмотрена теория к визуализации процесса проектирования интерфейсного модуля сопряжения в режиме запроса от объекта.

1. Управление объектом автоматизации. Рассмотрим модель управления дозированием в режиме индивидуального запроса и индивидуального адреса для флагов F1–F6 локальной системы автоматизации технологического процесса (ЛСА ТП) [1].

Математическая модель решения функциональной задачи в этом режиме представлена на рис. 1. Здесь использованы флаги: F1 – для включения-выключения заслонки бункера; F4 – для включения-выключения средств оповещения оператора об аварийной ситуации на объекте; F6 – состояние датчика накопления дозы в аккумуляторе (увеличивается до дозы).

2. Модификация базовых электрических функциональных схем физического (аппаратного) слоя подсистемы (рис. 3) выполняется в соответствии с вариантом задания. Модификация касается **подключения к базовой схеме узлов формирования запросов, сброса запросов и чтения флагов F5 и F6** состояния объекта дозирования сыпучих материалов [2]. Функциональные схемы этих узлов представлены на рис. 3–5 для проектируемого варианта [1, 2].

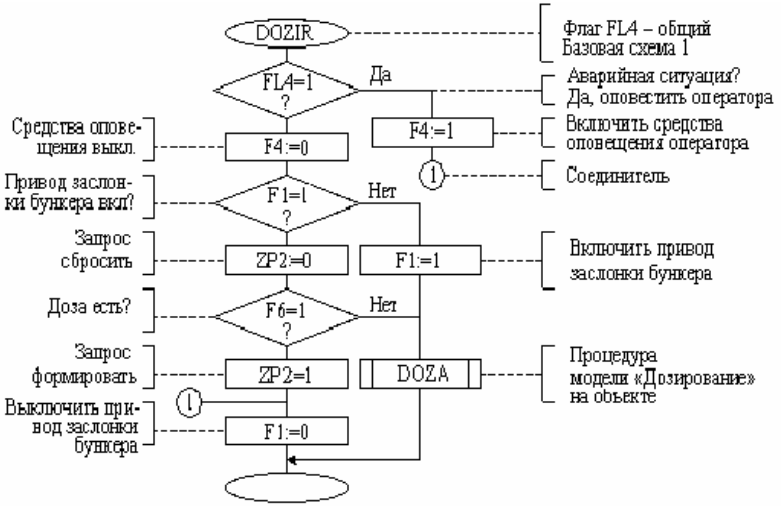


Рис. 1. ЛСА ТП, этап 3. Модель управления дозированием.
Флаги F1–F4 имеют индивидуальные адреса

Концептуальная модель модификации схем модуля представлена на рис. 2. Базовая схема 1 связана с каналом в соответствии с протоколом программного обмена. Из базовой схемы 1 исключены все элементы структуры, не относящиеся к функциям, указанным в варианте задания.

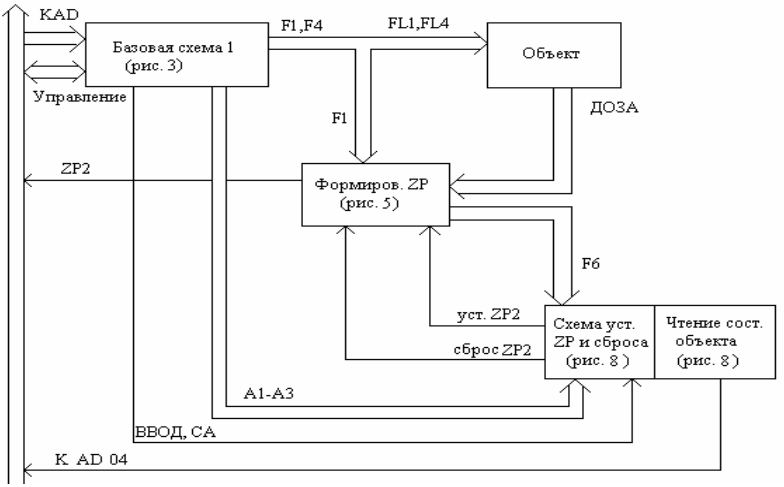


Рис. 2. Концептуальная модель модификации модуля сопряжения. Проектируемая структурная схема модуля сопряжения

3. Проектирование узлов блока МВ модификации модуля сопряжения на функциональном уровне показано на рис. 3, 4, 5.

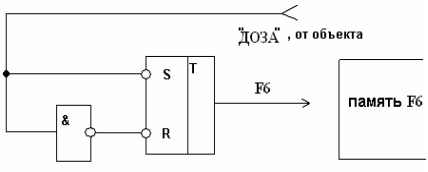


Рис. 3. Формирование состояния флага F6 от датчика объекта

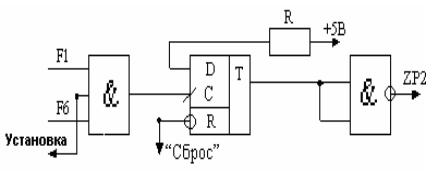


Рис. 4. Формирователь запроса по логике ZP2 : = УСТ & F1 & F6

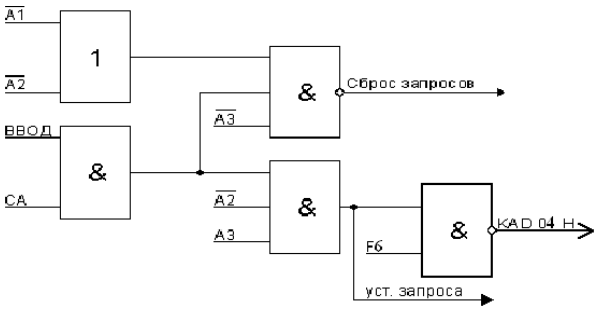


Рис. 5. Формирователь сигналов установки, сброса запросов и чтение флага F6

Из рис. 5 видно, что формируются сигналы УСТ и СБРОС запроса ZP2 по логике:

УСТ: = (ВВОД & СА) & ($\overline{A2}$ & А3)

СБРОС: = (ВВОД & СА) & ($\overline{A1}$ + $\overline{A2}$)& $\overline{A3}$

Чтение в канал состояния «Доза» объекта через флаг F6 производится так:

К АД 04 Н: = (ВВОД & СА) & ($\overline{A2}$ & А3)& F6 .

Для других вариантов задания такая логика описана на уровне математических моделей.

Выводы. Проблема модификации базовых схем с помощью подключения узлов формирования запросов, сброса запросов и чтения флагов F5 и F6 усложняет задание курсовой работы студентов. В результате была разработана теория к визуализации процесса модификации модуля сопряжения, с помощью которой можно доступно и наглядно визуализировать процесс сопряжения для проектируемого варианта.

ЛИТЕРАТУРА

1. *Прищепа Л.С.* Компьютерные средства в системах автоматизации и управления. Системотехника, вычислительные комплексы и сети ЭВС: Учебное методическое пособие к курсовому проектированию. Томск: ТМЦДО, 2003. 144 с.

2. ВЕСТНИК Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. Спец. Выпуск. Системная интеграция и безопасность. Томск: В-Спектр, 2006. 154 с.

АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ОТЛАДКИ МИКРОПРОЦЕССОРНЫХ СРЕДСТВ

С.В. Яковлев; Л.А. Торгонский, к.т.н., доцент

ТУСУР, г. Томск, т. 8-923-401-64-50, Yacovlev.Sergey@sibmail.com

Работа, представляемая докладом, направлена на сокращение времени отладки программ управления микропроцессорными стендами учебной лаборатори. Объектами лабораторного цикла являются микроЭВМ учебного микропроцессорного комплекта (УМК) с блоком расширения М1 и персональная ЭВМ. Микроэвм (УМК) оснащена пультом ввода программ и данных, средствами отображения адреса, данных памяти и объектов программной модели базового процессора микроэвм. Названная микроЭВМ, представляет интерес для применения в изучении фундаментальных положений организации вычислительных устройств, состава рабочих циклов взаимодействия процессора с памятью, команд / данных с портами. Процессор микроЭВМ имеет разделенные шины

адреса, команд/данных, управления и является классической иллюстрацией вычислительной машины с архитектурой фон Неймана.

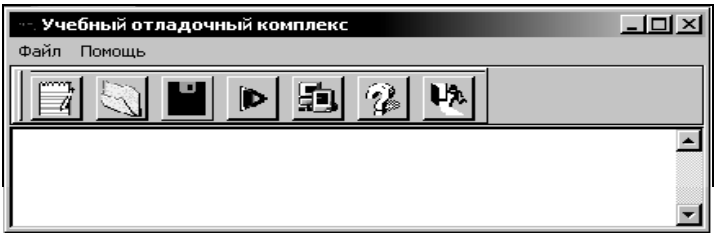
Информационное взаимодействие УМК и ПЭВМ реализовано по последовательному асинхронному интерфейсу. Для этого на макетном блоке М1 смонтированы синхронно-асинхронный приемопередатчик, таймер, селектор адресов, преобразователь сигналов информационных посылок по спецификации COM порта ПЭВМ и разъем соединительного кабеля для подключения к ПЭВМ.

Системная программа «Монитор» УМК не поддерживает прием и передачу данных в последовательном формате. Поэтому программный модуль «Монитор» в постоянном запоминающем устройстве (ПЗУ) УМК дополнен двумя программами «Прием» (адрес 400h) и «Передача» (адрес 450h). Так как доступный объем ПЗУ УМК составляет 2 кбайта, из которого 1 кбайт занят резидентным «Монитором», а остальная часть ПЗУ является свободной, то программы «Прием», «Передача» размещены во второй половине ПЗУ УМК.

Стенд УМК применяется не только для изучения архитектуры микроЭВМ, но и для обучения основам программирования микропроцессоров, проектирования и отладки программ управления оборудованием, подключенным к портам периферийных средств [1].

Применение ПЭВМ для подготовки, отладки, загрузки программ и данных в микроЭВМ для последующей отладки на реальных аппаратных средствах с последующим возвратом программ в ПЭВМ для сохране-ния, экспорта или импорта данных.

Для удобства работы с аппаратно-программной средой отладочного комплекса исполнен пользовательский интерфейс комплекса. Экранная форма основного окна интерфейса приведена на рисунке.



Форма программы диалог

Программа поддерживает следующие функции:

 – подготовка программы к работе,

 – загрузка файла в окно программы,

 – сохранение исходного текста программы в файл,

 – компиляция исходного текста программы,

 – загрузка откомпилированного файла в УМК,

 – руководство по эксплуатации учебного комплекса,

 – завершение работы программы.

В состав программного комплекса включены две внешние программы: кросс-ассемблер для компилирования программ и программа загрузки компилированного файла в УМК.

Для создания интерфейса программы диалога был выбран объектноориентированный язык программирования Delphi. Существенные преимущества языка Delphi от ближайших аналогов состоит в быстрой разработке приложений, обладающих сложным пользовательским интерфейсом, особенно имеющим сильные взаимосвязи между элементами управления, расположенными в окнах программы [2].

В результате проделанной работы разработан учебный отладочный комплекс, расширяющий возможности отладочного оборудования учебной лаборатории.

ЛИТЕРАТУРА

1. *Эксплуатационная* документация УМК.

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

РАЗРАБРОТКА БАЗ ДАННЫХ НА ОСНОВЕ СУБД MS SQL Server 2000

М. Захар, студент гр. 572-1;

ТУСУР, г. Томск, т. 8-962-780-68-91, zahar82@sibmail.com

Базы данных играют большую роль в жизни человека, так как успех любой структуры вне зависимости от рода ее деятельности в основном зависит от документации, работа с которой является главной целью построения баз данных.

SQL Server 2000 является многоцелевым сервером со сложной архитектурой. Этот сервер может использоваться как в промышленных

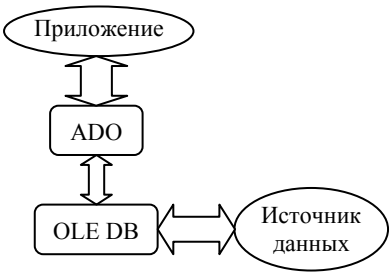
системах, так и в корпоративной среде, сочетая в себе легкость взаимодействия с приложениями с высокой надежностью и отказоустойчивостью. Сервер предназначен для одновременной работой с большим количеством транзакций. Как и многие продукты Microsoft, сервер использует в своей работе технологию COM, а для связи с приложениями – DCOM.

Целью работы является создание базы данных клиентов системы электронной отчетности по каналам связи (ЭКОС) в клиент-серверной СУБД MS SQL Server 2000 и разработка программного обеспечения, позволяющего манипулировать данными этой базы.

Программное обеспечение должно удовлетворить следующим требованиям:

1. безопасное соединение с сервером;
2. полный доступ к базе данных (добавление, редактирование и удаление записей);
3. печатать необходимые документы о клиентах, подключенных к системе ЭОКС;
4. удобный интерфейс.

Для реализации данного проекта используется среда программирования Delphi 7, так как в ней поддерживается технология ADO (ActiveX Data Objects – объекты данных, построенные как объекты ActiveX), которая усиленно развивается корпорацией Microsoft. ADO представляет собой высокоуровневую объектную надстройку над OLE DB. ADO может использоваться для работы с любыми провайдерами OLE DB. Схема приведена на рисунке1.



Доступ к данным при помощи ADO

В качестве источников данных могут выступать различные хранилища информации, например, таблицы, файлы и базы данных.

Пока данное ПО находится на стадии разработки и в дальнейшем планируется к вышеперечисленным требованиям добавить новые требования.

ГЕНЕРАТОР СПЕЦИФИКАЦИЙ ОБЪЕКТОВ ОБУЧАЮЩИХ ПРОГРАММ

А.В.Захаров, студент 5 курса каф. КИБЭВС
Л.А. Торгонский, доцент каф. КИБЭВС
ТУСУР, г. Томск, e-mail: zav@ms.tusur.ru

Учебный процесс в современном вузе показывает необходимость использования автоматизированных программ, помогающих тестировать студента, а также выполнять поставленные задачи – лабораторные, практические и иные учебные работы. Перед выполнением практической части, например, целесообразно проверить теоретические знания студентов, чтобы оценить степень их подготовки.

Данная программа ориентирована на использование в предмете «Проектирование интегральных микросхем и микропроцессоров».

Обзор работ в области создания программ считывания и обработки систематизированных записей показывает необходимость доработки существующих приложений [1–3].

Основные трудности в использовании этих программ – это сложность их модификации преподавателем, а также запутанная логика приложения.

К положительным моментам существующих программ можно отнести язык хранения данных XML, который позволяет создавать гибкие записи полей базы данных.

Программа должна состоять из двух взаимосвязанных частей – приложения преподавателя и приложения студента. Приложение преподавателя позволит ему производить корректировку введенных ранее значений и формул объектов. Приложение студента должно выполнять тестирование, по итогам которого предоставлять студенту вычислительные ресурсы программы для выполнения своих работ.

При разработке данного приложения возникает ряд вопросов: как организовать гибкую структуру данных, какой формат данных использовать, как производить распознавание строковой функции.

Ответы на эти вопросы дает нам расширяемый язык разметки XML.

XML – рекомендованный Консорциумом Всемирной паутины язык разметки, фактически представляющий собой свод общих синтаксических правил. XML предназначен для хранения структурированных данных (взамен существующих файлов баз данных), для обмена информацией между программами, а также для создания на его основе более специализированных языков разметки (например, XHTML), иногда называемых словарями.

Использование этого языка позволит нам вводить неограниченное количество элементов XML, одноименных с названиями переменных, хранить их значение, а также вводить значения необходимых атрибутов

в тело элемента. Ниже приведен пример записи элемента XML для «толщины базового слоя» полупроводникового резистора с атрибутом, указывающим на размерность данной величины:

```
<XB razmer=«мкм»>Толщина базового слоя (XB)</XB>
```

Заметим, что даже при первом прочтении данного отрывка XML-кода сразу становится понятно о сути и структуре представленных данных. Это заслуга языка XML.

Теперь, когда нам известна модель представления данных и структура приложения, возникает вопрос преобразования данных из текстового формата XML в формат представления данных и функций языка Pascal. Для этих целей используются парсеры – трансляторы языка.

Основные функции, реализованные парсером:

– совмещение различных кодировок представления данных,

– расшифровка XML документа,

– получение «сырых» данных из XML,

– генерация кода XML,

– преобразование текстовых формульных выражений XML в формулы языка Pascal,

– способность отслеживать ошибки в документах XML.

Проанализировав требования, предъявляемые к разрабатываемой системе, приведем ее примерный визуальный состав.

1. «Исходные данные» – форма, предназначенная для ввода исходных данных с рисунками и комментариями.

2. «Форма спецификации» – форма для внесения в базу формул и зависимостей для данной технологии и топологии.

3. «Тестирование» – форма студента, позволяющая выводить необходимую информацию для тестирования. В этом режиме студент должен указать определяющие параметры для предложенной переменной.

К системе предъявляются следующие требования:

– надежность в работе,

– дружественный интерфейс,

– удобство и легкость в использовании,

– учет специфических требований для предмета,

– возможность систематизации и использования полученной информации.

ЛИТЕРАТУРА

1. *Фаронов В.* Программирование в Delphi 7. Учебный курс. СПб.: Питер, 2005. 459 с.

2. *Марк Грейвс.* Проектирование баз данных на основе XML. М.: Вильямс, 2002. 640 с.

3. *Научная* сессия ТУСУР-2006. Ч. 2. Томск: В-Спектр, 2006. 324 с.

БЫСТРОДЕЙСТВИЕ СИСТЕМЫ ТЕЛЕМЕХАНИКИ МАГИСТРАЛЬНОГО ТРУБОПРОВОДА НА ОСНОВЕ СВЯЗИ СТАНДАРТА GSM

Д.Д. Зыков, аспирант; А.А. Шелупанов, д.т.н, проф.
ТУСУР, г. Томск, т. 41-34-26, d-zykov@ngs.ru

Рассмотрим систему телемеханики линейной части магистрального трубопровода. Системой телемеханики называют комплекс технических средств для передачи на расстояние по каналам связи команд от оператора или управляющей вычислительной машины к объектам управления, а также контрольной информации в обратном направлении. При управлении магистральным трубопроводом такая система включает несколько контрольных пунктов (КП), установленных на трубопроводе через каждые 10–15 км, и один диспетчерский пункт (ДП) (рисунок).

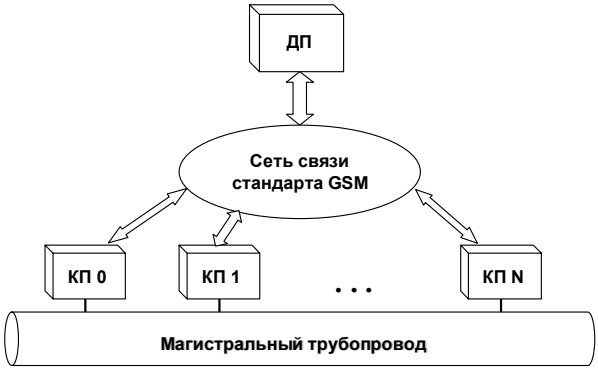


Схема системы телемеханики с использованием сети связи стандарта GSM

На практике для оценки быстродействия систем телемеханики применяются следующие показатели:

1) время получения сигналов ТИ со всех КП,
2) время доставки одного сигнала ТС, ТУ.

Перечислим основные услуги сети стандарта GSM: SMS, режим Data call и режим GPRS.

В результате предварительных исследований были получены следующие значения:

1) среднее время доставки SMS равно 7 с;
2) среднее время на установление и разрыв соединения в режиме Data Call равно 30 с.

Качество работы услуги GPRS было признано группой экспертов неудовлетворительным, и эта услуга была временно исключена из дальнейших исследований.

Данные ТУ, ТС и ТИ имеют разные свойства (табл. 1).

Таблица 1

Свойства данных, передаваемых в системе телемеханики

Свойство	ТИ	ТС, ТУ
Объем	Большой	Маленький
Время доставки	Менее критично	Более критично
Надежность доставки	Стандартные требования	Повышенные требования

Для примера рассмотрим систему телемеханики, состоящую из двух КП и одного ДП. Пусть с каждого КП необходимо получать данные ТИ объемом 3 Кбайт и данные ТС в количестве 10 сигналов, размер каждого сигнала не более 32 байт. Также нужно передавать на каждый КП 10 сигналов ТУ (размером до 32 байт).

Полученные значения показателей быстродействия для данной задачи были сведены в табл. 2.

Таблица 2

Значения показателей быстродействия для услуг Data call и SMS

Показатель быстродействия	Услуга сети GSM	
	Data call	SMS
Время получения сигналов ТИ со всех КП, с	66	308
Время доставки одного сигнала ТС, ТУ, с	30	7

Из табл. 2 видно, что по первому показателю выигрывает Data Call, а по второму, наоборот, SMS.

Для оптимизации системы по быстродействию нами было предложено следующее решение: сигналы ТИ передавать посредством Data Call, а сигналы ТС, ТУ посредством SMS.

В существующих системах телемеханики на основе GSM, как правило, используется только один вид услуги, предоставляемой оператором [1]. Более универсальные из применяемых в настоящее время разработок позволяют выбрать одну из услуг GSM для передачи информации, но одновременная работа Data Call и прием/передача SMS в них не реализованы.

Таким образом, для осуществления одновременного приема/передачи SMS и работы Data Call потребовалась разработка новых алгоритмов и программно-аппаратных средств. Эта задача была успешно решена на базе программируемого логического контроллера (ПЛК) ЭлСи-ТМ, разработанного и выпускаемого ЗАО «ЭлеСи», г. Томск [2].

Задачи дальнейших исследований:

1. Изучение влияния других факторов (внешних условий и различных параметров системы) на показатели быстродействия;

2. Осуществление дальнейшей оптимизации разработанной системы для расширения сферы ее применения.

ЛИТЕРАТУРА

1. *Зыков Д.Д., Шелупанов А.А.* Управление магистральным трубопроводом через сеть связи стандарта GSM // Интеллектуальные системы в управлении, конструировании и образовании: Сб. статей. Выпуск 5 / Под ред. А.А. Шелупанова. Томск: Изд-во Института оптики атмосферы, 2006. С. 93–98.

2. *Зыков Д.Д., Шелупанов А.А.* Защищенная система управления магистральным трубопроводом // Научная сессия ТУСУР-2006: Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. Томск, 4–7 мая 2006 г. Томск: В-Спектр, 2006. Ч. 3. С. 186–188.

ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ GSM В АВТОМАТИЗАЦИИ

Д.Д. Зыков, аспирант; А.А. Шелупанов, д.т.н, проф.

ТУСУР, г. Томск, т.41-34-26, d-zykov@ngs.ru

Компания Festo и ее дочерняя фирма Beck продемонстрировали GSM возможности контроллера Beck IPC FEC FC38 на выставке SPS/IPC Drives в Нюрнберге (Германия) в декабре 2000 г. [1]. Новый контроллер включал разработанное ПО, которое позволяло создавать SMS сообщения и интерпретировать их.

Связь, основанная на котроллере FEC FC38, подходит для небольшой управляющей системы с примерно 20 сигналами ввода/вывода для проверки сигналов ошибки от заданного процесса или для отправки команд системе управления. К этому набору добавлены стандартные коммуникационные возможности, такие как последовательные порты и порты Ethernet. GSM-модем встроен в корпус контроллера, позволяя отправлять и получать SMS-сообщения.

Opto 22, Temecula, Calif., разработчик и производитель аппаратного и программного обеспечения для промышленной автоматизации, удаленного мониторинга, корпоративного сбора данных и M2M применений интегрировала управляющий терминал GT48 от Sony Ericsson (London) со своим оборудованием ввода/вывода (I/O) OptoGSM, получив в результате более дешевую и более гибкую беспроводную систему для M2M приложений [2].

OptoGSM I/O первоначально дебютировало в мае 2003 г. как часть семейства продуктов Opto 22 для M2M. Используя сочетание промышленного стандарта, подключаемых модулей цифрового ввода/вывода

вместе со встроенным аналоговым вводом/выводом и встроенной беспроводной радиосвязью, обеспечивает взаимодействие с производственными ресурсами и передает технологические или служебные данные через любую сотовую сеть GSM.

Sony Ericsson GT48 – это управляющий GSM/GPRS-терминал, разработанный чтобы обеспечить беспроводную связь для M2M применений. Однако в отличие от большинства беспроводных модулей телеметрии, радиостанций, модемов и других компонентов, которые просто обеспечивают связь посредством сотовых сетей, GT48 – это интеллектуальное устройство, которое может быть настроено, чтобы независимо выполнять управляющие и сигнальные функции, используя встроенный механизм скриптов. Это означает, что GT48 может быть запрограммирован, чтобы кроме всего прочего исполнять бизнес-логику и взаимодействовать с подключенным оборудованием, таким образом позволяя пользователям добавлять мониторинг, обмен сообщениями и локальные функции управления по необходимости. Результат – более настраиваемое, эффективное и экономически выгодное M2M-решение.

Opto 22 в течение десятилетий разрабатывает системы ввода/вывода мирового класса, так что ее сотрудники смогли быстро распознать ценность встроенного интеллекта и других возможностей управляющего терминала GT48. С его робастным и перенастраивамым промышленным интерфейсом ввода/вывода GT48 доказал, что он является отличным выбором для интеграции с оборудованием OptoGSM I/O для создания дешевых беспроводных M2M-решений.

M2M система была внедрена в BioLab Inc., Decatur, Ga., подразделения Great Lakes Chemical, West Lafayette, Ind., одного из крупнейших в мире поставщиков водоочистных продуктов для отдыха и развлечений и промышленного рынка, имеющего сеть уполномоченных распространителей и поставщиков услуг [3]..

Оригинальная и пионерная система M2M появилась, благодаря всестороннему сотрудничеству участников Opto 22, www.opto22.com/m2m, Temecula, Calif.; Nokia Inc., www.nokiausa.com/solutions/m2m, Irving, Texas; BioLab; and nPhase LLC, http://www.nphase.com/, Chicago, Ill. и ее родительской компании Professional Consulting Services (PCS), Chicago, Ill., с AT&T Wireless, http://www.attws.com/, Redmond, Wash., предоставившей свои сетевые услуги.

Технология и телекоммуникационное оборудование Opto 22-Nokia обеспечивают беспроводную доставку данных реального времени от распределенных предприятий посредством сетей GSM (global system for mobile communications) и GPRS (general packet radio service).

nPhase, филиал компании PCS, которая является 13-летней IT фирмой, комплексным поставщиком M2M-решений. Заказчики BioLab, их подчиненные и распространители имеют доступ к мировому порталу управления nPhase через BioLab.

В этих решениях датчики отображают состояние воды в резервуаре, включая pH и санитарные уровни. Водоочистные химикаты выпускаются автоматически, эффект измеряется и сообщается в центр управления nPhase.

Результаты позволили заказчикам BioLab определять, когда необходимо обслуживание, отправлять заявки на обслуживание, наблюдать потребление и даже менять параметры для отдельных химикатов, информацию, которая дает BioLab и ее возможность лучше управлять сетью поставок.

Операторы водных сооружений и коммерческие поставщики водных услуг имеют возможность получать доступ к своим системам через Интернет посредством широкого спектра готовых карманных устройств удаленной работы, таких как PDA (personal digital assistants), сотовые телефоны и пейджеры.

Критическая информация может быть автоматически передана на любое из этих устройств, вызывая немедленную реакцию или последующую проверку посредством более обширного анализа системы.

Эти и другие примеры, описанные авторами ранее [4], показывают, что решения на основе GSM являются весьма эффективными в областях учета энергоресурсов, удаленного сбора информации, навигации, телеметрии, логистики, безопасности и др.

Однако, в настоящее время на основе GSM еще не разработаны коммерческие системы по управлению сложными промышленными объектами, такими как, например, магистральные трубопроводы для перекачки нефти, нефтепродуктов и газа.

ЛИТЕРАТУРА

1. *Peach M.* Easy control in the Palm of your hand // Design News. February 1, 2001.

2. *Mintchell G.* Opto 22 Adds Capability to M2M Offering // Automation World. March 31, 2004.

3. *Emond M.* BioLab M2M Takes Over Water Service // M2M Magazine. September, 2003.

4. *Зыков Д.Д., Шелупанов А.А.* Управление магистральным трубопроводом через сеть связи стандарта GSM // Интеллектуальные системы в управлении, конструировании и образовании: Сб. статей. Выпуск 5 / Под ред. А.А. Шелупанова. Томск: Изд-во Института оптики атмосферы, 2006. С. 93–98.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Н.Е. Новиков, студент гр. 522-1., 5 курс, каф. КИБЭВС.
dj_novikoff@mail.ru

В настоящий момент «СургутНИПИнефть» состоит из множества отделов и структурных подразделений, в каждом из которых находится большое количество компьютерной техники (рабочие станции, принтеры, сканеры, сетевое оборудование). Кроме оборудования, находящегося в эксплуатации, некоторая часть находится на складах как запасные части, фактически выведенная из эксплуатации, но требующая учета. С течением времени происходит замена оборудования, старое изнашивается, выходит из строя. В связи с тем, что нет автоматизированной системы учета техники, скапливается большое количество различного рода информации на бумажных носителях, а также в виде текстовых файлов. Это существенно затрудняет поиск нужного оборудования и его владельца, бумажные носители портятся, занимают большое количество места. В ходе решения этих проблем была создана база данных.

Перед первым сеансом работы с системой необходимо убедиться, что работники отдела САПР произвели полную установку и настройку программного комплекса, а также дали права доступа к БД ORACLE системы учета и движения вычислительной техники на предприятии [1]. Задача базы данных – сохранять актуальную информацию о компьютерном оборудовании, такую как серийные и инвентарные номера, месторасположение, место входа в локальную сеть, принадлежность оборудования и т.д. Задача клиентского программного обеспечения – обновление и пополнение базы данных и выдача всей необходимой отчетной и справочной информации о компьютерном оборудовании. Оно должно позволять работать с базой данных на нескольких рабочих местах.

Для того чтобы построить инфологическую модель, необходимо проанализировать объект автоматизации и выделить основные таблицы, необходимые для хранения данных. На следующем этапе разработки была построена структура таблиц, в результате чего были наложены ограничения на каждый атрибут, выделены первичные и внешние ключи, и наложены ограничения на связи. Целостность данных поддерживается на уровне базы данных, благодаря первичным и вторичным ключам. Поле первичного ключа определяет уникальность строки в конкретной таблице. Вторичный ключ связывает поле в одной таблице со строкой в другой таблице.

База данных реализована на сервере Oracle 8.1.7i, выбор Oracle определяется тем, что на данном предприятии это основная система

управления базами данных. В качестве средства разработки клиентского программного обеспечения выбран пакет Oracle Forms [2].

Oracle Forms является одним из основных компонентов системы Developer/2000. Oracle Developer 2000 – одно из основных средств, разработки клиентского программного обеспечения на данном предприятии, обеспечивающее быструю разработку и поддержку в процессе эксплуатации. С помощью Oracle Forms можно быстро разрабатывать эффективные приложения для представления и обработки практически любых данных.

Приложения, созданные с помощью Oracle Forms, позволяют выполнять следующие действия:

– вставлять, обновлять, удалять и выбирать данные, используя богатый интерфейс работы с данными, работать как с текстовыми, так и с графическими данными, а также с элементами управления Visual Basic (VBX Controls); управлять работой форм, использующих различные окна и выполняющих отдельные транзакции базы данных;

– непосредственно использовать все возможности приложений Oracle Graphics и OLE2;

– работать с широким набором интегрированных меню;

– пересылать данные непосредственно в Oracle Reports.

При создании приложений с помощью Oracle Forms возможно [3]:

– разрабатывать формы, использующие самые различные данные, в том числе из базы данных Oracle;

– оперативно создавать приложения, используя мощные графические средства интерфейса GUI;

– разрабатывать приложения, работающие как в графическом, так и в символьном режимах;

– легко копировать и переносить объекты и их атрибуты из одного компонента приложения в другой;

– использовать уже знакомые продукты, входящие в Developer / 2000, такие как редактор макета, объектный навигатор и среда разработки PL/SQL.

Во избежание недоразумений и путаницы в терминологии необходимо привести несколько определений и понятий из языка инфологической модели (ЯИМ) по классификации Дейта:

Объект (сущность) – элемент какой-либо системы, информация о котором сохраняется. Объект может быть как реальным (например, принтер), так и абстрактным (например, событие – факт перемещения этого принтера, т.е. установка его другому пользователю).

Выделяются три основные класса сущности:

– стержневые,

– ассоциативные,

– характеристические.

Кроме того, выделяется подкласс ассоциативной сущности с названием: Обозначение.

Стержневая сущность (стержень) – это независимая сущность, как правило, определяющая основные, постоянные признаки объекта.

Ассоциативная сущность (ассоциация) – это сущность, реализующая связь многих во многом.

Характеристическая сущность (характеристика) – это связь между двумя сущностями, являющаяся частным случаем Ассоциации. Реализует связи: много к одному и один к одному. Уточняет стержневую.

Обозначение – это связь между двумя сущностями и отличается от характеристики только тем, что не зависит от обозначения сущности.

Атрибут – это информационное отображение свойств объекта. Каждый объект характеризуется рядом основных атрибутов. Например, сотрудник предприятия имеет такие атрибуты, как фамилия, имя, отчество. Каждый атрибут в модели должен иметь уникальное имя – идентификатор. Атрибут при реализации информационной модели на каком-либо носителе информации часто называют элементом данных, полем данных или просто полем.

Таблица – упорядоченная структура, состоящая из конечного набора однотипных записей.

Первичный ключ – атрибут (или группа атрибутов), позволяющих однозначным образом определить каждую строку в таблице.

Все современные средства СУБД поддерживают реляционную модель данных.

В реляционной модели данных объекты и связи между ними представляются в виде таблиц, при этом связи тоже рассматриваются как объекты.

Все строки, составляющие таблицу в реляционной базе данных, должны иметь первичный ключ.

ЛИТЕРАТУРА

1. *Стивен Бобровски.* Oracle 7 и вычисления клиент-сервер. М.: Лори,1995. 651 с.

2. *Когаловский М.Р.* Энциклопедия технологий баз данных. М.: Финансы и статистика, 2002. 800 с.

3. *Jayne Marlow, Glenn Maslen.* Oracle Forms: Учебный курс. Oracle Corporation, 1995.

СЕКЦИЯ 11

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

АНАЛИЗ НАТУРАЛЬНОГО ЧИСЛА НА ПРИНАДЛЕЖНОСТЬ ЕГО К КВАДРАТУ ЦЕЛОГО ЧИСЛА

М.С. Афанасьева, студентка 2 курса;
А.Н. Колесов, каф. систем радиосвязи (СРС), к.т.н., доцент
ТУСУР, г. Томск, т. 413-709, mrc@main.tusur .ru

Постановка задачи. Посредством анализа цифр натурального числа *C* (далее – «числа») установить, может ли *C* быть точным квадратом другого целого числа. Задача возникает тогда, когда при переборе некоторых целочисленных вычислительных ситуаций, связанных с нахождением квадратного корня (далее – «корня»), интерес представляют лишь числа, в которых целочисленный корень извлекается без остатка.

Сформулируем несколько утверждений (теорем). Пусть имеем квадрат двучлена, содержащего лишь целые числа $a,b,n \geq 0$.

$$(a \cdot 10^n + b)^2 = (a \cdot 10^n)^2 + 2 \cdot a \cdot 10^n \cdot b + b^2 . \qquad (1)$$

1. Из (1) следует: если *b* из *n* цифр, то $(a \cdot 10^n)^2$ даст вклад в результат, начиная с $(2n+1)$-го разряда. Таким образом, цифры в разрядах с $(n+1)$ до $2n$ определяются вторым и третьим слагаемыми в правой части (1).

2. Если в (1) вместо *a* подставить $(a+5)$, то $(n+1)$-я цифра квадрата совпадет с таковой в исходном выражении (1).

3. Второе слагаемое в правой части (1) всегда четно.

4. Квадрат *b* из *n* цифр содержит $2n$ или $(2n+1)$ цифр.

Пусть в *C* последние *n* цифр совпадают с таковыми в (1) и предположительно являются цифрами *n* младших разрядов квадрата *b*. Тогда можно утверждать следующее.

5. Если четность $(n+1)$-й цифры C совпадает с четностью $(n+1)$-й цифры b^2, то эта цифра принадлежит квадрату некоторого числа bx, большего, чем b.

Действительно, цифра $(n+1)$-го разряда в (1) сохраняет четность $(n+1)$-го разряда b^2 (по свойству 3). Значит, беря в качестве a цифру такой величины, чтобы последняя цифра суммы $(a\cdot 2\cdot b)$ с цифрой $(n+1)$-го разряда b^2 совпала с $(n+1)$-й цифрой C, найдем минимальное $bx = a\cdot 10^n + b$.

Если теперь с найденной цифрой a найти сумму двух последних слагаемых в правой части (1), то $(n+2)$-я цифра суммы будет представлять $(n+2)$-ю цифру bx^2 (по свойству 1).

Этот процесс может быть повторен до n раз (в пределах разрядов, где вклад $(a\cdot 10^n)^2$ отсутствует – смотри 1). Действительно, заменяя в свойстве 5 n на $(n+1)$, b на bx, найдем новое bx, содержащее уже $(n+2)$ цифры, и т. д.

Утверждения последних двух абзацев усматривается и из следующих выкладок. Второе слагаемое в (1) можно представить, как

$$2\cdot a\cdot 10^n b = 2\cdot 10^n b\cdot\left(\sum_{i=1}^{n} a_i\cdot 10^i\right), \qquad (2)$$

где a_i – значащие цифры числа a, стоящие левее n нулей справа (см. левую часть (1)), которые последовательно могут быть найдены, следуя доказательству в пункте 5 (при условии совпадения четностей соответствующих цифр у C и текущего bx^2, в противном случае процесс прерывается, поскольку C – не квадрат целого числа).

Вычисляя при фиксированном b в (2) правую часть равенства (с использованием процедуры из пункта 5), получим n цифр a после n нулей подряд, являющихся головными цифрами $2n$-значного основания, первые n цифр которого являются цифрами исходного основания b (для данного этапа, т.е. при фиксированном n).

Находя квадрат вновь полученного основания и проделывая аналогичные операции при благоприятных условиях, получим на очередном этапе $4n$ цифр подходящее текущее основание bx.

Для нахождения только что упомянутого квадрата можно к найденному (текущему) основанию (вместе с его продолжением в сторону старших разрядов) прибавить квадрат только что найденного числа (из цифр a_i), умноженного на $10^{2\cdot n}$. Выполнение такой операции вместо «возведения в квадрат» текущего основания позволит существенно сократить время вычислений (умножение чисел в два раза более коротких!).

Из описанной схемы определения подходящего (для данного C) текущего основания следует следующее утверждение.

6. С каждым этапом процедуры определения нового b длина b (по количеству цифр) удваивается.

Отсюда следует, что для анализа, например, 100-значного C «при старте с двузначным основанием b» нужно проделать не более 6 шагов. Шаг – определение очередных a_i в $[(n+1)\ (n+2)]$.

7. Если все шаги анализа по пункту 5 будут успешны, то в итоге будет получено предполагаемое основание b_{ok}, состоящее из $2n$ или $(n+2)$ (при нечетном числе цифр C) цифр (здесь n – число цифр у последнего предыдущего текущего основания). Если старшие разряды у b_{ok}^2 (с номерами, большими 2 n при четном числе цифр у C и большими $(2n + 1)$ в противном случае) совпадают с соответствующими разрядами у C, то $C = b_{ok}^2$. В противном случае C не является целочисленным квадратом.

Проверка работы алгоритма при длине чисел, соответствующих возможностям алгоритмического языка Паскаль, подтвердила его предполагаемые возможности и выявила возможные «разветвления путей анализа». Так, при старте рассматриваемого анализа, в отсутствие каких либо дополнительных сведений о числе C, число первоначальных вариантов анализа может достигать восьми. Однако при проведении дальнейшего анализа часть вариантов отпадает, как не удовлетворяющие текущим критериям формирования текущего *bx*.

Проверка осуществлялась с квадратами случайных целых чисел, в некоторые разряды которых намеренно вносились искажения значений цифр.

Остается задача выяснения «протяженности» ложных ветвей анализа. Эту работу планируется выполнить в скором времени.

Интерес к рассматриваемой проблеме существует давно, о чем свидетельствуют материалы в [1–3].

ЛИТЕРАТУРА

1. *Трост Эрнст*. Простые числа. М.: ГИФМЛ, 1959. 135 с.

2. *Журавлева И.С.* Таблица квадратов трехзначных чисел // Прикладной системный анализ. Материалы региональной научно-техничес-кой конференции студентов и молодых специалистов, 28–30 ноября 2000. С. 38.

3. Журавлева И.С., Колесов А.Н. Уточнение признаков неизвлекаемости целочисленного корня квадратного // Радиотехнические устройства, информационные технологии и системы управления. Конференция ТУСУР. Томск, 2001. С. 138–142.

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА «УВЕДОМЛЕНИЕ НАЛОГОПЛАТЕЛЬЩИКА О ЗАКРЫТИИ СЧЕТА В ОБСЛУЖИВАЮЩЕМ БАНКЕ»

В.В. Алехин, С.А. Пахандрин, А.Б. Миронов, ФВС, студенты 4курс
ТУСУР г. Томск, mail@inbox.ru

При неуплате налогов налогоплательщиком по его счету в банке приостанавливаются операции. Управление ФНС формирует для банков документ о приостановлении операций по счетам и отправляет в банк через инспекции по системе «Банк-счета».

Налогоплательщику, по счетам которого приостанавливаются операции, также формируется документ и отправляется на его юридический адрес по почте. Следует отметить, что формирование и отсылка такого документа – функция отдела ФНС, отличного от отдела приема отчетности по каналам связи. Документ формируется на базе готового шаблона решения в формате .doc.

В рамках проекта ЭОКС (электронная отчетность по каналам связи) было разработано программное обеспечение, позволяющее формировать и отправлять подобного рода уведомление по системе «Спринтер».

Данная задача была реализована проектной группой в виде небольшого приложения, не занимающего много места и не требующего большого количества системных ресурсов при работе. Программа находится в системном трэе и после соответствующей настройки работает полностью в автоматическом режиме, не беспокоя пользователя.

Принцип работы АИС «Sender».

Сканируется заранее заданная директория с определенным интервалом времени (устанавливается в настройках). При обнаружении файла с решением, производятся поиск абонента в базе данных ИФНС и автоматическое формирование письма на основании найденного документа-решения. Программа выделяет электронный адрес абонента в системе ЭОКС по ИНН организации, указанном в документе. В качестве транспорта «Sender» использует входящую в программный комплекс «Спринтер» Dipost-Factor LTD.

Использование разработки на стороне ИФНС вносит некоторые изменения в работу инспектора, автоматизируя функцию отправки уведомлений налогоплательщика о закрытии счета организации в обслуживающем банке. Это позволяет экономить время, затрачиваемое на оформления и отправку такого решения вручную, а также сокращает время доставки сообщения.

МОДЕЛИРОВАНИЕ УГРОЗ ДЛЯ ОБЪЕКТНО ОРИЕНТИРОВАННЫХ СЕТЕЙ ХРАНЕНИЯ ДАННЫХ

И.Л. Алферов
МИФИ, г. Москва, igor@alferov.net

Сети хранения данных (СХД, англ. Storage Area Network) стали широко применяться для надежного хранения больших массивов данных с оперативным доступом. В то же время публикации в средствах массовой информации свидетельствуют об устойчивом росте количества инцидентов, связанных с нарушением безопасности хранимой в СХД информации [1]. Это свидетельствует о недостаточной проработке вопросов обеспечения безопасности хранилищ данных в различных организациях.

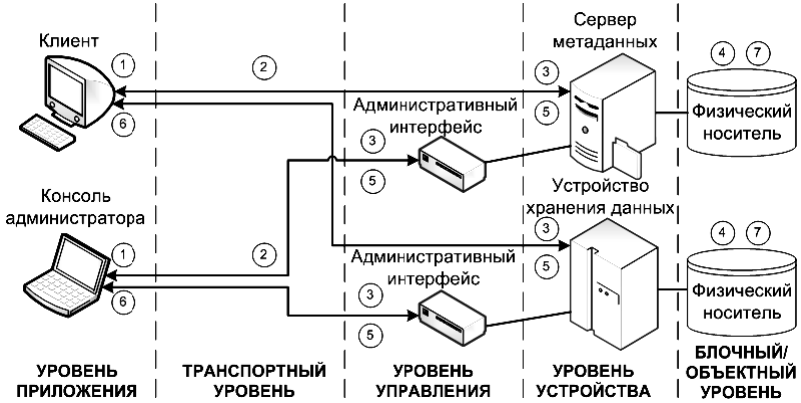
Даже если информационной безопасности уделяется достаточно внимания, а вопросы формирования политики безопасности и управления рисками решаются в соответствии со стандартами ISO 17799/ISO 27001, это не является достаточным условием защищенности СХД. Стандарты включают в себя практические требования и рекомендации общего характера, а каталоги угроз безопасности и контрмер в различных методологиях управления информационными рисками (таких как CRAMM или OCTAVE) не отражают специфики среды распределенного хранения данных. Поэтому анализ и управление рисками для СХД организации должны проводиться высококвалифицированными специалистами, обладающими знаниями о технических аспектах функционирования сети и способными выявить полное множество возможных уязвимостей и атак на систему. Сделанные на данном этапе ошибки напрямую влияют на безопасность СХД, так как отсутствие адекватной контрмеры хотя бы для одной разновидности атаки может привести к компрометации всей сети.

Для идентификации всех возможных угроз и уязвимостей в любом сложном комплексе может эффективно применяться системный подход – моделирование угроз [2]. Другие подходы, например «мозговой штурм», имеют более высокую вероятность того, что выявленные множества угроз и уязвимостей окажутся неполными.

Наиболее актуальным представляется вопрос моделирования угроз для СХД, построенных на основе стремительно развивающейся технологии объектно ориентированного хранения данных [3]. Хотя для традиционных СХД с блочным интерфейсом доступа к данным уже проведен ряд исследований отдельных классов атак и предпринята попытка построения модели угроз, особенности архитектуры объектно-ориентированных сетей приводят к необходимости проведения для них независимого анализа угроз.

Для моделирования угроз прежде всего необходимо классифицировать информационные активы, на которые могут быть нацелены атаки нарушителей. Для объектно ориентированных СХД такими активами являются хранимые данные, метаданные и управляющие данные. К управляющим данным относится любая информация, передаваемая через административные интерфейсы устройств сети.

Сам процесс моделирования угроз предлагается проводить путем последовательного анализа этапов жизненного цикла для каждого вида информационных активов. Выделяемые этапы жизненного цикла соответствуют пребыванию информации в структурно различных компонентах СХД, группируемых в ряд архитектурных уровней. На рисунке эти этапы представлены в соответствии с их нумерацией.



1. Жизненный цикл информационных активов в СХД

1. Создание/обновление данных. Информационные активы в СХД порождаются клиентскими и административными приложениями.

2. Передача данных. Созданная, обновленная или запрашиваемая информация передается через сетевую инфраструктуру.

3. Запись данных. Согласно поступившим запросам информация обрабатывается и сохраняется устройствами на физических носителях.

4. Хранение данных. Информация хранится на физических носителях до тех пор, пока не будет запрошено ее уничтожение.

5. Считывание данных. Для обработки запроса на получение информации устройство считывает данные с физического носителя и проводит их подготовку для отправки.

6. Получение данных. Приложение получает запрошенную информацию и может выполнять над ней дальнейшие операции.

7. Уничтожение данных. Информация, хранение которой больше не требуется, уничтожается с физических носителей.

Каждому этапу соответствует определенное множество точек доступа, которыми может воспользоваться нарушитель. Для 1-го этапа, например, можно выделить следующие точки доступа: устройства ввода/вывода, операционная система, используемые приложением файлы, оперативная память и сетевые интерфейсы. Анализ этапа жизненного цикла заключается в определении всех возможностей нарушения конфиденциальности, целостности или доступности информационного актива с использованием имеющихся точек доступа. Физические атаки, такие как хищение носителей данных, нарушение сетевых соединений или цепей питания устройств, рассматриваются наряду с остальными атаками. В результате анализа формируется иерархический перечень атак, структурными элементами которого являются: вид информационного актива (хранимые данные, метаданные, управляющие данные), этап жизненного цикла, точка доступа, вид угрозы (нарушение конфиденциальности, целостности, доступности) и атака, реализующая угрозу.

Предложенный подход к моделированию угроз позволяет выявить полное множество угроз и уязвимостей в объектно ориентированной СХД независимо от вероятности их появления и потенциального ущерба в случае реализации. Оценка вероятностей и величин ущерба входит в процесс анализа и управления информационными рисками, проводящийся после построения модели угроз. В результате этого процесса для СХД формулируются требования по безопасности и ставятся задачи разработки и внедрения необходимых контрмер.

ЛИТЕРАТУРА

1. *Hasan R., Yurcik W.A.* Statistical Analysis of Disclosed Storage Security Breaches // Proc. of the 2nd International Workshop on Storage Security and Survivability, 2006.

2. *Myagmar S., Lee A., Yurcik W.* Threat Modeling as a Basis for Security Requirements // Proc. of the Symposium on Requirements Engineering for Information Security, 2005.

3. ANSI INCITS 400-2004. Information Technology – SCSI Object-Based Storage Device Commands (OSD), 2004.

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ ПРЕДПРИЯТИЯ

О.А. Анженко, студент 5 курса

ТУСУР, г. Томск, zagadochka@mail.ru

Анализ информационных рисков – это то, с чего должно начинаться построение любой системы информационной безопасности. Он включает в себя мероприятия по обследованию безопасности предприятия, це-

лью которого 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.

Анализ рисков можно разделить на несколько последовательных этапов.

1. Инвентаризация информационных ресурсов предприятия.

На первом этапе осуществляется перечень ценной информации предприятия.

2. Изучение текущего состояния системы информационной безопасности.

На втором этапе следует изучение текущего состояния системы информационной безопасности с целью определения, что из защиты информации на предприятии уже реализовано, в каком объеме и на каком уровне.

3. Определение возможных угроз информационной безопасности предприятия.

На третьем этапе нужно описать все возможные угрозы и уязвимости информационной системы предприятия.

Угрозы по классам:

– форс-мажорные обстоятельства,
– недостатки организационных мер,
– ошибки человека,
– технические неисправности,
– преднамеренные действия.

Для составления полного списка угроз производится дальнейшая детализация каждого класса угроз. Можно также использовать уже существующие базы, содержащие наиболее распространенные угрозы и уязвимости (CRAMM, BSI , DSECCT) [1–3].

4. Составление таблицы рисков предприятия.

На четвертом этапе происходит расчет информационных рисков предприятия.

Для расчета рисков необходимо определить такие параметры, как величина ущерба от угрозы и вероятность ее возникновения.

Величина ущерба от угрозы может быть представлена в виде шкалы оценок, где каждой оценке ставится в соответствие ущерб, который может быть нанесен предприятию (табл. 1).

Далее, исходя из критичности возможных угроз для информационной системы и вероятности их реализации, составляется таблица рисков предприятия.

Таблица 1

Величина ущерба от угрозы

Величина ущерба (УЩЕРБ)	Описание
0	Раскрытие информации принесет ничтожный моральный и финансовый ущерб предприятию
1	Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение предприятия не затронуты
2	Финансовые операции не ведутся в течение некоторого времени, за это время предприятие терпит убытки, но его положение на рынке изменяется минимально
3	Значительные потери на рынке и в прибыли
4	Потери очень значительны, предприятие на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы
5	Предприятие прекращает существование

Вероятность возникновения угрозы также может быть представлена в виде шкалы оценок, определяющей частоту возникновения угрозы (табл. 2).

Таблица 2

Вероятность возникновения угрозы

Вероятность ($P_{\text{возникновения}}$)	Средняя частота появления
0	Данный вид атаки отсутствует
1	Реже, чем раз в год
2	Около 1 раза в год
3	Около 1 раза в месяц
4	Около 1 раза в неделю
5	Практически ежедневно

Используя данные табл. 1 и 2 для всех описанных на предыдущем этапе угроз, риск рассчитывается по следующей формуле:

$$\text{РИСК}=P_{\text{возникновения}} * \text{УЩЕРБ} \ . \qquad (1)$$

Таким образом, таблица содержит список угроз, где каждой из них ставится в соответствие величина риска (1).

Далее проверяется каждая строка таблицы рисков предприятия, определяется возможный максимальный риск. Строки с максимальными показателями означают, что данный вид угрозы высок для информационной системы предприятия. Следовательно, по этим видам угроз надлежит принять меры, направленные на снижение риска.

5. Рекомендация мер по снижению рисков.

На пятом этапе производится выбор необходимых контрмер, направленных на снижение риска от каждого из видов угроз, имеющих в таблице рисков предприятия максимальные значения.

ЛИТЕРАТУРА

1. www.dsec.ru – Digital Security.

2. www.citforum.ru/internet/infsecure/ – Методы и средства защиты информации (курс лекций).

3. www.security.ukrnet.net – Безопасность информационных технологий.

СИСТЕМА УПРАВЛЕНИЯ КОНТЕНТОМ WEB-РЕСУРСА СО СРЕДСТВАМИ АВТОРИЗАЦИИ И ШИФРОВАНИЯ

А.И. Балашов, студент 1 курса ФВС

ТУСУР, wirg@sibmail.com

На данном этапе развития сети Интернет часто возникает необходимость создания в короткое время Web-ресурса, наполнение его разнообразным контентом и его администрирование в процессе работы ресурса. Очень часто для этих целей разрабатывается или используется уже готовая Система управления контентом, которая позволяет производить все вышеперечисленные действия человеку не имеющему обширных знаний IT-индустрии.

Целью данной разработки является создание системы управления контентом (содержимым) (CMS), написанной на интерпретируемом языке PHP с применением технологий JavaScript, CSS, XML. Данная система может быть использована для хранения и публикации большого количества документов, изображений и других мультимедийных ресурсов. Такая система также позволяет управлять текстовым и графическим наполнением Web-сайта, предоставляя пользователю и администратору удобные инструменты хранения, публикации информации и мультимедийных ресурсов. Кроме того, такая система управления контентом должна иметь достаточно низкие требования к аппаратному обеспечению сервера, что в общем случае можно обеспечить, сводя к минимуму число запросов системы к базе данных. Необходимо также разработать систему авторизации пользователей, использующую шифрование для защиты от несанкционированного доступа к административным инструментам системы управления контентом [1].

В ходе работы ставились задачи:

- создать такой механизм работы CMS, при котором достигается минимальная нагрузка на аппаратную часть сервера;

• создать систему авторизации пользователей с возможностью шифрования пароля;

• упростить процесс загрузки мультимедиа контента на сервер; организовать поиск информации по заданным пользователем критериям в базе данных и вывод найденных элементов;

• предоставить инструментарий для администрирования системы и внесения в нее изменений пользователями с различными степенями доступа.

Созданная на данный момент CMS-система управления контентом сайта построена на принципе, позволяющем существенно сократить нагрузку именно на постулате «Генерация страниц при редактировании». Система такого типа при внесении изменений в содержание сайта создает набор статичных страниц, которые выводятся при каждом обращении пользователя к сайту. При таком способе жертвуется интерактивность, но уменьшается время вывода страницы. Система управления контентом имеет полноценные возможности для создания, удаления и редактирования всех элементов системы, а именно статей, категорий, пользовательских сообщений, опросов и голосований. Также в системе организовано создание учетных записей пользователей и их авторизация, т.е. процедура проверки соответствия пользователя и того, за кого он пытается себя выдать, с помощью имени и пароля, который содержится в зашифрованном виде в базе данных и впоследствии организуется предоставление административных полномочий на работу с системой. Кроме того, система управления контентом имеет возможность генерировать RSS и ATOM ленты новостей. В рамках системы управления контентом реализован механизм поиска данных по выбранным пользователем критериям в базе данных и механизм загрузки и хранения мультимедийных приложений на сервере [2, 3].

Данная разработка может найти практическое применение в качестве инструмента для создания и управления современным Интернет-проектом, позволяющего пользователям, помимо простого просмотра контента и получения лент новостей в виде RSS и ATOM, принимать участие в информационном обмене, используя возможности CMS. Для администрирования Web-ресурса построенного на данной системе, не требуется знания синтаксиса HTML.

ЛИТЕРАТУРА

1. *Мазуркевич А. Еловой Д.* PHP. Настольная книга программиста. М.: Новое знание, 2006, 495 с.

2. *Ульман Л.* Основы программирования на PHP: Самоучитель. М.: ДМК Пресс, 2001, 288 с.

3. *John Wiley & Sons.* PHP5 and MySQL. Bible. ftp:// ftp.ihome.net.ua/Books/IT/

БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Р.А. Белик, студент 5 курса, ФВС КИБЭВС
ТУСУР, г. Томск, ga-fsb@mail.ru

Информационная сфера все более превращается в арену международного соперничества, противоправных действий криминальных структур и террористов, создающих существенные угрозы национальным интересам государств, реализации прав и законных интересов личности, общества и государства. По мере распространения современных информационно-телекоммуникационных технологий по всему миру резко возрастают угрозы проведения актов информационного терроризма и возникновения информационных войн. Особую опасность такого рода действия представляют для России из-за нестабильного характера общественного и государственного развития Российской Федерации и ее субъектов.

Объектом исследования проведенной работы является разработка методов защиты и нормативно-правовая база при реализации информационно-телекоммуникационных сетей.

Цель работы – рассмотрение и разработка методов построения защиты информационно-телекоммуникационных сетей и законодательных актов, положений и стандартов необходимых для реализации безопасных информационно-телекоммуникационных сетей на территории Российской Федерации.

Реализация программы защиты информации должна осуществляться на основе комплексного использования систем и средств безопасности, исходя из предпосылки, что невозможно обеспечить требуемый уровень защищенности только с помощью одного отдельного средства или мероприятия, или их простой совокупности. Необходимо их системное согласование. В этом случае реализация любой угрозы может воздействовать на защищаемый объект только в случае преодоления всех уровней защиты.

В процессе работы были разработаны комплексный метод защиты и рекомендации, законы и нормативные акты, стандарты, лицензирования и других действий, связанных с осуществлением цели работы.

БЕЗОПАСНЫЕ КОРПОРАТИВНЫЕ СИСТЕМЫ

С.К. Бычков, студент гр. 522-1., 5 курса каф. КИБЭВС
serhius@yandex.ru

В настоящее время перед людьми, работающими в различных отраслях промышленности и бизнеса, ставятся все новые и различной степени сложности проблемы: усовершенствование и ускорение докумен-

тооборота организации, повышение эффективности бизнеса, разграничение доступности информации в компании, разграниченное управление данными в БД и т.д. Для решения такого рода проблем может послужить корпоративная система.

Существует множество определений «безопасной» корпоративной системы. Для данного проекта будем использовать следующее определение: «Безопасной называется система, при эксплуатации которой будет обеспечена защита данных, их целостность и сохранность» [1]. Кроме того, на современном этапе развития компьютерных технологий чаще всего строятся системы, упрощающие и ускоряющие документооборот в организации и за ее пределами.

Для построения безопасно функционирующей корпоративной системы были организованы следующие механизмы.

– Авторизация и аутентификация пользователей

Для предотвращения доступа несанкционированных пользователей к данным система в первую очередь должна распознавать своих пользователей, т.е. все действия в ней должны производиться от имени зарегистрированных (авторизованных) пользователей [1]. При этом система должна иметь механизмы проверки соответствия пользователя заявленному им имени (аутентификации). Подобные механизмы обязательно имеют и операционная система, и СУБД. Прикладная система вполне может использовать их для реализации собственных, но ни в коем случае они не могут заменять авторизацию и аутентификацию пользователя прикладной системы.

– Доступ к информации в базе данных

Современный стандарт SQL закрепляет поддержку СУБД избирательного контроля доступа, при котором пользователю СУБД предоставляются различные права доступа к различным объектам, с которыми СУБД работает. Стандартом SQL определены две команды: GRANT – для предоставления и REVOKE – для лишения пользователя привилегий, а в рамках сессии известен аутентифицированный пользователь СУБД через встроенную функцию CURRENTUSER.

– Группы и роли пользователей

Не следует забывать, что, когда при эксплуатации системы возникнет необходимость назначать права реальным пользователям, ответственный персонал столкнется с нелегкой задачей. При большом количестве пользователей корпоративной системы и немалом количестве сущностей, полномочия доступа к которым надо определять, администрирование системы может стать проблемой.

– Шифрование данных

ОС или СУБД могут шифровать данные в рамках реализации своей концепции безопасности, но этот механизм совершенно прозрачен для системы и не имеет отношения к ее дизайну.

– Аудит

Контрольное слежение является одним из важных аспектов обеспечения безопасности. Средства контрольного слежения должны позволять персоналу, отвечающему за эксплуатацию системы, получать различную информацию о действиях, выполненных пользователями. И целью здесь является не только обнаружение атак и несанкционированных действий. Дело в том, что стандартные промышленные СУБД не ведут базы как хронологические, а в процессе эксплуатации часто возникают вопросы о том, кто, когда и как изменял данные. И здесь крайне неудачным решением будут попытки частным образом решить проблему для отдельных таблиц, например, простое добавление в справочник клиентов столбцов с датой последнего изменения строки и идентификатором пользователя, выполнившего изменение. Необходим механизм, который позволит, с одной стороны, включить регистрацию хронологии изменений для любой таблицы, а с другой – зафиксирует информацию об истории изменений с необходимой подробностью.

– Целостность и сохранность данных

Потеря достоверной актуальной информации реально является одной из угроз безопасной эксплуатации приложения. Поэтому нельзя не коснуться этого аспекта при рассмотрении создания безопасной корпоративной системы [2].

Для разработки корпоративных систем возможно использование различных наборов программных средств. Это зависит от структуры функционирования организации [3]. Так, при наличии единой базы данных необходима СУБД для ее управления. Использование такого языка, как PHP, и такой базы данных, как MySQL, позволяет делать сайты динамическими, настраиваемыми и содержащими информацию, изменяемую в реальном времени.

Для достижения успешности бизнеса, совершенства функционирования организации требуется корпоративная система, которая свяжет все единицы бизнеса и организации [2].

ЛИТЕРАТУРА

1. *Обеспечение* информационной безопасности бизнеса / А.П. Курило [и др.]. М.: БДЦ-пресс, 2005. 512 с.

2. *Разработка* Web-приложений на PHP и MySQL: Пер. с англ./Лаура Томсон, Люк Веллинг. 2-е изд., испр. СПб.: ООО «ДиаСофтЮП», 2003. 672 с.

3. MySQL. Библиотека профессионала / Пер. с англ. М.: Вильяме, 2002. 624 с.

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ТЕЛЕНАБЛЮДЕНИЯ ПРЕДПРИЯТИЯ (АЛЮМИНИЕВОГО ЗАВОДА)

Н.П. Борисов, студент 5 курса каф. КИБЭВС
А.П. Зайцев, к.т.н., профессор каф. КИБЭВС
ТУСУР, г. Томск, e-mail: bnp_85tn@mail.ru

В настоящее время при проектировании комплексной системы безопасности (или модернизации старой) все больше внимания уделяется системам видеонаблюдения.

Последние события в мире еще раз напоминают нам, что вопросам безопасности нужно уделять гораздо больше внимания, чем уделяется в настоящее время. Спектр охранного оборудования, обеспечивающего безопасность людей в целом, достаточно широк и включает в себя пожарную и охранную сигнализации, системы контроля доступа и т.д. Но наиболее активным и информативным, а соответственно, и важным звеном в комплексной системе безопасности являются системы видеонаблюдения. Видеонаблюдение – это основа безопасности. Видеонаблюдение является одним из первых рубежей охраны объекта. При помощи него можно отчасти предотвратить событие или, если оно произошло, восстановить последовательность. Оно помогает не только контролировать обстановку на объекте, но и является первым помощником охранника.Система видеонаблюдения может быть как цифровой, так и аналоговой. В последнее время аналоговая система видеонаблюдения используется довольно редко, так как существенно уступает цифровой в силу ограниченного количества функций [1, 2].

Практика проектирование систем видеонаблюдения показывает, что необходим научно обоснованный подход к решению проблем и задач охраны объектов, в особенности если это особо важные, особо опасные объекты, объекты особого риска или объекты, содержащие большие материальные ценности. Очевидно, коль скоро действия преступников (нарушителей) часто носят не просто ухищренный, а системно продуманный профессионалами характер, им следует противопоставить организацию и оснащение системы видеонаблюдения, выполненные на более высоком уровне профессионализма. Этим и объясняется необходимость разработки обобщенной системной концепции по обеспечению объектов системами видеонаблюдения, которые в каждом конкретном случае должны быть адаптированы к каждому отдельному объекту, исходя из условий его функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды, обстановки [3–5].

Целью данной работы является разработка системы видеонаблюдения, позволяющей обеспечивать не только непрерывный оперативный контроль ситуации на объекте, но и автоматически обнаруживать вторжение в контролируемое пространство, осуществлять видеозапись тревожных событий или непрерывную запись всей видеоинформации.

Разработанная система теленаблюдения имеет следующие преимущества:

1) возможность использования камер различного типа;

2) возможность интеграции СТН в комплекс инженерно-технических средств охраны;

3) общее количество видеокамер имеет возможность расширения;

4) возможность задания неограниченного числа зон детекции движения;

5) благодаря применению алгоритма видеокомпрессии Delta-Wavelet, обеспечивается поддержка видеоархива большого объема;

6) осуществляется непрерывный мониторинг состояния элементов системы.

ЛИТЕРАТУРА

1. *Кравченко П.П., Хусаинов Н.Ш., Хаджинов А.А., Погорелов К.В., Шкурко А.Н.* Программная система многостороннего обмена аудиовидеоинформацией для использования в системах видеонаблюдения: Учебное пособие. М.: МИФИ, 1999.

2. *Иванов К.Н.* Системы видеонаблюдения на промышленных и протяженных объектах: Учебное пособие. М.: МИФИ, 2001.

3. http://www.complexsb.ru – Проектирование и монтаж систем видеонаблюдения и безопасности.

4. http://www.foreview.ru – Компания Foreman Electronics.

5. http://www.nslabs.ru – Компания NS Labs.

КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ НА БАЗЕ ОБРАТИМОГО КЛЕТОЧНОГО АВТОМАТА

С.И. Боровков, студент 4 курса

ТУСУР, г. Томск, т. 41-88-44, 8-913-850-2755, bhome@yandex.ru

Цель работы – разработка и реализация криптографического алгоритма на базе обратимого клеточного автомата.

Проблема использования криптографических методов в информационных системах в настоящий момент стала особо актуальна. Появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически не раскрываемыми.

Сейчас существует множество криптографических алгоритмов, которые применяются для шифрования информации. Они постоянно исследуются на предмет наличия уязвимостей. Естественно, существует потребность в разработке принципиально новых алгоритмов шифрования. Весьма интересно выглядит идея использования в криптосистемах клеточных автоматов [1].

Клеточные автоматы являются дискретными динамическими системами, поведение которых полностью определяется в терминах локальных зависимостей. Клеточный автомат может мыслиться как стилизованный мир. Пространство представлено равномерной сеткой, каждая ячейка которой, или клетка, содержит несколько битов данных; время идет вперед дискретными шагами, 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. Таким образом, законы системы являются локальными и повсюду одинаковыми.

Область клеточных автоматов предоставляет широкие возможности для построения криптографических алгоритмов. Можно создать множество различных модификаций в зависимости от требуемых показателей.

Особенность клеточных автоматов, благодаря которой они широко применяются в моделировании различных физических процессов, может быть использована и в криптографии. Эта особенность заключается в том, что будущее состояние каждой клетки поля клеточного автомата зависит от состояния ее соседей. При использовании разных правил (законов мира) при тех же начальных условиях система будет изменяться по-другому. Это предоставляет некоторые преимущества в плане защищенности зашифрованного сообщения от попыток криптоанализа.

Если каким-то образом представить данные, подлежащие шифрованию, в виде некоторого поля, состоящего из клеток, где клетка будет являться битом информации, т.е. иметь состояние ноль или единица, то мы получим начальное состояние клеточного автомата. В данном случае пространство представлено равномерной сеткой, каждая ячейка которой содержит один бит данных (кроме этого возможно использование трехмерной сетки). Остается только ввести набор правил (законы мира), по которому будет изменяться система, т.е. каждая клетка на каждом шаге будет вычислять свое новое состояние. Набор правил можно задавать в виде ключа, который используется для шифрования информации. Например, каждый элемент ключа будет содержать одно правило, которое будет действовать в течение одного шага времени. В начале каждого шага элемент ключа будет сменяться, и в течение этого шага система будет изменяться уже в соответствии с новым установленным прави-

лом. Таким образом, состояние системы изменится столько раз, сколько символов содержится в ключе. Но для расшифрования сообщения алгоритм криптографического преобразования должен быть обратимым. Теория обратимых клеточных автоматов содержит много проблем. Неизвестна, в частности, общая процедура определения того, имеет ли данное правило обратное. После проведения некоторых исследований стало ясно, что при соблюдении определенных правил обработки поля клеток в процессе его изменения согласно введенным законам можно сделать систему обратимой.

Какими преимуществами над известными сегодня криптографическими алгоритмами обладает алгоритм, построенный на базе обратимого клеточного автомата? Для начала необходимо отметить, что он удовлетворяет всем современным требованиям к криптосистемам. Алгоритм имеет принципиальное отличие: в нем не производятся типичные операции с числами. Самое существенное для шифра на базе обратимого клеточного автомата в плане его криптостойкости состоит в том, что клетка будет вычислять свое новое состояние по состояниям ее восьми соседей. Каждый бит информации будет зависеть от восьми соседних битов. Биты как будто сцеплены друг с другом, что делает дешифрование по частям невозможным. В отличие от всех распространенных шифров здесь результат преобразования каждого символа (блока символов) зависит не только от ключа, но и от соседних символов (блоков символов). Это создает серьезные проблемы при попытке дешифровать данные методом последовательного перебора (грубой силы), так как каждый новый выбранный элемент ключа приходится применять полностью ко всему шифротексту. В противном случае дешифровать даже часть текста не удастся. Это намного увеличивает время перебора. Алгоритм считается вычислительно безопасным, если он не может быть взломан с использованием доступных ресурсов сейчас или в будущем. В данном случае, если у криптоаналитика имеется исходный текст и шифротекст при условии, что ему известен сам алгоритм, методом грубой силы он теоретически сможет найти ключ, но только целиком. Он не сможет сократить время и найти только отдельные символы ключа. Ему придется пытаться найти весь ключ сразу.

Для взлома какого-либо шифра могут применяться параллельные компьютеры: задача разбивается на множество кусочков, решение которых не требует межпроцессорного взаимодействия. В нашем случае компьютеры должны постоянно взаимодействовать между собой, так как для вычисления каждого последующего возможного состояния системы необходимо вычислить ее возможное предыдущее состояние. Учитывая, что каждый элемент ключа может иметь 255 возможных со-

стояний, которые нужно применить ко всему зашифрованному сообщению, для каждого из этих вариантов необходимо применить еще столько же возможных состояний следующего элемента ключа и т.д.

Расчетное время дешифрования путем перебора всех возможных ключей при известной длине порядка 64 бит на современных машинах значительно превышает срок жизни отдельного человека (в десятки и сотни миллионов раз). Причем размер ключа не фиксирован.

Представленная реализация этого алгоритма позволяет шифровать файлы размером 1 мегабайт 64-битным ключом в среднем за 6 с, в зависимости от вычислительных возможностей машины.

Результаты архивирования зашифрованных файлов показали, что они практически не содержат избыточной информации, которая используется при криптоанализе. Это практическое доказательство стойкости шифра.

Использование обратимых клеточных автоматов дает преимущество в криптостйкости и простоте разработки алгоритма.

ЛИТЕРАТУРА

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

ЗАЩИТА ПРОТОКОЛОВ С ПОМОЩЬЮ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

В.М. Боровой, студент 5 курса каф. КИБЭВС
С.К. Росошек, доцент каф. КИБЭВС
ТУСУР, г. Томск, Victor2305@mail.ru

Проблема защиты информации в информационных системах в настоящее время особенно актуальна, тем более что существует тенденция перехода с бумажного документооборота на электронный. Одним из решений данной проблемы может служить использование электронной подписи в общей автоматизированной системе для передачи данных. В основе протокола этого класса содержится некоторый алгоритм вычисления ЭЦП на передаче с помощью секретного ключа отправителя и проверки ЭЦП на приеме с помощью соответствующего открытого ключа, извлекаемого из открытого справочника, но защищенного от модификаций. В случае положительного результата проверки протокол обычно завершается операцией архивирования принятого сообщения, его ЭЦП и соответствующего открытого ключа. Операция архивирования может не выполняться, если ЭЦП используется только для обеспе-

чения свойств целостности и аутентичности принятого сообщения, но не безотказности. В этом случае после проверки ЭЦП может быть уничтожена сразу или по прошествии ограниченного промежутка времени ожидания. Протоколы идентификации / аутентификации: в основе протокола идентификации содержится некоторый алгоритм проверки того факта, что идентифицируемый объект (пользователь, устройство, процесс, ...), предъявивший некоторое имя (идентификатор), знает секретную информацию, известную только заявленному объекту, причем метод проверки является, конечно, косвенным, т.е. без предъявления этой секретной информации. Обычно с каждым именем (идентификатором) объекта связывается перечень его прав и полномочий в системе, записанный в защищенной базе данных. В этом случае протокол идентификации может быть расширен до протокола аутентификации, в котором идентифицированный объект проверяется на правомочность заказываемой услуги. Роль секретной информации играет секретный ключ ЭЦП, а проверка ЭЦП осуществляется с помощью открытого ключа, знание которого не позволяет определить соответствующий секретный ключ, но позволяет убедиться в том, что он известен автору ЭЦП.

ЛИТЕРАТУРА

1. *Брюс Шнайер*. Прикладная криптография. М.: Триумф, 2002. 815 с.

2 *Иванов М.А.* Криптографические методы защиты информации в комплексных системах и сетях. М.: ОЦ. Кудиц-образ, 2001. 620 с.

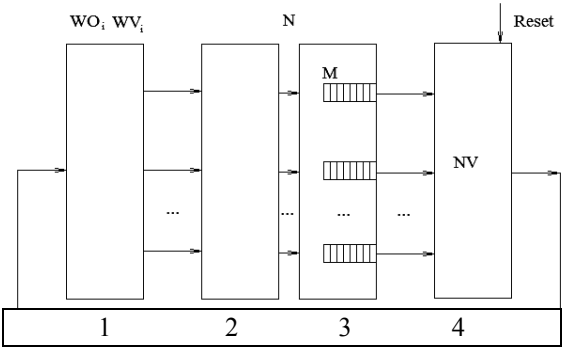
МОДЕЛИРОВАНИЕ СИТУАЦИИ ПИКОВОЙ НАГРУЗКИ В ИНФОРМАЦИОННОЙ СЕТИ

Н.Г. Булахов, аспирант

ТГУ, г. Томск, т. 923-402-72-32, nboolahov@yandex.ru

Сегодня вирусные атаки являются одной из первостепенных угроз информационной безопасности. Такие действия наносят финансовый ущерб, а также позволяют реализовать многие другие опасные угрозы. И это – несмотря на то, что для борьбы с такими вредителями уже разработано много сигнатурных, статистических и эвристических методов. В их основе лежат модели функционирования сети, по которым передается зловредный трафик в различных ситуациях (например, эпидемиологическая модель и ее модификации). Применение этих методов ограничивает приближенность описания функционирования сетей либо малое число релевантных параметров.

Поэтому актуальна разработка модели, устраняющей вышеперечисленные недостатки. Основу предлагаемой модели составляет устройство пересылки пакетных данных, имеющее N входов и N выходов (рисунок). Входы и выходы не равноправны между собой, что позволяет отразить наличие в реальной сети магистральных каналов и присоединение оконечных станций. Для учета различия между ними каждому каналу присваивается свой весовой коэффициент $W=WO+WV$, который показывает, насколько вероятнее появление пакета на данном входе относительно всех остальных. Вес WO соответствует нагрузке канала за счет полезных пакетов, вес WV – за счет саморазмножающихся пакетов. Входящие пакеты имеют адрес назначения, указывающий выходной порт. Каждый выходной порт рассчитан на очередь длиной M пакетов.



Структура устройства пересылки пакетов с N входами и N выходами:
1 и 2 – блоки распределения пакетов на входе и по выходам соответственно;
3 – блок очередей; 4 – блок обработки информации о выходных пакетах

В заданный такт времени условие того, что на входе n есть пакет, определяется формулой

$$f(n)=\begin{cases}1, rnd \le \dfrac{WO_i+WV_i}{WO_{\max}+WV_{\max}},\\ 0, rnd > \dfrac{WO_i+WV_i}{WO_{\max}+WV_{\max}}.\end{cases} \quad (1)$$

Если на входе n имеется пакет, то условие того, что он – саморазмножающийся либо полезный, есть

$$f_1(n)=\begin{cases}1, rnd \le \dfrac{WV_i}{WO_i+WV_i},\\ 2, rnd > \dfrac{WV_i}{WO_i+WV_i}.\end{cases} \quad (2)$$

В зависимости от порта назначения k каждый пакет помещается в выходную очередь согласно условию.

$$\sum_{i=1}^{k}(WO_i + WV_i) \le random(\sum_{i=1}^{N}(WO_i + WV_i)) < \sum_{i=1}^{k+1}(WO_i + WV_i) \qquad (3)$$

А если число пакетов в очереди достигает M, то M+1-й пакет отбрасывается. Между входом и выходом устройства есть положительная обратная связь. Если число пакетов на выходе каждого типа NO_t и NV_t., то обратная связь задается формулой

$$WV_{i,t} = WV_{i,t-1} \bullet \frac{NV_t + 1}{NV_{t-1} + 1}. \qquad (4)$$

Предложенное обобщенное устройство пересылки пакетных данных и статистическая модель его функционирования позволяет корректно описать работу реальной сети в различных ситуациях, включая случай пиковой нагрузки. Проведенная верификация модели показала ее корректность. Достоинством предложенной модели оказывается возможность учета различных сетевых топологий с целью выяснения их влияния на распространение саморазмножающихся пакетов. При этом принципы построения исходной модели и соотношения (1)–(4) сохраняются.

ЛИТЕРАТУРА

1. *Zou C.C., Gong W, Towsley D.* Code Red Worm Propagation Modeling and Analysis // Доступно в сети Internet:
http://tennis.ecs.umass.edu/~czou/research/codered.pdf

2. *Kim J., Radhakrishnan S., Dhall S.K.* Measurement and Analysis of Worm Propagation on Internet Network Topology // Доступно в сети Internet: http://www.computer.org.ru/ieee_lib/Catalog/catalog_14_.html

МОДЕЛЬ КИБЕРПРЕСТУПЛЕНИЯ КАК СРЕДСТВО АНАЛИЗА ФАКТОВ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

И.В. Давыдов, аспирант кафедры КИБЭВС
ТУСУР, г. Томск, 413-426, davidoffi@mail.ru

С каждым днем все большее число компьютеров и компьютерных сетей подключается к глобальной информационной сети Интернет, становясь тем самым доступными для киберпреступников. Количество киберпреступлений с каждым годом растет, и, что самое главное, повышается технологичность их совершения.

Не многие из пользователей ПК при работе в «глобальной паутине» не задумываются о проблемах безопасности, даже не подозревая, что тем самым только помогают злоумышленникам, предоставляя им свои информационные и аппаратные ресурсы в негласное пользование [1–3].

Вполне очевидно, что все киберпреступления совершаются по какой-то определенной модели, что существуют определенные этапы, через которые обязательно необходимо пройти злоумышленнику при совершении противоправных действий (например, изучение объекта атаки, получение доступа к объекту, кража информации и заметание следов) [4, 5].

Все созданные до данного момента модели совершения киберпреступлений в общей части содержат три этапа: изучение жертвы, атака на жертву и сокрытие следов киберпреступления. Каждый из этапов содержит по три стадии: рекогносцировка, сканирование, составление карты, получение доступа к системе, расширение полномочий, кража информации, уничтожение следов, создание «черных ходов» и отказ в обслуживании [6]. Однако у всех имеющихся моделей киберпреступлений имеется мно-жество недостатков, касающихся отображения процессов формирования связей, управлений и механизмов, а также среды их возникновения.

На основании этих недостатков была создана новая модель киберпреступлений, которая содержит три основных этапа – информационный обмен, совершение киберпреступления, расследование киберпреступления. Для анализа фактов получения несанкционированного доступа к информации интерес будет представлять этап совершения киберпреступления, потому что для полноценной оценки необходимо восстановить первоначальную ситуацию и понять, что произошло [7].

Этап совершения киберпреступления содержит шесть стадий – получение доступа, расширение полномочий, кража информации, зомбирование, уничтожение следов и отказ в обслуживании.

Поскольку после каждого шага злоумышленника рождаются все новые следы, ущерб соответственно становится специфическим. Тщательно исследуя ущерб и проводя обратные действия с объектом атаки, возможно реконструировать само киберпреступление буквально по шагам.

Так, например, если в ходе анализа узнается, что злоумышленник периодически похищал конфиденциальную информацию с закрытого источника в сети, становится очевидным, что он не мог провернуть этого без первоначального получения доступа к сети объекта, без увеличения полномочий в данной сети, без сканирования информационных ресурсов и без зомбирования объекта (исключения составляют инсайдеры). Информация обо всем этом непременно должна остаться в файловых журналах серверов, тщательное изучение которых вполне может указать непосредственно на злоумышленника.

Если в ходе изучения фактов узнается, что особо ценная информация уничтожена общеизвестными вредоносными программами, которые не могли проникнуть на объект вследствие наличия на последнем межсетевого экрана, то необходимо уделить особое внимание открытым каналам передачи данных (флеш-накопители, компакт-диски и т.п.), а также произвести поиск приватных кодов. Подозрения могут в этом случае пасть на упакованные исполняемые файлы в системных папках операционной системы, которых просто там быть не должно.

Или, например, если становится известным, что злоумышленник модифицировал данные в определенной базе данных, то стоит уделить внимание модифицированным в этот период записям, в результате чего можно определить круг учетных записей, под которыми был получен несанкционированный доступ. Также стоит уделить внимание системным журналам базы данных, в которых может остаться информация о том, под какой учетной записью пытался получить доступ злоумышленник и был ли пароль взломан грубым перебором или был уже заранее известен. Из анализа проведенных злоумышленником изменений можно определить уровень его познаний в области этой базы данных и сузить круг подозреваемых лиц.

Пошаговое восстановление хроники событий в первую очередь необходимо правоохранительным органам для расследования киберпреступлений. Однако оно также полезно и для администраторов безопасности объекта, которые могут практически оценить действительные угрозы, оценить риски и управлять ими. Таким образом, первые получат существенный организационный и технический вклад в расследовании киберпреступления, а вторые получат проверенную практикой эффективную политику безопасности.

Также с помощью модели киберпреступлений администраторы безопасности могут провести анализ вероятных угроз и оценить риски, связанные с ними, что, в свою очередь, будет являться серьезным упреждающим воздействием.

Только четкое представление проводящего анализ специалиста о том, что все кибепреступления совершаются в определенной последовательности, а также о том, какие следы рождаются в процессе информационного взаимодействия на разных стадиях, позволят ему взглянуть на имеющиеся факты получения несанкционированного доступа к охраняемой информации комплексно и адекватно.

ЛИТЕРАТУРА

1. *Lewis J.A.* Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. Washington, D.C., 2003. http:// crime.vl.ru/docs/stats/stat_82.htm

2. *Shinder D.L.* Scene of the Cybercrime: Computer Forensics Handbook, Chapter 1, Facing the Cybercrime Problem Head On, Center for Strategic and International Studies. Washington, D.C., 2002. http://crime.vl.ru/docs/stats/stat_68.htm

3. *Denning D.E.* Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, Georgetown University. N.Y., 2001. http://crime.vl.ru/docs/stats/stat_92.htm

4. *Расторгуев С.П.* Информационная война. Проблемы и модели. Экзистенциальная математика. М.: Гелиос АРВ, 2006. 240 с.

5. *Тропина Т.* Киберпреступность и кибертерроризм. http://www.phreaking.ru/printpage.php?s=&pageid=54233

6. *Макклуре С., Скембрэй Дж., Куртц Дж.* Секреты хакеров, проблемы и решения сетевой защиты. М.: ЛОРИ, 2001. 435 с.

7. *Давыдов И.В.* Формализация модели совершения киберпреступлений, совершаемых с использованием вредоносных кодов. Вестник Томского политехнического университета. 2006. Т.309. № 8. С. 126–129.

ЗАЩИЩЕННЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

А.Ю. Ефимов, С.О. Козьмин, студенты 5 курса каф. КИБЭВС
Н.А. Новгородова, ассистент каф. КИБЭВС
ТУСУР, г. Томск, efimov5221@yandex.ru

Электронный документооборот (ЭДО) подразумевает организацию конфиденциальной переписки между участниками системы, использование электронно-цифровой подписи для заверения документов и обмен ими в электронном виде.

Основой безопасного использования ЭДО в открытых компьютерных сетях является необходимость гарантированного подтверждения:

– личности абонента, отправлявшего электронный документ;

– того, что документ обязательно будет получен и может быть прочитан только указанным адресатом;

– того, что при передаче по сети в документ не внесены изменения.

Эти гарантии обеспечиваются при помощи специальных программно-технических решений. Аутентификация абонента основывается на использовании электронного цифрового паспорта – аналога удостоверяющего документа. Электронно-цифровая подпись является средством авторизации электронных документов и контролирует их целостность. Секретность документа и недоступность его содержимого для всех, кроме указанного адресата, обеспечиваются его кодированием при запечатывании в электронный конверт.

Защита электронных документов наиболее эффективна в специализированных приложениях – системах защищенного документооборота,

защищенных клиент-серверных и веб-приложений. Основной принцип таких систем – защита документа с момента его создания и до момента его уничтожения. В тех организациях, в которых весь документооборот ведется в системах защищенного документооборота, конфиденциальные документы наиболее защищены от внутренних угроз. Все действия авторизованных пользователей с конфиденциальными документами, включая их сохранение в неавторизованном месте, печать и другие, представляющие угрозу утечки информации, отслеживаются и документируются. Такие системы хранят все черновики и версии документов, любые изменения и попытки несанкционированных действий фиксируются.

Защищенный юридически значимый обмен документами в электронном виде (первичной бухгалтерской и налоговой документацией, счетами-фактуры, договорами, соглашениями и др.) происходит на основе средств криптографической защиты информации (СКЗИ) [1–5].

В основе криптографических решений – понятия «шифрование» и «электронная цифровая подпись (ЭЦП)». В соответствии с действующим законодательством РФ использование несертифицированных средств ЭЦП не допускается в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления.

Тем самым защищенный юридически значимый электронный документооборот для государственных структур должен обеспечиваться за счет использования сертифицированных средств криптографической защиты информации.

Защищенный электронный документооборот необходим для решение следующих задач:

1. Удобная и безопасная работа с документами (защищенный документооборот через Интернет):

– между организацией и ее филиалами, иными отдаленными структурными подразделениями;

– внутри самой организации (между отделами, службами, специалистами с разными уровнями доступа к документам);

– между государственными структурами и бюджетополучателями;

– налоговая и бухгалтерская отчетность (обмен документами в электронном виде по телекоммуникационным каналам связи);

– предоставление информации от официальных источников (отчетов, планов, заявлений, договоров и т.д.) большому числу контрагентов.

2. *Передача конфиденциальных и рабочих документов по защищенному соединению*, что позволит избежать беспокойства по поводу просмотра важной информации, ее искажения и перехвата.

3. *Централизованное и скоординированное размещение документов* и файлов, предназначенных *для широкого круга контрагентов*, в публичных разделах сервиса для открытого доступа и ознакомления с информацией.

ЛИТЕРАТУРА

1. http://www.rutoken.ru/ – Интернет ресурс.
2. http://www.rczi.ru/ – Интернет ресурс.
3. http://www.trusted.ru/ – Интернет ресурс.
4. http://www.infowatch.ru/ – Интернет ресурс.
5. http://www.infosec.ru/ – Интернет ресурс.

ПРИМЕНЕНИЕ КРИПТОЯДРА К ЗАЩИТЕ БАЗ ДАННЫХ

А.Ю. Ефимов, студент 5 курса каф. КИБЭВС
Н.А. Новгородова, ассистент каф. КИБЭВС
ТУСУР, г. Томск, efimov5221@yandex.ru

Защита баз данных является одной из самых сложных задач, стоящих перед подразделениями, отвечающими за обеспечение информационной безопасности. С одной стороны, для работы с базой необходимо предоставлять доступ к данным всем сотрудникам, кто по долгу службы должен осуществлять сбор, обработку, хранение и передачу конфиденциальных данных. С другой стороны, укрупнение баз данных далеко не всегда имеет централизованную архитектуру (наблюдается ярко выраженная тенденция к территориально распределенной системе), в связи с чем действия нарушителей становятся все более изощренными. При этом четкой и ясной методики комплексного решения задачи защиты баз данных, которую можно было бы применять во всех случаях, не существует, в каждой конкретной ситуации приходится находить индивидуальный подход.

В первую очередь это управление доступом пользователей. С точки зрения перспективности, удобства управления и надежности, можно рекомендовать схемы ролевого управления, основанные на применении в качестве расширенных учетных записей пользователей цифровых сертификатов X.509.

Эффективным способом защиты конфиденциальной информации, хранящейся в таблицах БД, может оказаться ее шифрование с помощью стойкого криптоалгоритма. Этим обеспечивается хранение информации в «нечитаемом» виде. Для получения «чистой» информации пользователи, имеющие санкционированный доступ к зашифрованным данным, имеют ключ и алгоритм расшифрования [1].

Защиту баз данных шифрованием предполагается выполнять при помощи разработанного программного продукта, использующего криптоядро CriptoMind, которое исполнено в виде динамической библиотеки и предназначено для выполнения основных процедур асимметричной криптографии на основе эллиптических кривых [2].

Библиотека содержит реализацию следующих стандартов:

а) стандарт ЭЦП ГОСТ Р 34.10-2001;

б) стандарт хэш-функции ГОСТ Р 34.11-94;

в) стандарт симметричного шифрования ГОСТ 28147-89;

г) алгоритмы ДПСЧ из стандарта FIPS 186-2;

д) модифицированный алгоритм асимметричного шифрования по схеме ElGamal на основе эллиптичских кривых.

Существует два направления защиты баз данных шифрованием:

– шифрование файлов баз данных. В этом случае не имеет значение выбор СУДБ, таким образом, возможна универсальная защита любых баз данных;

– шифрованием содержимого таблиц баз данных, что накладывает некоторые ограничения, связанные с возможностью СУДБ работать с внешними программными модулями (например, CriptoMind).

Реализация предложенных методов защиты баз данных позволит уменьшить вероятность несанкционированного доступа к базам данных, а также позволит осуществить защищенный документооборот в общедоступных сетях.

ЛИТЕРАТУРА

1. *Рябко Б.Я., Фионов А.Н.* Криптографические методы защиты информации: Учебное пособие. М.: Горячая линия – Телеком, 2005.

2. Бергер Д.А. Пояснительная записка к дипломной работе. Реализация и исследование эффективности работы криптоядра. Томск, 2006.

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ МАРКОВСКИХ ПРОЦЕССОВ

С.С. Ерохин, 5 курс, ФВС

ТУСУР г. Томск, ess_84@inbox.ru

Вопросы обеспечения информационной безопасности исследуются в разных странах довольно давно. В настоящее время сложилась общая точка зрения на концептуальные основы информационной безопасности. Четко стандартизовать аспекты безопасности впервые были удачно предприняты в Британском стандарте BS7799 «Практические правила

управления информационной безопасностью» в 1995 г. Позже этот стандарт переиздан в 2002 г. – ISO1779902. Одним из основных критериев в стандарте ISO1779902 является критерий анализа рисков. Само понятие «анализ рисков» появилось сравнительно недавно и вызывает большой интерес у специалистов в области информационной безопасности.

Анализ информационных рисков – это процесс комплексной оценки защищенности информационной системы (ИС) с переходом к количественным или качественным показателям степени защищенности информационной системы.

Оценка защищенности ИС предполагает изучение и систематизацию угроз защиты информации, а также определение требований к средствам защиты.

Изучение и систематизация угроз защиты информации предусматривает следующие этапы [1]:

а) выбор объектов ИС и информационных ресурсов, для которых будет проведен анализ;

б) разработка методологии оценки риска;

в) анализ угроз и определение слабых мест в защите;

г) идентификация угроз и формирование списка угроз;

д) формирование детального списка угроз и матрицы угрозы/элементы ИС или информационных ресурсов.

Для построения надежной защиты необходимо выявить возможные угрозы безопасности информации, оценить их последствия, определить необходимые меры и средства защиты.

Разнообразие потенциальных угроз столь велико, что все равно не позволяет предусмотреть каждую из них, поэтому анализируемые виды уместно выбирать с позиций здравого смысла, одновременно выявляя не только собственно угрозы, вероятность их осуществления, масштаб потенциального ущерба, но и их источники.

Оценка защищенности может проводиться с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации [2].

Так как модели анализа защищенности ИС на данный момент существуют в ограниченном количестве, была предпринята попытка формализации и написания такой модели. В основу данной модели была заложена теория скрытых Марковских процессов [3]. При помощи этой теории можно построить граф для ИС, определить вероятности нахождения системы в каком-либо состоянии, при воздействии угроз ИБ, а следовательно, давать рекомендации по повышению уровня безопасности ИС путем введения контрмер и формировать требования к системе защиты информации.

Модель определения поведения системы при воздействии угроз ИБ и контрмер данным угрозам.

Исходные данные:

1. Множество угроз информационной безопасности $X=\{x_i\}$.

2. Множество контрмер угрозам безопасности $Y=\{y_i\}$.

3. Вектор начального состояния Марковского процесса $\overline{a}=(a_0,a_1,...,a_i)$, где i – количество состояний рассматриваемой системы.

4. Матрица переходных вероятностей Марковского процесса размерностью $m\times n$:

$$D=\begin{pmatrix} d_{0,1} & d_{0,2} & .... & d_{0,m} \\ d_{1,1} & d_{1,2} & .... & d_{1,m} \\ .... & .... & .... & .... \\ d_{n,1} & d_{n,2} & .... & d_{n,m} \end{pmatrix}.$$

5. Интенсивность потока отказа (угрозы ИБ $x_i\in X$) $\lambda=(\lambda_0\ \lambda_1\ ...\ \lambda_i)$, причем $\sum_{i=0}^{i}\lambda_i=1$, где $i-$ количество состояний рассматриваемой системы.

6. Интенсивность потока восстановления (контрмеры угрозам ИБ $y_i\in Y$) $\mu=(\mu_0\ \mu_1\ ...\ \mu_{i-1})$, причем $\sum_{i=0}^{i-1}-\mu_i=1$, где $i-$ количество состояний рассматриваемой системы.

Алгоритм работы модели:

Находим распределение нестационарных вероятностей состояния системы в момент времени (t) [3,4].

Уравнения Колмогорова составляют систему дифференциальных уравнений и могут быть представлены в следующем виде: $\dot{x}=x\cdot A$, где $x=(x_0(t),x_1(t),...,x_{n-1}(t))$ – вектор строка, компонентами которой являются неизвестные функции; $\dot{x}=\left(\frac{d}{dt}x_0(t),\frac{d}{dt}x_1(t),...,\frac{d}{dt}x_{n-1}(t)\right)$ – вектор производных функций (градиент); $A=(a_{ij})_{k\times k}$ – квадратная матрица из постоянных коэффициентов.

Решение системы линейных дифференциальных уравнений $\dot{x}=x\cdot A$ удобно выразить через собственные числа $(\upsilon_1,\upsilon_2,....,\upsilon_{k-1})$ и собственные векторы $\left(z^{\langle 1\rangle},z^{\langle 2\rangle},...,z^{\langle k-1\rangle}\right)$ матрицы A^T порядка k, тогда решение системы уравнений можно представить в виде $x(t)=\sum_{i=0}^{n-1}b_i e^{\upsilon_i t}(z^{\langle i\rangle})^T$.

Алгоритм решения системы дифференциальных уравнений $x(t)=\sum_{i=0}^{n-1} b_i e^{\upsilon_i t}(z^{\langle i\rangle})^T$ [3, 4]:

а) формируем матрицу А согласно формуле $A=D(P-I)$, где D – диагональная матрица, на диагонали которой стоят интенсивности потока отказов (угрозы ИБ) $\lambda_0,\lambda_1,...,\lambda_{n-1}$;

б) находим собственные числа $(\upsilon_1,\upsilon_2,....,\upsilon_{k-1})$ и собственные векторы $\left(z^{\langle 1\rangle},z^{\langle 2\rangle},...,z^{\langle k-1\rangle}\right)$ матрицы A^T;

в) составляем матрицу Z, столбцами которой являются собственные векторы $\left(z^{\langle 1\rangle},z^{\langle 2\rangle},...,z^{\langle k-1\rangle}\right)$;

г) формируем вектор-строку $e^{(i)}=(0,...,0,1,0,...,0)$ с единственной единицей на i-м месте и вычисляем вектор $b=(b_0,b_1,...,b_{n-1})$ по формуле $b=e^{(i)}\left(Z^T\right)^{-1}$;

д) вычисляем вектор-строку $x(t)=(p_{i,0}(t),p_{i,1}(t),...,p_{i,n-1}(t))$.

2. Задаем интенсивность потока восстановления μ (контрмеры заданным угрозам).

3. Составляем систему дифференциальных уравнений Колмогорова для Марковского процесса по формуле

$$\frac{dp_i(t)}{dt}=\sum_{j=1}^{n} p_j(t)\lambda_{ji}(t)-p_i(t)\sum_{j=1}^{n}\lambda_{ij}(t)$$

и вычисляем вероятность состояний системы в момент времени t (момент времени должен быть одинаковым при определении вероятности состояний без учета потока восстановления μ и с учетом потока восстановления μ). Система дифференциальных уравнений для разных систем будет разная.

4. Проводим анализ и определяем эффективность введенного потока восстановления μ (контрмер для угроз ИБ) по формуле $E=(P_{i(\lambda)}-P_{i(\lambda,\mu)})\cdot 100\%$, т.е. эффективность i-й контрмеры относительно i-й угрозы. Отрицательный результат говорит от том, что контрмеры не являются эффективными, а положительный результат говорит о той или иной эффективности контрмер поставленным угрозам ИБ.

Модель является адекватной только в том случае, когда собственные числа матрицы являются различными.

ЛИТЕРАТУРА

1. *Петренко С.А.* Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК-Пресс, 2005. 384 с.

2. *Домарев В.В.* Безопасность информационных технологий. Системный подход: К.: ООО «ТИД ДС», 2004. 992 с.

3. *Вентцель Е.С., Овчаров Л.А.* Теория случайных процессов и ее инженерные приложения. М.: Наука. Гл. ред. физ.-мат. лит., 1991. 384 с.

4. *Андронов А.М., Копыткова Е.А., Гринглаз Л.Я.* Теория вероятностей и математическая статистика: Учебник для вузов. СПб.: Питер, 2004. 461 с.

БЕЗОПАСНОСТЬ ДАННЫХ В СУБД ORACLE

И.В. Фролов, студент 3 курса;
Н.А. Новгородова, ассистент каф. КИБЭВС
ТУСУР, г.Томск, т.89234077762, ivanfr@sibmail.com

На сегодняшний день использование хорошо защищенных СУБД является наиболее актуальным вопросом. Так как базы данных используются почти во всех сферах жизнедеятельности, также немаловажно, чтобы они были защищенными и использовали различные криптографические технологии для сокрытия конфиденциальной информации. Oracle является одной из таких СУБД, которая может обеспечивать защиту конфиденциальных данных.

На протяжении 25 лет Oracle совершенствовал и улучшал свои технологии безопасности. На данный момент Oracle является одной из мощнейших СУБД, в которой есть все необходимое для хранения и защиты данных. СУБД Oracle позволяет использовать хранимые процедуры, триггеры, представления и многое другое. Oracle позволяет управлять доступом на уровне строк, что влияет на безопасность БД. Шифрование данных в Oracle используется как дополнительная мера безопасности, которая позволяет использовать следующие алгоритмы шифрования данных: DES, 3DES, AES, RC4, MD5 Checksum.

В Oracle присутствуют сетевые технологии безопасности, которые обеспечивают достаточный уровень конфиденциальности защиты данных:

– строгая Аутентификация (3rd Party X.509, Kerberos, Radius),
– криптографическое контрольное суммирование,
– аутентификация и авторизация через LDAP,
– аутентификация и авторизация с помощью других решений,
– шифрование (Net8 Native, SSL, Java).

Поддерживает следующие технологии аутентификации:
– Public key infrastructure (PKI),
– RADIUS,
– Kerberos,
– Token и smart-карты
– Биометрические.

Данные технологии аутентификации и сетевой безопасности препятствуют не только получению доступа злоумышленников к системе, но и получения конфиденциальной информации, находящейся непосредственно в базе данных.

Также Oracle поддерживает симметричные, асимметричные и гибрид – симметричные + асимметричные технологии шифрования. Симметричные хороши тем, что они быстрые и понимаемые (математика не меняется). В асимметричных – проста технология распространения ключей, плюс великолепный механизм для цифровой подписи. Эти технологии позволяют надежно хранить, передавать данные между лицами, кому они предназначены, а если вы не тот, кому предназначены эти данные, вы их просто не сможете получить. В Oracle возможно применение цифровых подписей, что позволяет удостовериться в целостности и достоверности полученной информации, что немаловажно для различных организаций.

СИСТЕМА ЦЕНТРАЛИЗОВАННОГО ХРАНЕНИЯ ИДЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ

О.И. Галкин, аспирант каф. КИБЭВС
ТУСУР, г. Томск, galkin.oleg@gmail.com

В данной статье приведено краткое описание проблемы идентификации пользователей в сети Интернет, кратко описаны существующие на данный момент решения по управлению идентификационной информацией, приведены их достоинства и недостатки, и предложен собственный вариант решения данной проблемы, основанный на централизованном хранении идентификационной информации.

На сегодняшний день практически повсеместно в сети Интернет идентификация пользователя осуществляется посредством идентификатора пользователя (login) и пароля. У данного способа идентификации имеется ряд существенных недостатков, которые являются причиной многих проблем безопасности, существующих в сети Интернет. Этими недостатками являются, например, недостаточная стойкость паролей, дублирование паролей, передача идентификаторов пользователей и па-

ролей в сети в открытом незашифрованном виде. У данного способа также имеются недостатки удобства использования (usability), а именно сам факт необходимости ввода идентификатора пользователя и пароля на целевом Интернет-ресурсе – WEB-сайте, что является причиной «фишинга», вида атак с подменой страницы Интернет-ресурса, где пользователем вводится идентификационная информация. Перечисленные недостатки дали толчок к исследованиям и разработке новых систем идентификации пользователей сети Интернет.

На данный момент существуют следующие решения для управления идентификационной информацией пользователей сети Интернет:

– инфраструктура открытых ключей (ИОК),

– технология Card Space фирмы Microsoft,

– OpenID.

Инфраструктура открытых ключей [1] представляет собой систему, предназначенную не только для идентификации пользователей в сети Интернет. Она решает множество проблем, включая проблемы доверия (trust). Это является, несомненно, достоинством данной системы в целом, но это является причиной сложности понимания, внедрения и использования инфраструктуры открытых ключей в классическом ее виде для целей, связанных с управлением идентификационной информацией.

В основе технологии Card Space фирмы Microsoft [2] лежат некоторые принципы инфраструктуры открытых ключей, но Card Space – это технология, предназначенная для управления идентификационной информацией. Данная технология не решает вопросы доверия.

Технология Card Space имеет следующие достоинства:

– разработана в соответствии с законами идентификации в сети Интернет [3];

– технология разработана на основе открытых протоколов, что позволяет сторонним разработчикам создавать ее реализацию для клиентских и серверных станций;

– имеет модульную архитектуру, которая обеспечивает гибкость реализации отдельных ее подсистем.

Недостатки технологии Card Space:

– необходимость создания/модификации клиентского и серверного программного обеспечения;

– наличие файла хранилища карт, который в случае необходимости нужно хранить на съемном носителе.

Протокол OpenID [4] и созданная на его основе технология управления идентификационной информацией отличается от Card Space. OpenID решает узкую задачу – данный протокол подтверждает принад-

лежность какого-либо URI (Uniform Resource Identifier) пользователю сети Интернет. Такой подход позволяет организовать идентификацию пользователя сети Интернет при помощи URL. Такого рода идентификация призвана решить проблему идентификаторов пользователей (login) и паролей, но она не решает проблему подтверждения реальной личности человека в сети Интернет.

OpenID имеет следующие достоинства:

– это уже реально работающая технология;

– технология является открытой, т.е. разрабатывается на основе Open Source лицензий;

– вся идентификационная информация хранится централизованно, нет никаких локальных хранилищ в виде файлов и т.д.;

– не требует модификации/установки клиентского программного обеспечения.

Недостатки OpenID:

– централизованное хранение идентификационной информации. Это является также и недостатком из-за вероятности потери или утечки всей информации сразу при успешно выполненной атаки злоумышленником;

– технология не обеспечивает приватности, поставщик удостоверений (Identity Provider) «знает», какие сайты посещает пользователь;

– требует модификации серверного программного обеспечения;

– подверженность «фишингу». Доступ к поставщику удостоверений осуществляется при помощи идентификатора пользователя и пароля. Это является прецедентом для подмены web-страницы ввода последних и тем самым для организации фишинг-атаки.

Предлагаемая система централизованного хранения идентификационной информации строится на основе технологии OpenID, но с необходимостью установки клиентского программного обеспечения, выполненного в виде подключаемого модуля (Plugin) к браузеру.

Подключаемый модуль позволит решить проблему «фишинга». Подключаемый модуль возьмет на себя обязанности идентификации пользователя поставщику удостоверений, т.е. будет предоставлять собственные, не web-ориентированные средства для ввода идентификатора пользователя и пароля. Подключаемый модуль также предлагается использовать в качестве менеджера паролей, но с тем условием, что идентификаторы пользователей и их пароли в зашифрованном виде будут храниться на поставщике удостоверений. Совмещение функций менеджера паролей и защищенного доступа к поставщику удостоверений позволит выполнить две задачи: во-первых, обезопасить пользователя от фишинг-атак с целью получения доступа злоумышленником к постав-

щику удостоверений, во-вторых, так как технология OpenID распространена, по масштабам сети Интернет, слабо, позволит решить проблему дублирования идентификаторов пользователей и паролей и вообще любой идентификационной информации на множестве серверов сети Интернет.

ЛИТЕРАТУРА

1. http://en.wikipedia.org/wiki/Public_key_infrastructure
2. *Kim Cameron and Michael B. Jones.* Design Rationale behind the Identity Metasystem Architecture, http://www.identityblog.com/
3. http://www.identityblog.com/?page_id=354
4. http://www.openid.net/

РАСЧЕТ ПОМЕХ (ПАРАЗИТНЫХ НАВОДОК) В ЛИНИЯХ СВЯЗИ

Р.И. Газизуллин, студент гр. 572-2;
ТУСУР, г. Томск, т. 8-923-405-79-66, gaz85@mail.ru

В электронных устройствах чаще других имеет место внешняя параллельная емкостная паразитная связь. Сопротивление $Z_{\text{вх1}}$ представлено в виде параллельно соединенных $R_{\text{вх1}}$ и $C_{\text{вх1}}$, что правомерно для большинства устройств, работающих на низких и средних частотах. Второй канал показан упрощенно, так как его параметры слабо влияют на значение наводки из второго канала в первый.

Рассмотрим расчет помехи $U_{\text{п.п.12}}$, наводимой из второго канала в первый. Напряжение сигнала во втором канале (на сопротивлении $R_{\text{вх2}}$) определяется выражением

$$U_{c2} = E_{c2} R_{\text{вх2}} / (R_{c2} + R_{\text{вх2}}).$$

Входное сопротивление первого канала связи для сигнала наводки образуется параллельным соединением следующих элементов: выходного сопротивления генератора R_{c1}, паразитной емкости линии связи C_{n11}, входного сопротивления приемника сигнала $R_{\text{вх}}$ и входной емкости приемника сигнала, т.е.

$$Z_{к1} = X_{c1} \| R_{к1},$$

где X_{c1} – импеданс паразитной емкости C_{n11};

$$C_{к1} = C_{n11} + C_{\text{вх1}} + C_{n12};\ \ R_{к1} = R_{\text{вх1}} R_{c1} / (R_{\text{вх1}} + R_{c1});$$

$R_{к1}, C_{к1}$ – входное сопротивление и собственная емкость первого канала.

При гармоническом сигнале во втором канале амплитуда помехи определяется по выражению

$$U_{\text{п.п12}} = U_{c2} T_{\text{п12}} \omega_{c2} / \sqrt{1 + T_{к1}^2 \omega_{c2}^2},$$

где $T_{к1} = R_{к1} C_{к1}$ – постоянная времени первого канала связи; $T_{\text{п12}} = R_{к1} C_{\text{п12}}$ – постоянная времени цепи паразитной связи первого канала со вторым; ω_{c2} – частота гармонического сигнала во втором канале.

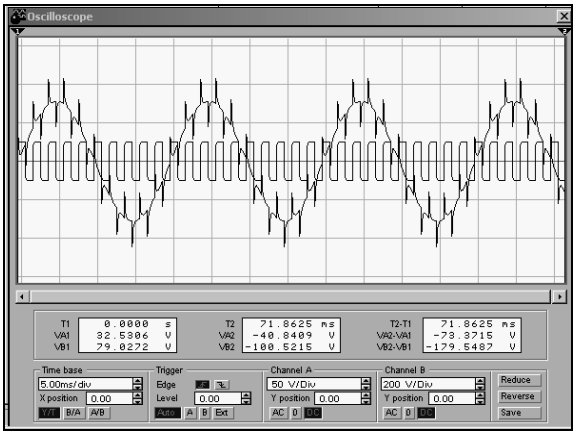


Рис. 1. Осцилограмма сигналов каналов связи

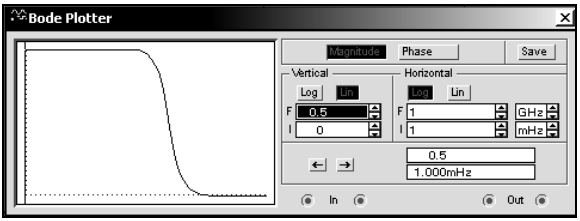


Рис. 2. АЧХ второго канала передачи информации

Рассчитаем емкость телефонной линии на один погонный метр (l = 100 см). Диэлектрическая проницаемость полихлорвинила $\varepsilon = 2{,}8$.

Расчетные размеры в приведенную ниже формулу подставляются в см. Для телефонного кабеля радиус провода r = 0,01 см, расстояние между проводниками кабеля d = 0,3 см. Емкость на погонный метр:

$$C_{\text{пог}} = \frac{1}{9 \cdot 10^{11}} \cdot \frac{l\varepsilon}{4 \ln \frac{d}{r}} = \frac{1}{9 \cdot 10^{11}} \cdot \frac{100 \cdot 2{,}8}{4 \ln \frac{0{,}3}{0{,}01}} = 2{,}29 \cdot 10^{-11} \text{ Ф/м}.$$

Для линии длиной 10 м $C_{n11} = 2{,}29 \cdot 10^{-10}$ Ф.

Определим амплитуду первой гармоники сигнала наводки в телефонную линию по формуле, полагая что по кабелю компьютерной сети передается информация в двоичном последовательном коде с частотой $f_{c2} = 1$ МГц, что соответствует угловой частоте $\omega_{c2} = 2\pi f_{c2} = 6{,}28 \cdot 10^6$ с$^{-1}$.

Исходные данные для расчета:

$R_{\text{вх1}} = 500$ Ом; $R_{c1} = 50$ Ом; $C_{n11} = 2{,}29 \cdot 10^{-10}$ Ф; $C_{n12} \approx 0{,}5 \cdot 10^{-10}$ Ф;

$E_{c2} = 5$ В; $R_{c2} = 50$ Ом; $R_{\text{вх2}} = 1000$ Ом; $C_{\text{вх1}} = 0$.

Предварительно определим эквивалентное сопротивление:

$$R_{к1} = \frac{R_{\text{вх1}} R_{c1}}{R_{\text{вх1}} + R_{c1}} = \frac{500 \cdot 50}{500 + 50} = 45{,}5 \text{ Ом};$$

$$C_{к1} = C_{n11} + C_{\text{вх1}} + C_{n12} = 2{,}29 \cdot 10^{-10} + 0{,}5 \cdot 10^{-10} = 2{,}79 \cdot 10^{-10} \text{ Ф}.$$

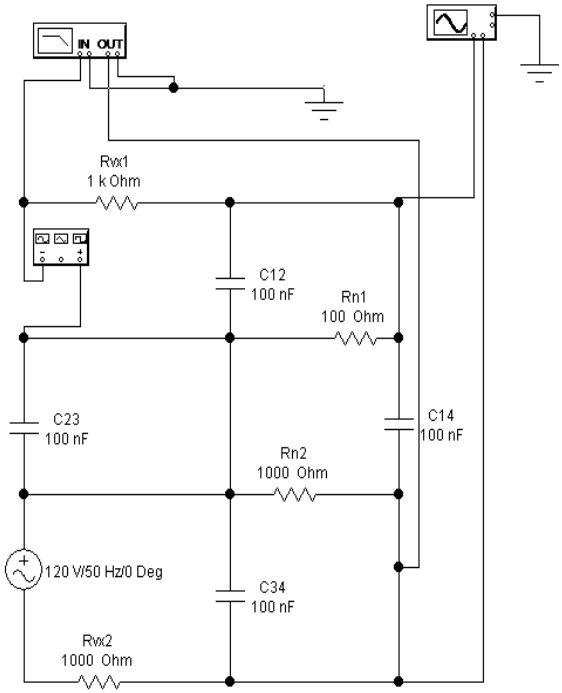


Рис. 3. Эквивалентная схема емкостной паразитной связи

Постоянная времени

$$T_{к1} = R_{к1} C_{к1} = 4{,}45 \cdot 2{,}79 \cdot 10^{-10} = 1{,}27 \cdot 10^{-8} \text{ с.}$$

Постоянная времени

$$T_{п12} = R_{к1} C_{п12} = 4{,}45 \cdot 0{,}5 \cdot 10^{-10} = 2{,}3 \cdot 10^{-9} \text{ с.}$$

Напряжение сигнала в компьютерном канале:

$$U_{с2} = E_{с2} \cdot R_{вх2} / (R_{с2} + R_{вх2}) = 5 \cdot 1000 / (50 + 1000) = 4{,}76 \text{ В.}$$

Амплитуда паразитной наводки в телефонной линии:

$$U_{nn12} = U_{с2} T_{п12} \omega_{с2} / \sqrt{1 + T_{к1}^2 \omega_{с2}^2} = \frac{4{,}76 \cdot 2{,}3 \cdot 10^{-9} \cdot 6{,}28 \cdot 10^6}{\sqrt{1 + (1{,}27 \cdot 10^{-8})^2 (6{,}28 \cdot 10^6)^2}} = 0{,}684 \, B.$$

Амплитуда паразитной наводки в телефонную линию от компьютерной сети достаточна для ее обнаружения, поэтому телефонную линию необходимо защитить от утечки наведенного в ней информационного сигнала. Параметры защитного устройства можно определить по амплитудно-частотной характеристике канала утечки информации на основании его передаточной функции.

Передаточная функция канала емкостной параллельной паразитной связи:

$$W_{n.n12}(p) = p C_{п12} R_{к1} / (p R_{к1} C_{к1} + 1) = T_{п12} p / (T_{к1} p + 1),$$

а в соответствии с передаточной функцией определяется амплитудно-частотная характеристика:

$$A_{n.n12}(\omega) = T_{п12} \omega_{с2} / \sqrt{1 + T_{к1}{}^2 \omega_{с2}^2},$$

где $\omega_{с2}$ – частота гармонического сигнала во втором канале.

Передаточная функция канала емкостной параллельной паразитной связи в числовом выражении имеет вид

$$W_{n.n12}(p) = T_{п12} p / (T_{к1} p + 1) = 2{,}3 \cdot 10^{-9} \, p \Big/ (1{,}27 \cdot 10^{-8} \, p + 1).$$

Приведем расчет методом контурных токов данной паразитной емкостной связи.

Для нахождения величины помехи нужно отыскать величину тока, который проходит через внутреннее сопротивление второго и четвертого каналов – $R_{н1.}, R_{н2}$

Для нахождения величин токов в этой схеме воспользуемся методом контурных токов, который базируется на втором законе Кирхгофа. Составляем систему:

При $E_1 = 60$ В.

$$\begin{cases} I_{11}*(R_1 - j/wC_1) + I_{22}*j/wC_2 = E_1 \\ I_{11}*(j/wC_1) - I_{22}*(jw/C_1 + R_{n1}) - I_{33}*R_{n1} = 0 \\ -I_{22}*R_{n1} + I_{33}*(j/wC_2 + R_{n1} - j/wC_3 + R_{n2}) - I_{44}*R_{n2} = 0 \\ I_{33}*R_{n2} - I_{44}*(j/wC_4 + R_2) + I_{55}*j/wC_4 = 0 \\ I_{44}*(j/wC_4) + I_{55}*(j/wC_4 + R_2) = 0 \end{cases}$$

$$\begin{cases} I_{11}*(1000 - j318) + I_{22}*(j318 - 1000) = 60 \\ I_{11}*j318 + I_{22}*(-j318 + 1000) - I_{33}*1000 = 0 \\ -I_{22}*1000 + I_{33}*(j636 + 1000 - j636 + 1000) - I_{44}*1000 = 0 \\ I_{33}*1000 - I_{44}*(j318 + 1000) + I_{55}*j318 = 0 \\ I_{44}*j318 + I_{55}*(-j318 + 1000) = 0 \end{cases}$$

При $E_2 = 60$ В.

$$\begin{cases} I_{11}*(R_1 - j/wC_1) + I_{22}*j/wC_2 = 0 \\ I_{11}*(j/wC_1) - I_{22}*(jw/C_1 + R_{n1}) - I_{33}*R_{n1} = 0 \\ -I_{22}*R_{n1} + I_{33}*(j/wC_2 + R_{n1} - j/wC_3 + R_{n2}) - I_{44}*R_{n2} = 0 \\ I_{33}*R_{n2} - I_{44}*(j/wC_4 + R_2) + I_{55}*j/wC_4 = 0 \\ I_{44}*(j/wC_4) + I_{55}*(j/wC_4 + R_2) = E_2 \end{cases}$$

$$\begin{cases} I_{11}*(1000 - j318) + I_{22}*(j318 - 1000) = 0 \\ I_{11}*j318 + I_{22}*(-j318 + 1000) - I_{33}*1000 = 0 \\ -I_{22}*1000 + I_{33}*(j636 + 1000 - j636 + 1000) - I_{44}*1000 = 0 \\ I_{33}*1000 - I_{44}*(j318 + 1000) + I_{55}*j318 = 0 \\ I_{44}*j318 + I_{55}*(-j318 + 1000) = 60 \end{cases}$$

С помощью программы Comcal находим токи I_{22} и I_{44}, они, соответственно, равны: $8{,}15 \cdot 10^{-3}$А и $8{,}51 \cdot 10^{-3}$А.

Отсюда находим напряжение помехи: $U_{п1} = I_{22}*R_{п1;}$ $U_{п2} = I_{44}*R_{п2}$; $U_{п1} = 8{,}15$В; $U_{п2} = 8{,}51$ В.

Проверка полученного результата проводилась в среде программной моделирующей системы версии EWB 5.12, расчетное и экспериментальное значения совпали.

Вывод: при наличии паразитных емкостных связей в линиях связи возможен съем информации через паразитные связи информативных каналов с неинформативными и дальнейший съем информативного сигнала.

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ БЕЗОПАСНЫХ СЕРВИСОВ ДЛЯ РАСПРЕДЕЛЕНИЯ ЗАДАНИЙ СТУДЕНТАМ

Д.В. Гаврилов, студент 1 курса; Е.Д. Головин доцент каф. КИБЭВС
Филиал ТУСУР, г.Сургут, т. (3462) 450106, rs24@yandex.ru

При выполнении студентом домашнего задания (самостоятельной, контрольной, курсовой работы) неизбежно возникают вопросы. Ответы на них не всегда можно найти в методической литературе по изучаемому предмету. Преподаватели, совершенствуя свой курс, вносят изменения и поправки в лекционный материал, задания к курсовым и практическим работам и, соответственно, к методическому обеспечению, по которому студентам приходится выполнять задания самостоятельно. Процесс обновления литературы занимает определенное время, поэтому многие преподаватели предоставляют обновленный материал в электронном виде, который обычно размещается в локально-вычислительной сети (ЛВС) университета.

Проблема заключается в том, что студенту приходится регулярно просматривать каталоги ЛВС университета для определения изменений в материале, что не всегда удобно. Эта проблема особенно существенна для студентов заочной формы обучения.

Еще одна проблема для студентов заочной формы – это консультации во время семестра. Естественно, что многие из них не могут в рабочее время посещать консультации преподавателя, а во многих случаях студенту бывает достаточно услышать простой ответ на свой вопрос.

Разработанный специально для Филиала ТУСУР в г. Сургуте вебсайт в значительной степени решает большинство озвученных проблем распределения обновленных заданий и удаленного общения преподавателя и студента. В век информационных технологий студент ТУСУР инженерной специальности, как правило, имеет дома компьютер с выходом в Интернет. Таким образом, пользователи получают доступ к информации, размещенной на сайте, а также его сервисам:

- общая информация об университете,
- раздел новостей,
- подписка на новости,
- автоматическое обновление расписания занятий,
- подписка на изменения расписания,
- задания по предметам,
- подписка на обновление заданий,
- чат,
- форум,
- фотогалерея.

Для работы с сайтом определены группы пользователей: администратор, преподаватель, студент, гость, администратор новостей, администратор обновлений. Для каждой группы администратор сайта назначает соответствующие права. Например, студент сможет просматривать свои текущие оценки по предметам [1, 2].

Для каждого преподавателя реализована возможность размещения обновления по своему предмету (новое задание, дополнение к заданию, удалить задание), которое может включать в себя текстовую информацию, файл, изображение. Система автоматически распределит задание по предметам, покажет дату обновления задания, последние обновления, вышлет информацию о добавлении нового задания на электронный адрес зарегистрированным подписчикам. Если дисциплина, которую указал преподаватель, не указана в перечне, то такое обновление проходит через администратора обновлений, который регистрирует новую дисциплину, или указывает существующую.

При просмотре обновлений в разделе «Задания по предметам», аналогично разделу «Новостей», выдаются краткие ссылки на последние обновления. Здесь же пользователь может просмотреть обновления по определенной дисциплине, выбрав соответствующее название.

На сайте предусмотрена возможность размещения сообщений об изменении каталога заданий ЛВС филиала, в котором преподаватели обычно размещают задания и методический материал.

На форуме зарегистрированный студент может задать свой вопрос, который по электронной почте одновременно поступит указанному преподавателю.

Для безопасности на сайте использованы различные функции для защиты приложений от взломов и атак. Эти функции предназначены для фильтрации входной информации от пользователей. Для защиты паролей пользователей на сайте используется тройное шифрование MD5. Также по причине безопасности на сайте не используются файлы cookies и стоит ограничение на загрузку файлов определенных форматов, таких как php, html и других исполняемых файлов.

Продуманная система размещения объявлений и заданий позволяет студентам, не выходя из дома, просмотреть любую информацию о событиях в вузе, просматривать задания по предметам, задавать вопросы и получать ответы в короткое время, несмотря на местонахождение преподавателей. Продуманные средства общения, такие как чат и форум, позволяют общаться студентам между собой, а также с преподавателями.

ЛИТЕРАТУРА

1. *Кузнецов М.В. Симдянов И.В* Самоучитель PHP5. СПб.: БХВ-Петербург, 2004. 560 с.

2. *Зольников Д.С.* PHP5. Как самостоятельно создать сайт любой сложности. М.: НТ-Пресс, 2005. 264 с.

БЕЗОПАСНОСТЬ ДАННЫХ В СУБД MS SQL-SERVER

Р.А. Хусаенов, ст. 3 курса; Н.А. Новгородова ассистент каф. КИБЭВС
ТУСУР, г.Томск, т.89234077753, rustikxxxxx@sibmail.com

MS SQL Server 2005 – это комплексное, интегрированное, законченное решение обработки данных, предоставляющее всем пользователям организации наиболее безопасную, надежную и производительную платформу для данных приложений.

Разработчики Microsoft автоматизировали многие операции SQL Server 7.0, и тому, кто только начинает работать в качестве администратора баз данных, будет полезно больше узнать о модели безопасности SQL Server.

Уровни и режимы защиты

В SQL Server предусмотрено три уровня безопасности. Во-первых, пользователи должны быть зарегистрированы в SQL Server. Разрешение на доступ к БД выдается пользователям на втором уровне защиты. На третьем уровне администратор может назначать права доступа к объектам в базе данных. Те же три уровня безопасности предусмотрены в Windows 2000 и NT, поэтому знания о системе безопасности Windows применимы и к SQL Server.

Первый режим. В SQL Server реализованы два режима аутентификации: режим безопасности NT и смешанный режим. Если выбрать режим NT и установить соответствие между процедурами пользовательской регистрации в NT и SQL Server, то пользователи, зарегистрировавшись в NT, могут установить соединение и с SQL Server. В этом режиме пользователи, не опознанные NT, не могут обращаться к SQL Server. В смешанном режиме пользователи, прошедшие регистрацию в NT, соединяются с NT и SQL Server так же, как и в режиме NT, а пользователи, не опознанные NT, могут предъявить имя и пароль для доступа к SQL Server. Альтернативный вариант – аутентификация в SQL Server. Обычно применяется режим безопасности NT, за исключением тех случаев, когда необходим смешанный режим.

Второй уровень защиты SQL Server – управление доступом к базам данных. SQL Server позволяет работать с несколькими БД на сервере, поэтому, вероятно, администратор пожелает разрешить большинству пользователей доступ к одним базам данных, но запретить обращение к другим. Учетная запись в SQL Server не дает права на доступ к БД до тех пор, пока данной учетной записи не присвоено право доступа к этой базе данных. К решению этой задачи можно подойти со стороны пользователя или со стороны базы данных. Также пользователя можно зарегистрировать в нескольких базах данных.

Третий уровень защиты – это задание полномочий. Независимо от того, назначаются полномочия базы данных пользователям или добав-

ленным ролям, выполнить задачу можно, начав с пользователя (помните, что учетная запись пользователя в SQL Server может соответствовать группе NT) или роли и назначения полномочий. Можно также начать с таблицы, представления данных или хранимой процедуры и назначить полномочия для работы с этим объектом соответствующему пользователю или пользовательским ролям базы данных.

Следующим шагом может быть создание сценария SQL Server. Данная функция строит сценарий, которым можно воспользоваться для регенерации базы данных, в том числе и политики безопасности. Предварительный запуск сценария можно осуществить в окне Query Analyzer. При необходимости можно выполнить лишь часть сценария, предназначенную для управления параметрами безопасности. С помощью сценария можно всего за несколько секунд завершить работу, выполнение которой в оснастке SQL Server Enterprise Manager заняло бы несколько часов.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС «КРИПТОГРАФИЯ»

М.В. Ильенко, М.Н. Цветков, студенты 3 курса ФВС;
С.К. Росошек, доцент каф. КИБЭВС
ТУСУР, г. Томск, marishail@rambler.ru

В процессе изучения дисциплины криптография у студентов возникает довольно большое количество проблем, связанных с усвоением материала. Особые трудности прохождение дисциплины вызывает у студентов, переведенных с дистанционной формы обучения. В помощь студентам, изучающим дисциплину криптография создается учебно-методический комплекс.

В настоящий момент для изучения криптографии студентам предоставлена программа CRYPT, содержащая большое количество ошибок и недочетов. Более того, в программе CRYPT лабораторные работы проходят в демонстрационном режиме без разбора алгоритмов шифрования и расшифрования. Целью создания учебно-методического комплекса является устранение ошибок, обнаруженных в CRYPT, а также дополнение некоторыми другими частями курса. Программа, написанная в рамках разработки учебно-методического комплекса, ориентирована на изучение дисциплины криптография студентами, ранее изучавшими дисциплину Специальные главы математики.

Изучение дисциплины разбито на 4 части:

– теоретическая часть,
– тренажеры,

– лабораторные работы,
– контрольные работы.

При этом теоретическая часть приводится для каждой лабораторной работы.

Лабораторные работы проходят в двух формах. Первая форма подразумевает детальную проработку алгоритмов шифрования на каждом шаге его выполнения. Это относится к шифрам небольшой сложности, таким как Афинный шифр, шифр Хилла, различные шифры гаммирования. Другая форма выполнения лабораторных работ подразумевает под собой демонстрационный режим ввиду своей трудоемкости. В процессе прохождения таких лабораторных работ студенту предлагается ввести небольшой текст для шифрования, а затем в виде демонстрации показывается работа данных алгоритмов. Этот режим предназначен для изучения таких трудоемких алгоритмов, как ГОСТ 28147-89.

В программе предусмотрено прохождение студентами тренажеров (по желанию). Тренажеры реализованы только для несложных алгоритмов шифрования.

В программе также реализована рейтинговая система. Рейтинговые баллы начисляются студенту по результатам прохождения им лабораторных и контрольных работ. Баллы за прохождения этих заданий начисляются единожды и затем хранятся в базе данных. После прохождения регистрации в программе студент попадает на личную страничку, на которой выведен его статус и положение согласно рейтинговой системе.

Внедрение данной системы для изучения студентами дисциплины «Криптография» позволит более наглядно и детально изучать все тонкости построения криптосистем.

ПОЛОЖЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

В.С. Казарин, студент группы 522-1.
ТУСУР, г. Томск

В процессе выполнения работы был рассмотрен административный уровень информационной безопасности предприятия, т.е. меры, предпринимаемые руководством организации. В основе всех мероприятий административного уровня лежит документ, часто называемый положением (политикой) информационной безопасности предприятия. Под положением (политикой) информационной безопасности понимается совокупность документированных управленческих решений и разрабо-

танных превентивных мер, направленных на защиту информационных ресурсов.

Разработка положения (политики) безопасности – длительный и трудоемкий процесс, требующий профессионализма, отличного знания нормативной базы в области безопасности, да и писательского таланта. Этот процесс обычно занимает многие месяцы и не всегда завершается успешно. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение информационной безопасности. Эта ответственность обычно концентрируется на руководителе отдела информационной безопасности, именно он координирует деятельность рабочей группы по разработке и внедрению положения (политики) безопасности на протяжении всего жизненного цикла.

Основной целью разработки данного положения является защита банка, его клиентов от возможного нанесения им материального, морального или другого ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования АБС или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования.

В ходе работы были рассмотрены требования, предъявляемые банком, рекомендации стандартов, Конституция, законы и иные руководящие документы, а также некоторые международные стандарты, такие как ISO 17799, BSI и другие. В результате чего был разработан документ, направленный на обеспечение безопасности информационных технологий банка и распределение функций и ответственности за обеспечение безопасности ИТ между подразделениями и среди сотрудников банка.

Разработка положения (политики) информационной безопасности – вопрос отнюдь не тривиальный. От тщательности ее проработки будет зависеть действенность всех остальных уровней обеспечения информационной безопасности – процедурного и программно-технического. Сложность разработки данного документа определяется проблематичностью использования чужого опыта, поскольку положение (политика) безопасности основывается на производственных ресурсах и функциональных зависимостях данного предприятия. Кроме того, Россия как государство не имеет подобного типового документа. Наиболее близким по идее можно назвать «Доктрину информационной безопасности РФ», однако, на мой взгляд, она носит слишком общий характер.

СОЗДАНИЕ И РЕАЛИЗАЦИЯ ШИФРА НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

А.С. Коботаев, студент 4 курса каф. КИБЭВС
ТУСУР, г. Томск, Fasta@sibmail.com

Криптография – одна из старейших наук, ее история насчитывает несколько тысяч лет. Но тем не менее криптография продолжает развиваться: разрабатываются новые алгоритмы и пишутся новые программы. Но параллельно с криптографией развивается и криптоанализ. Также бурными темпами растут вычислительные мощности компьютеров, что не лучшим образом сказывается на стойкости существующих шифров.

В данной статье описывается шифр, в основе которого лежит клеточный автомат. В процессе шифрования данным шифром используются соседние биты для каждого шифруемого бита. Таким образом получается очень большое количество зависимостей, что затрудняет применение многих видов криптоанализа.

Описываемый шифр является блочным симметричным, т.е. для зашифрования и расшифрования используется один и тот же ключ [2]. При этом данные разделяются на блоки определенного размера и обрабатываются по отдельности.

Ядро шифра – симметричный клеточный автомат. Клеточный автомат – это набор клеток, образующих некоторую периодическую решетку с заданными правилами перехода, определяющихся состояние клетки в следующий момент времени через состояние клеток, находящимися от нее на расстоянии не больше некоторого в текущий момент времени [1]. Симметричный клеточный автомат производит преобразования таким образом, что не происходит потерь информации [1, 2].

Правила перехода содержатся в ключе, который генерируется случайным образом. Правила перехода используются при зашифровке или расшифровке: если бит ключа равен 0, то бит, над которым производятся преобразования, будет инвертирован; если бит ключа равен 1, то будет произведена операция сложения по модулю 2 (XOR) со следующим битом. Предварительно шифруемый байт дополняется нулем слева и справа.

Если длина ключа больше восьми бит, то шифруемый текст разбивается на блоки, равные длине ключа и к каждому байту блока применяется поочередно байт ключа, как в примере, приведенном выше. Обязательным условием является кратность ключа восьми битам.

При расшифровке проделываются подобные операции, только в обратном порядке.

Была написана программа, выполняющая зашифровку, расшифровку и генерацию ключей способами, описанными выше. Время расшиф-

ровки равно времени зашифровки. Время шифрования зависит от двух параметров – от объема шифруемых данных и от размера ключа. Зависимость прямо пропорциональна: при увеличении/уменьшении объема данных в *n* раз, увеличивается/уменьшается время шифрования в *n* раз соответственно. Также при увеличении/уменьшении длины ключа в *n* раз время шифрования увеличивается/уменьшается в *n* раз соответственно.

На практике программа тестировалась на машине с процессором AthlonXP 2500. Время шифрования файла объемом 105 Мб при размере ключа 128 бит составило 27 сек (~3,8 Мб/с).

В дальнейшем планируется повысить производительность программы за счет оптимизации узких мест и добавления многопоточности.

ЛИТЕРАТУРА

1. *Тоффоли Т., Марголус Н.* «Машина клеточных автоматов». М.: Мир. 1991.

2. *Википедия:* http://ru.wikipedia.org/wiki

ФОРМИРОВАНИЕ СИГНАЛОВ ЗАКЛАДОЧНЫХ УСТРОЙСТВ С ПОМОЩЬЮ ПАК «АВРОРА» И ИХ ПОИСК

Н.А. Кокорева, студентка группы 522-1;

ТУСУР, г. Томск

В наши дни наука и технологии развиваются такими темпами, что уровень профессиональной подготовки специалистов по поиску закладочных устройств все заметнее отстает от требований времени.

Арсенал закладочных устройств стремительно пополняется новыми высокотехнологичными изделиями с высокой скрытностью работы от традиционных средств обнаружения сигналов. В закладочных устройствах все чаще применяются различные способы накопления информации, позволяющие резко сократить время ее передачи или отложить передачу на другое, более удобное время. В этих устройствах все шире используются разнообразные методы закрытия информации, шумоподобные широкополосные сигналы, специальные алгоритмы скачкообразной перестройки несущей частоты и другие приемы.

Все это предъявляет особые требования к поисковой аппаратуре, требует наличия у операторов навыков обнаружения и идентификации любых сигналов современных закладочных устройств.

Специалистами ЗАО НПЦ Фирмы «НЕЛК» был разработан принципиально новый, не имеющий аналогов имитатор радиосигналов – аппаратно-программный комплекс Аврора.

Обучающий тренажерный комплекс по подготовке специалистов в области поиска и обнаружения радиозакладочных устройств Аврора-Т предназначен для формирования и излучения в эфир радиосигналов, имитирующих работу различных радиопередающих устройств.

Принцип работы комплекса заключается в излучении передатчиком радиосигнала с заданными оператором параметрами несущей частоты, мощности, видами модуляции и модулирующего сигнала.

Для проведения учебного процесса с применением тренажера необходимо было сформировать различные сигналы закладочных устройств и отработать методы идентификации этих сигналов с помощью комплекса RS turbo Mobile-L и анализатора спектра Rohde & Schwarz FS300.

С помощью специального программного обеспечения были сформированы следующие модели сигналов:

– частотно-модулированный сигнал с частотой несущей 750МГц;

– частотно-модулированный сигнал с равномерной перестройкой частоты от 1 до 1,5 ГГц с шагом 50 МГц;

– частотно-модулированный сигнал с неравномерной перестройкой частоты от 1 до 1,5 ГГц;

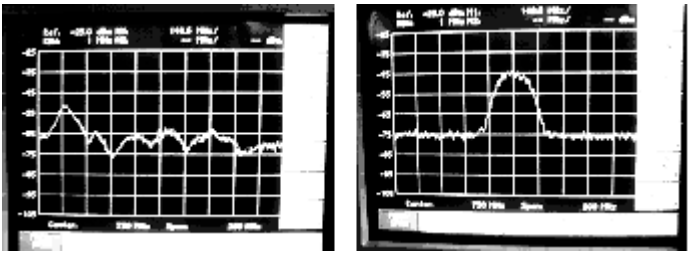
– шумоподобный сигнал с фиксированной частотой несущей 750 МГц;

– шумоподобный сигнал;

– сигнал со сверхкороткой передачей информации.

Результаты обнаружения радиозакладочных устройств различными комплексами радиомониторинга показаны на рисунке.

RS turbo Mobile-L удобен в обнаружении сигналов с простыми характеристиками и позволяет локализовать источник излучения частотно-модулирующего сигнала с микрофоном. Так как комплекс сканирует диапазоны только в определенные моменты времени, то обнаружить сигнал с перестройкой частоты, особенно неравномерной весьма трудоемко.



а *б*

Рис. 3. Обнаружение шумоподобного сигнала с фиксированной частотой с помощью анализатора спектра: *а* – включен генератор шума; *б* – включен ШП-сигнал

Анализатор спектра функционирует в режиме реального времени, поэтому его можно использовать при обнаружении закладок с равномерной и неравномерной перестройкой частоты. Также он идеально подходит для обнаружения простых сигналов.

Как видно из рис. 2 и 3, можно отличить сигнал типа «белый шум» постороннего генератора шума от шумоподобного сигнала, имитатора с фиксированной частотой несущей.

Обнаружения закладок со сверхкороткой передачей информации, шумоподобных сигналов с нефиксированной частотой несущей не увенчались успехом. Выяснилось, что ни одно из имеющихся на кафедре поисковых средств не способно обнаруживать сигналы такого типа.

Если не знать, как должен выглядеть в эфире сигнал, а тем более не знать, что конкретно надо искать в эфире, то невозможно распознать даже обычную шумоподобную закладку с фиксированной частотой. Таким образом, даже при наличии у специалистов нескольких образцов закладочных устройств вряд ли справедливо требовать от них умения быстро распознавать сигналы закладочных устройств, обладающих другими, отличными от имеющихся образцов характеристиками.

СПЕЦИССЛЕДОВАНИЕ МОНИТОРА НА ПОБОЧНЫЕ ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ

Н.А. Кокорева, студентка гр. 522-1; А.В. Грасмик, ст. гр. 523-3
ТУСУР, г. Томск

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. Характер ПЭМИ определяется назначением, схемными решениями, элементной базой, мощностью устройства, его конструкцией, а также материалами, из которых изготовлен корпус. Излучение может происходить в широком диапазоне частот (от единиц герц до единиц и даже десятков гигагерц), а дальность реального перехвата информации может достигать сотен метров.

Необходимо провести исследование на побочные электромагнитные излучения. Объектом исследования стал монитор на электронно-лучевой трубке с разрешением экрана 640×480 точек ViewSonic E50. Электромагнитные поля, возникающие около проводников, по которым видеосигнал подается на кинескоп монитора, – это и есть побочные

электромагнитные излучения. И часто перехватить их можно при помощи обычного телевизионного приемника, размещенного на расстоянии нескольких метров от монитора персонального компьютера. Четкость изображения при этом может быть достаточной для чтения текста.

Исследования проводились с помощью программно-аппаратного комплекса «Легенда», предназначенного для поиска и измерения в автоматическом и полуавтоматическом режимах побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых исследуемыми техническими средствами электронно-вычислительной техники, автоматизированного расчета опасных зон R1 и R2 и контроля защищенности объектов ЭВТ.

Согласно действующим нормативно-методическим документам при проведении специальных исследований требуется измерять информативные ПЭМИ, т.е. такие излучения, создаваемые исследуемым техническим средством, которые содержат обрабатываемую данным техническим средством информацию. Такие излучения составляют лишь малую долю от всего спектра излучений технического средства. Все прочие излучения не должны фиксироваться при измерениях. Для того чтобы выделить информационные ПЭМИ на исследуемом техническом средстве, предусматривают специальные тестовые режимы его работы. В нашем случае использовался тест «Зебра», который обеспечивал вывод на экран определенного числа белых и черных горизонтальных полос, содержащих одинаковое число строк развертки монитора.

В соответствии с методикой проведения специальных исследований технических средств по измерению их собственного электромагнитного излучения проводились следующие операции.

1. На контролируемом устройстве (монитор) включался тестовый режим.

2. На определенном расстоянии от устройства устанавливалась антенна для приема электрической составляющей поля, изучаемого анализируемым устройством.

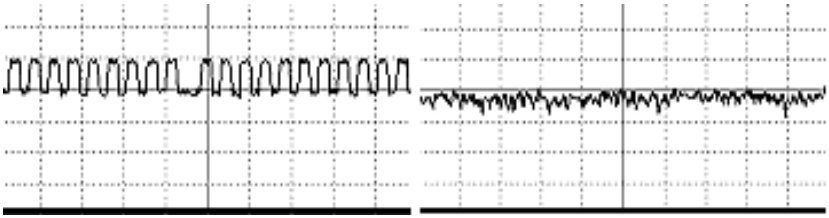
3. Электрический сигнал с выхода антенны подавался на вход приемно-регистрирующего измерительного устройства (анализатор спектра), с помощью которого по результатам измерений по определенной методике производился расчет контролируемой зоны.

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.

Результаты исследования. В полуавтоматическом режиме управляющей программы, используя энергетический принцип, нашли на частоте 20,007 МГц тестовый сигнал (рисунок).



а *б*

Осциллограмма сигнала на частоте 20,007 МГц: *а* – тест монитора включен; *б* – тест монитора выключен

Структура сигнала практически полностью передает информацию о том, что отображает монитор в данный момент времени.

В качестве эталона тестового сигнала был выбран сигнал на частоте 20,007 МГц.

При поиске гармонических составляющих тестового сигнала вручную проверялся каждый пик трека спектра.

На частотах 60, 100, 140, 180, 220, 260, 300, 340, 380, 420, 460, 500, 540, 580, 620, 660, 700 МГц был обнаружен тестовый сигнал.

Далее работа проводилась в автоматическом режиме. Перед проведением поиска составляющих по информационному критерию, то есть по сходству демодулированного на данной частоте сигнала с эталоном, необходимо было произвести предварительный контроль электромагнитной обстановки при выключенном тесте на исследуемом техническом средстве.

Для предварительного контроля электромагнитной обстановки была составлена программа исследования, в которой указывался вид исследования, диапазон исследования, вид составляющей электромагнитного поля, используемая антенна и параметры прибора (полоса обзора, полоса пропускания, детектор, количество усреднений).

Для поиска составляющих тестового сигнала также следовало заполнить программу исследований. После заполнения программы исследования был загружен эталон и рассчитано значение порогового коэффициента корреляции.

По завершении автоматического поиска и измерения ПЭМИН была проконтролирована правильность обнаружения.

Полученные данные были переданы в расчетную программу, по завершению работы которой были получены результаты, представленные в таблице.

Расчетная программа предназначена для выполнения автоматизированного расчета минимально допустимых расстояний от элементов технических средств до границы контролируемой зоны (зон R2), до сосредоточенных случайных антенн (зон r1), рассредоточенных случайных антенн (зон r1') по 1, 2 и 3-й категориям.

Зоны разведдоступности

Категория	R2, м	r1, м	r1′,м
Первая	18,1	1,4	0,6
Вторая	2,9	1,4	0,6
Третья	2,9	1,4	0,6

Из таблицы следует, что для обеспечения безопасности информации требуется контролировать зоны до 18,1 м от исследуемого средства.

ЗАЩИТА ИНФОРМАЦИИ ОТ ВНУТРЕННИХ УГРОЗ

С.И. Коковин, гр. 552-1

ТУСУР, г. Томск, т. 9095401727, ksi@ms.tusur.ru

В нашей стране к вопросам информационной защиты наиболее серьезно подходят компании, имеющие отношение к информационным технологиям, к банковскому сектору, сотовой связи: компании, проводящие операции с ценными бумагами. Что касается других организаций, согласно результатам различных исследований руководители многих из них знают об основных видах угроз, но не уделяют должного внимания этим вопросам, полагая, что обеспечение информационной безопасности не имеет смысла, если отсутствует видимая угроза. Тем не менее, постепенно руководители российских компаний изменяют свой взгляд на информационную безопасность, начиная относиться к ней как к одному из способов повышения конкурентоспособности компании. Как правило, сначала они осознают необходимость защиты от внешних атак, а позже, по мере изучения проблемы, – от атак внутренних [1].

Внешние атаки могут быть разными по принципам действия, по используемым каналам, однако все их объединяет тот факт, что воздействие происходит из-за пределов информационной среды предприятия. Но

замыкаться на внешних угрозах, недооценивая серьезность внутренних угроз, было бы ошибкой, так как значительно больший ущерб компании может нанести некорректное поведение сотрудников, нарушающих корпоративную политику безопасности. В отличие от внешних злоумышленников внутренний нарушитель – это авторизованный пользователь, имеющий официальный доступ к ресурсам интрасети, в том числе к тем, в которых циркулирует конфиденциальная информация. На самом деле, представление о том, что безопасность можно обеспечить защитой периметра сети от внешних атак, уже давно не является полным. Необходимо вырабатывать комплексную стратегию, обеспечивающую безопасность как от внешних, так и от внутренних угроз.

Владение информацией о противнике – один из наиболее действенных способов конкурентной борьбы на рынке. Необходимость решения проблемы утечки конфиденциальной информации связана с выживанием и успешным ведением бизнеса компании.

Ущерб от раскрытия конфиденциальной информации может выражаться в потере конкурентных преимуществ, упущенной коммерческой выгоде, санкциях со стороны регулирующих органов, административной и уголовной ответственности за раскрытие персональных данных, ухудшении морального климата в коллективе вследствие раскрытия информации о заработной плате работников, планируемых кадровых перестановках и т. п.

Количество потенциальных способов утечки информации достаточно велико. Наиболее распространенные из них относятся к категории неумышленного раскрытия информации сотрудниками по причине неосведомленности или недисциплинированности. Отсутствие представлений о правилах работы с конфиденциальными документами, неумение определить, какие документы являются конфиденциальными, и просто обычные разговоры между сотрудниками – все это может привести к рассекречиванию данных [2].

Умышленное разглашение информации встречается значительно реже, зато осуществляется целенаправленно и с наиболее опасными последствиями для организации.

С учетом множественности категорий и способов утечки информации становится очевидно, что в большинстве случаев проблему утечки нельзя решить каким-либо простым способом, тем более избавиться от нее окончательно. Кроме того, реализация любых мер по ограничению доступа к информации или ее распространению потенциально снижает эффективность основных бизнес-процессов организации. Это означает, что требуется система организационно-технических мероприятий, позволяющих перекрыть основные каналы утечки информации с опреде-

ленной степенью надежности и минимизировать существующие риски без значительного снижения эффективности бизнес-процессов. Без такой системы права на юридическую защиту интересов организации как собственника информации нереализуемы.

В основе системы защиты информации лежат внутренние нормативные документы, устанавливающие ответственность и определяющие правила по защите информации, обязательные для исполнения всеми сотрудниками организации. К ним относятся положение о коммерческой тайне, руководство по защите конфиденциальной информации; правила работы пользователей в корпоративной сети, инструкции по использованию сервисов безопасности, регламент предоставления доступа к информационным ресурсам [3].

Система предотвращения утечки конфиденциальной информации включает в себя три основных составляющих – работу с персоналом, политику безопасности, сервисы безопасности.

Основным источником утечки информации из организации является ее персонал. Человеческий фактор способен «свести на нет» любые самые изощренные механизмы безопасности. Неудивительно, что работа с персоналом – главный механизм защиты.

В организации должен быть разработан соответствующий дисциплинарный процесс, проводимый в отношении нарушителей безопасности и предусматривающий расследование, ликвидацию последствий инцидентов и адекватные меры воздействия.

В организации должно быть разработано положение по защите конфиденциальной информации и соответствующие инструкции. Эти документы должны определять правила и критерии для категорирования информационных ресурсов по степени конфиденциальности, правила маркирования конфиденциальных документов и правила обращения с конфиденциальной информацией, включая режимы хранения, способы обращения, ограничения по использованию и передаче третьей стороне и между подразделениями организации.

Должны быть определены правила предоставления доступа к информационным ресурсам, внедрены соответствующие процедуры и механизмы контроля, в том числе авторизация и аудит доступа.

Многие правила политики безопасности должны быть понятны сотрудникам и выполняются ими в большинстве случаев на интуитивном уровне. Остальные требуют обучения.

Таким образом, на сегодняшний день, несмотря на то, что несанкционированное раскрытие информации является во многих случаях административно и уголовно наказуемым деянием, в условиях, когда информационное законодательство РФ еще полностью не сформировано, а

процессы законотворчества сильно отстают от уровня развития информационных технологий, возникают существенные трудности в обеспечении юридической защиты интересов собственников конфиденциальной информации.

ЛИТЕРАТУРА

1. *Патий Е.* Мой офис – моя крепость. IT-News, 2006.

2. *Доля А.* Программные решения для выявления и предотвращения утечек конфиденциальных данных // Экспресс Электроника. 2006.

3. *Фисенко Л.* Системы защиты: фокус на комплексные решения // Экспресс Электроника. 2005. № 6.

ВЫДЕЛЕНИЕ КЛЮЧЕВЫХ ПАРАМЕТРОВ РЕЧЕВОГО СИГНАЛА ПРИ ПОМОЩИ НЕЙРОННОЙ СЕТИ

Е.Ю. Костюченко, аспирант каф. КИБЭВС, ТУСУР

г. Томск, e-mail: key@keva.tusur.ru

Проблема выделения ключевых параметров речевого сигнала до сих пор остается актуальной. Несмотря на значительные успехи в этом направлении исследований, остается нерешенным целый ряд задач:

– определение с набором необходимых и достаточндых для решения задач анализа речи (распознавание речи и идентификация диктора) ключевых признаков;

– ранжировка этих признаков по информативности в зависимости от класса решаемых задач;

– ускорение процесса обработки речевого сигнала: в настоящее время процесс анализа сигнала занимает длятельное время, тогда как для некоторых задач (анализ телефонных переговоров для выявления злоумышленника, идентификация пользователя по голосу) необходимо, чтобы анализ проводился в режиме, максимально приближенном к режиму реального времени.

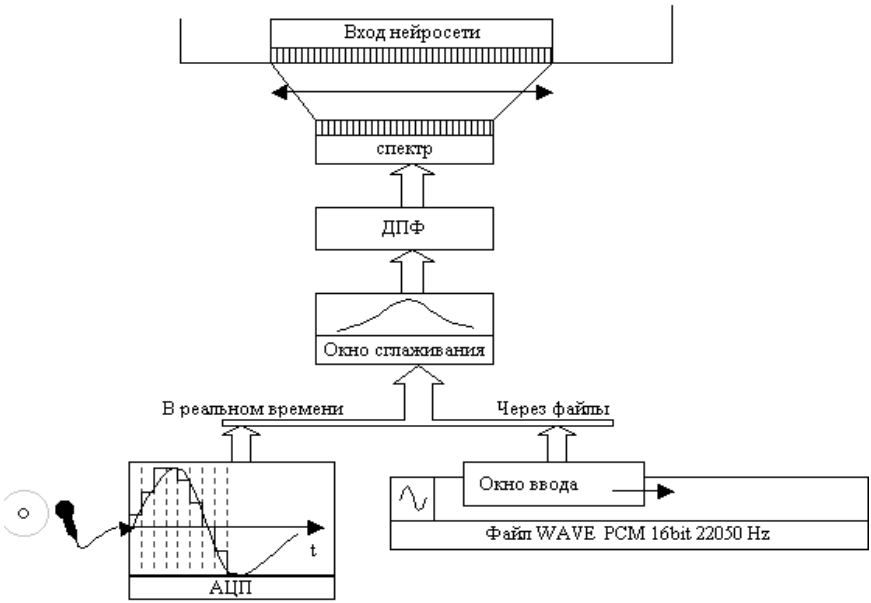
Существует несколько подходов к решению указанных проблем, один из которых базируется на использовании нейронных сетей. В данном направлении можно выделить, например, работу [1]. В ней предлагается следующий алгоритм обработки речевого сигнала, рисунок.

Здесь окно сглаживания – окно сглаживания Хэмминга:

$$\text{newData}[i] = \text{Data}[i]\left(0{,}54 - 0{,}46\cos\frac{2\Pi i}{N-1}\right), \qquad (1)$$

N – размер окна ДПФ.

ДПФ – дискретное преобразование Фурье, в качестве спектра используется энергетический спектр, информация о фазе сигнала отбрасывается.



Обработка речевого сигнала перед подачей его на входы нейронной сети

Утверждается, что для получения формантной структуры достаточно 50–100 входов нейронной сети. Применение нейронной сети позволяет значительно ускорить процесс выделений частот формант, поскольку обработка в нейронных сетях ведется быстро, основные усилия и время затрачиваются на обучение нейронной сети, однако не найдено сведений о дальнейшем развитии данной работы и ее применении. В настоящее время ведутся исследования, направленные на анализ приведенных результатов и возможности указанного подхода для выделения других параметров речевого сигнала.

Кроме того, ведутся исследования по сжатию речевого сигнала при помощи нейронной сети и оценке возможности использования получаемых параметров сжатого речевого сигнала в качестве параметров для анализа речевого сигнала.

ЛИТЕРАТУРА

1. *Москаленко А.М.* Использование нейросетей для автоматического распознавания и синтеза речи. http://alexmoshp.chat.ru/sas/sas.htm

РЕАЛИЗАЦИЯ ГРАФИЧЕСКОГО ПАРОЛЯ

С.О. Козьмин, студент 5 курса каф. КИБЭВС
Н.А. Новгородова, ассистент каф. КИБЭВС
ТУСУР, г. Томск, e-mail: serkozik@pochta.ru

Идентификацией субъекта при доступе к информационной системе называется процесс сопоставления его с некоторой хранимой системой характеристикой субъекта – идентификатором. Аутентификацией субъекта называется процедура верификации принадлежности идентификатора субъекту. Аутентификация производится на основании того или иного секретного элемента (аутентификатора), которым располагают как субъект, так и информационная система. Основными методами аутентификации являются парольная аутентификация, аутентификация на основе уникального предмета, аутентификация на основе биометрических данных. Аутентификация на основе графики имеет две основных модели – во-первых, на основе одной картинки со множеством деталей и, во-вторых, на основе нескольких мелких картинок (пиктограмм) [1–4].

Разрабатываемая система представляет собой клиент-серверную модель. В клиентской части представлен набор пиктограмм, на основе которых формируется пароль пользователя, причем расположение картинок на форме генерируется случайным образом. На сервере хранится база данных учетных записей. Для обеспечения подлинности данных в картинки внедряются цифровые водяные знаки. Конечный программный продукт находится в трее и при обращении к программам пакета Microsoft Office (Ms Word, Ms Access, Ms Excel) активизируется, запрашивая авторизацию.

ЛИТЕРАТУРА

1. *Анин Б.* Защита компьютерной информации. БХВ-Петербург, 2002. 386 с.
2. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. Наука и техника, 2004. 384 с.
3. *Щербаков Д.В.* Компьютерная безопасность. Введение в теорию и практику. НОЛИДЖ. 2003. 352 с.
4. http://cominfo.md/ – портал информационных технологий.

БЕЗОПАСНОСТЬ БЕЗНАЛИЧНОГО РАСЧЕТА

К.Б. Красников, студент 5 курса; Г.А. Праскурин, ассистент
ТУСУР, г. Томск, Constantine@ultranet.tomsk.ru

Стремительное развитие научно-технического прогресса за последние пятьдесят лет не могло не сказаться на развитии банковских технологий, несмотря на консерватизм этой сферы общественной жизни.

Применение компьютеров позволило не только значительно сократить трудовые затраты при совершении банковских операций, унифицировать бухгалтерский учет, ускорить взаиморасчеты, но и дало возможность широкого внедрения принципиально новых банковских продуктов. К числу таких продуктов, несомненно, относится и осуществление взаиморасчетов посредством пластиковых карт [1–4].

Защита от несанкционированных операций является первостепенной задачей любой системы. Очевидно, что безопасность той или иной системы это вещь комплексная и многоуровневая и зависит от взаимодействия всех механизмов защиты, используемых в мистеме [5–10]. Достоверность информации и финансовая подкрепленность платежей обеспечиваются такими эффективными механизмами, как:

1) аппаратные возможности карты: использование микропроцессорных карт превращает возможность их подделки в чисто теоретическую;

2) проверка принадлежности карты предъявителю;

3) проверка действительности карты и ее принадлежности к системе;

4) проверка по «черному списку», т.е. списку карт, запрещенных к приему. Этот механизм защиты позволяет надежно обезопасить систему от украденных и потерянных карт, а также от карт банков, выбывших из системы;

5) проверка по набору лимитов расходования;

6) on-line авторизация внелимитных операций;

7) страхование финансовых рисков участников системы.

Комплексное применение всех перечисленных механизмов безопасности позволяет с высокой степенью надежности гарантировать защищенность системы от проведения в ней несанкционированных операций.

ЛИТЕРАТУРА

1. *Гайкович Ю.В, Першин А.С.* Безопасность электронных банковских систем. М.: Единая Европа.

2. *Крысин В.А.* Безопасность предпринимательской деятельности. М.: Финансы и статистика.

3. *Титоренко Г.А. и др.* Компьютеризация банковской деятельности. М.: Финстатинформ.

4. *Аглицкий И.* Состояние и перспективы информационного обеспечения российских банков. Банковские технологии.

5. *Завалев В.* Пластиковая карточка как платежный инструмент. Центр информационных технологий.

6. *Славников Д.В.* Пластиковую карточку – каждому интернетчику (и не только…) // Компьютерная газета. 2000. №16.

7. *Чуясов В.* Деньги – Интернет – деньги // Человек & Internet №13. 2001.

8. *Шастель В.* Будущее за карточками с микропроцессором // Банковский вестник. 1999. №22.

9. *Куранов А.И.* Интеллектуальные карты – новые методы обеспечения информационной безопасности.
10. *Материалы* агентства «Интерфакс». 1995–1999.

БЫСТРЫЕ АЛГОРИТМЫ ГЕНЕРАЦИИ ПСЕВДОПРОСТЫХ ЧИСЕЛ, РЕАЛИЗОВАННЫЕ В BORLAND C++ 3.1

И.А. Кукало, 2-й курс РТФ (РЗИ); Р.В. Литвинов, к.ф.-м.н., доцент
ТУСУР, г. Томск, т. 413-884, litvinovrv@rzi.tusur.ru

При создании ключей в современных ассиметричных криптосистемах используются большие простые числа, разрядность (биты) которых может достигать нескольких сотен или даже тысяч. Арифметичес-кие операции с такими числами на обычных ПК требуют создания специального программного обеспечения [1], в том числе и реализации быстрых алгоритмов генерации простых чисел [2]. Огромная разрядность этих чисел, диктуемая современными требованиями безопасности, делает детерминированные алгоритмы малоэффективными. В настоящее время для этой цели используются методы генерации чисел, простоту которых можно обеспечить с вероятностью не менее $1–2^{-128}$.

В настоящем сообщении представлены результаты исследования быстродействия алгоритмов генерации простых чисел методами малой теоремы Ферма, Рабина – Миллера и Соловея – Штрассена, использующими фильтр деления на малые простые числа. Все три алгоритма имеют одинаковую теоретическую оценку сложности вычислений [3]:

$$N = \mathrm{O}\left(\log^3 n\right) = \mathrm{O}\left(k^3\right), \qquad (1)$$

где n – k-разрядное число.

Перечисленные выше алгоритмы были реализованы в виде специальных программ, написанных на языке Borland C++ 3.1 с использованием подключаемых модулей для элементарных арифметических операций с большими числами [1]. В телепрограмме был организован счетчик времени ее работы. Время генерации псевдопростого числа являлось выходным параметром программы, как число и количество занимаемых им бит. Программа реализующая какой-либо из описанных выше методов запускалась не менее 25 раз на ПК со следующими параметрами: Toshiba Satellite L100–194 15"XGA CM–1700 / 256 Мб DDRII / 40 Гб / DVD–RW / WiFi / WXPh. Время генерации усреднялось по всем полученным реализациям.

Результаты работы программ представлены на рис. 1. в виде зависимостей времени генерации от числа бит. Их особенностью является флуктуирующий характер. Амплитуда флуктуаций уменьшается с рос-

том числа реализаций, используемых при получении усредненной зависимости (на единичных реализациях амплитуда флуктуаций на порядок выше). Наличие флуктуаций обусловлено вероятностным характером реализованных алгоритмов генерации простых чисел (рисунок).

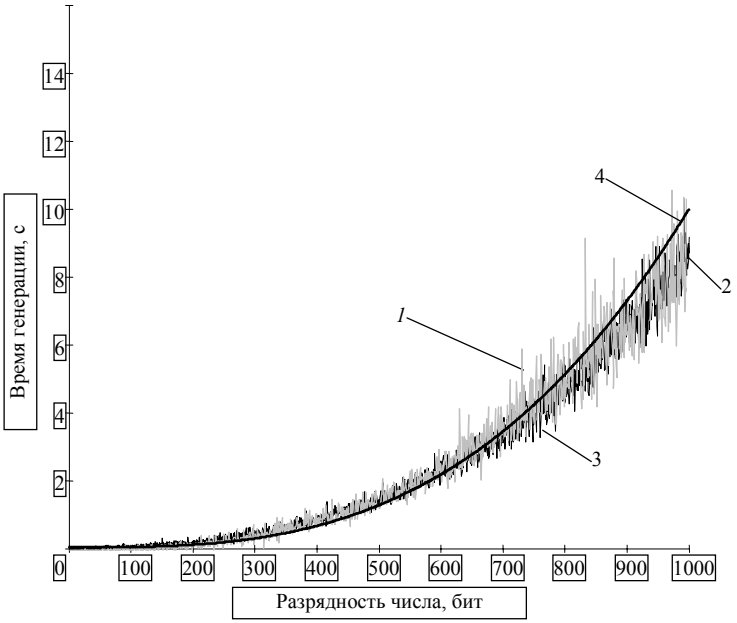


Рис. 1. Зависимость времени генерации простого числа от его разрядов методом на Миллера – Рабина (*1*), малой теоремы Ферма (*2*); Соловэя – Штрассена (*3*). Кривая *4* соответствует теоретической оценке сложности вычислений

Кривая *4* на рисунке описывается зависимостью $N = 10^{-8} k^3$ и соответствует теоретической оценке с ограничивающей постоянной $C = 10^{-8}$ для данного ПК. Из сравнения этой кривой с кривыми *1–3* видно, что реализованные программы генерации простых чисел с числом разрядов, превышающим 800 бит, работают чуть быстрее, чем предсказывает теоретическая оценка.

Таким образом, в работе представлены результаты работы алгоритмы генерации больших простых чисел на основе методов пробного деления, Миллера – Рабина, малой теоремы Ферма, Соловэя–Штрассена, непосредственно пригодные для программной реализации в среде Borland C++3.1. Выполнены численные расчеты скорости генерации от числа разрядов. Определена нижняя граница числа разрядов, начиная с

которой разработанные программы работают быстрее, чем предсказывает теоретическая оценка сложности вычислений.

ЛИТЕРАТУРА

1. *Вельшенбах М.* Криптография на Си и С++ в действии. М.: Триумф, 2004. 464 с.

2. *Смарт Н.* Криптография. М.: Техносфера, 2005. 528 с.

3. *Черемушкин А.В.* Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. 104 с.

МЕТОДИКА ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ ДЛЯ ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ

А.С. Лысов, аспирант

ТюмГУ, г. Тюмень, т. +73452251255, alllys@gmail.com

В нашей стране задача перехода от бумажного делопроизводства к электронному рассматривается достаточно давно, уже разработан ряд стандартов по работе с электронными версиями документов: в банковском деле, обсуждается стандарт оформления документов в медицинских организациях. Но из-за невозможности во всех случаях обеспечить защищенность работы с электронными документами еще не во всех областях деятельности приняты отраслевые стандарты работы с электронными документами. Еще одним фактором, тормозящим переход от бумажных версий документов к электронным, является отсутствие надежного механизма оценки гарантированного уровня защищенности для электронных документов. Для решения данной проблемы можно использовать уже широко используемый в бизнес организациях метод – анализ информационных рисков. С помощью анализа информационных рисков можно оценить уровень защищенности используемых информационных технологий и дать еще одно математически обоснованное доказательство надежности систем электронного документооборота.

В данной работе рассматривается разработанная для государственных учреждений методика анализа информационных рисков. Методика анализа рисков строилась с ориентацией на государственные структуры, поэтому мы постарались автоматизировать большинство процессов, уменьшить сложность методики, перейдя на язык отечественных специалистов по защите информации (далее экспертов) и избежать запроса малоформализованных данных у экспертов. Для разработки методики был выбран стандарт BSI, а не ГОСТ Р ИСО/МЭК 15408 по причине того, что BSI является единственным открытым стандартом в области информационной безопасности, затрагивающим очень широкий спектр

вопросов технической защиты информации. Он может быть применим в первую очередь для оценки программно-технической стороны защиты.

Приведем основные этапы методики:

Нулевой этап (вводный). На данном этапе эксперт должен заполнить данные о себе, чтобы сформировать степень доверия к данному эксперту.

Первый этап (ввод данных об инфраструктуре). Выбираем, какие информационные системы присутствуют в инфраструктуре организации. На данном этапе необходимо ввести все информационные ресурсы организации, подлежащие учету, и службы, их использующие.

Второй этап (ввод данных об уже реализованных службах безопасности). Здесь для каждого ресурса и процесса мы должны выбрать набор средств, которыми уже обеспечена информационная безопасность.

Третий этап (оценка параметров угроз экспертами). Для всех ресурсов и процессов, заданных на первом этапе, мы оцениваем вероятность и ущерб от реализации угрозы.

Четвертый этап (генерация рекомендаций). На данном этапе подсчитываются и определяются результаты оценки угроз.

На момент написания тезисов методика анализа информационных рисков проходила внедрение в одном из государственных учреждений, поэтому о результатах работы говорить еще рано. Но в целом автор данной работы согласен с мнением [1], что использование технологий анализа рисков позволит обеспечить надежную оценку уровня безопасности используемых информационных технологий.

ЛИТЕРАТУРА

1. *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК Пресс, 2004. 384 с.

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ ДЛЯ ЗАЩИТЫ ТРАНСПОРТНОЙ ПОДСИСТЕМЫ

П.А. Мельниченко, аспирант каф. КИБЭВС, ТУСУР
г. Томск, mpa@udcs.ru

Виртуальная частная сеть (VPN, Virtual Private Network) использует в качестве среды для передачи данных существующую коммуникационную инфраструктуру, например, сеть Интернет. Вопросы безопасности обеспечиваются путем шифрования передаваемых данных и использования ряда механизмов противодействия несанкционированному доступу [1, 2].

Сущность виртуальных частных сетей заключается в использовании публичной телекоммуникационной инфраструктуры для обеспечения безопасного доступа удаленных филиалов и пользователей к основной сети организации (Remote Access VPN) или для объединения географически удаленных локальных сетей (LAN-to-LAN VPN).

Наиболее универсальным способом построения VPN является использование технологии туннелирования, или инкапсуляции. Эта технология позволяет передавать пакеты одной сети (первичной) по каналам связи другой (вторичной). Для этого пакет первичной сети (данные и протоколы) инкапсулируется в пакет вторичной сети и становится виден как данные. Вообще говоря, инкапсуляция не предусматривает кодирования. Если для повышения уровня безопасности оно необходимо, то должно выполняться средствами частной сети до процедуры инкапсуляции.

Туннель можно представить как сквозной виртуальный канал, имеющий начальную точку (инициатор туннеля) и одну или более конечных (терминаторов туннеля). Этими точками могут быть компьютер удаленного пользователя, работающий как VPN-клиент, маршрутизатор, шлюз или сервер доступа к сети (Network Access Server – NAS). На обоих концах необходимо установить аппаратное и программное обеспечение (включая шифрование/дешифрование, если оно присутствует), работающее в соответствии с теми протоколами, посредством которых был образован туннель. Хотя термин «туннель» ассоциируется с фиксированным путем, на самом деле для сетей с коммутацией пакетов (Internet в частности) это не так. Зашифрованные и инкапсулированные пакеты могут использовать различные маршруты между конечными точками. Основное назначение туннеля – обеспечить конфиденциальность сессии. Это значит, что никто, кроме получателя, не расшифрует (в идеале) пакет, и чужие пакеты не могут попасть в туннель, поскольку маршрутная информация для VPN хранится отдельно от общей.

Традиционно VPN (туннелирование и/или шифрование) организуют на нижних уровнях коммуникационного стека протоколов – канальном (Layer 2) и сетевом (Layer 3).

Так как реализация VPN позволяет использовать шифрование передаваемой информации на низком уровне, то это позволяет использовать данное решение в качестве основы защиты системы транспорта.

Например, при использовании почтового сервера, подключения к которому разрешены только из внутренней сети организации, и VPN-сервера, соединение с которым участников документооборота позволяет быть внутри данной сети, полностью «скрывает» содержание обмена информацией между участниками информационного обмена.

Но проблема состоит в том, что использование стандартных средств построение VPN не дает требуемого уровня защиты передаваемых данных. Известный специалист по криптографии Брюс Шнейер (Bruce Shneier) и член команды «LOPHT» Петер Мудж (Peter Mudge) проанализировали реализацию корпорацией Microsoft протокола PPTP. Обзор технических особенностей найденных свойств опубликовал AlephOne в Phrack Magazine (http://www.phrack.com). AlephOne явно показал незащищенность PPTP и предложил методы обмана сервера PPTP для извлечения сведений об аутентификации [3, 4].

Альтернативные средства построения VPN, такие как «ViPNet» от компании «Инфотекс», требуют больших материальных и кадровых затрат на проектирование, развертывание, распространение и внедрение.

ЛИТЕРАТУРА

1. http://www.hostinfo.ru/dictionary/index.php – Виртуальные частные сети.

2. http://www.itc.ua/article.phtml?ID=10982&IDw=60 – Виртуальные частные сети.

3. http://www.void.ru/content/832 – Уязвимости виртуальных частных сетей (VPN) – обзор.

4. http://www.infotecs.ru/ – Компания Инфотекс. Решения ViPNet – виртуальные частные сети (VPN) и средства защиты информации.

ИСПОЛЬЗОВАНИЕ АЛЬТЕРНАТИВНЫХ ПУТЕЙ ПЕРЕДАЧИ СООБЩЕНИЙ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ОБМЕНА ЭЛЕКТРОННЫМИ СООБЩЕНИЯМИ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

П.А. Мельниченко, аспирант каф. КИБЭВС, ТУСУР

г. Томск, mpa@udcs.ru

В настоящее время для организации защищенного обмена электронными сообщениями по открытым каналам связи в качестве транспортной подсистемы в большинстве случаев используется обычная электронная почта или ее аналоги, построенные на сходных принципах [1].

Защищенность таких систем основывается на использовании средств криптографической защиты информации (СКЗИ) для исключения возможности нарушения конфиденциальности (шифрование) и целостности (электронно-цифровая подпись) передаваемой информации. Главным требованием использования СКЗИ является сохранение в тайне закрытой части (в случае использования ассиметричного шифрования и/или электронно-цифровой подписи) или всей (в случае использования симметричного шифрования) ключевой информации. То есть в слу-

чае, если это требование не будет соблюдено, передаваемая информация станет доступна для ознакомления и модификации злоумышленником.

Но для того, чтобы выполнить обратное криптографическое преобразование (расшифрование) передаваемой информации, злоумышленник должен обладать преобразованной (зашифрованной) информацией. В случае использования в качестве транспортной подсистемы обычной электронной почты это возможно с большой вероятностью, что показано в [1].

Существует еще несколько способов перехвата передаваемой информации, основанных на пассивном перехвате трафика [2]. В случае передачи информационных пакетов целиком, как это делается в электронной почте, достаточно установить оборудование, осуществляющее перехват информации в любой точке, через которую идет маршрут пакетов.

Как показывает практика, в настоящее время люди, работающие с ключевой информацией для проставления электронно-цифровой подписи и зашифрования документов, не в полной мере осознают важность хранения в тайне закрытой части (в случае использования ассиметричного шифрования и/или электронной цифровой подписи) или всего ключа (в случае использования симметричного шифрования). Это обстоятельство позволяет злоумышленнику завладеть ключевой информацией, не прилагая больших усилий.

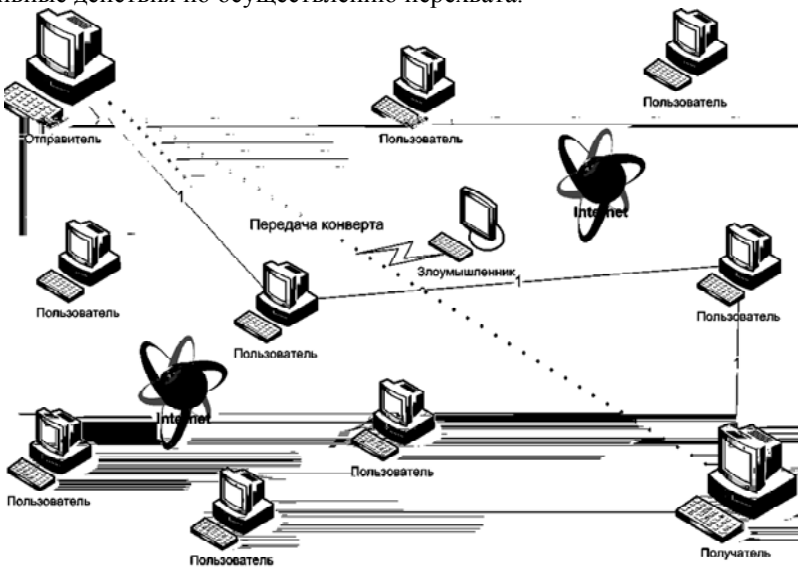
Вследствие этого возникает потребность использовать альтернативные способы передачи информации по открытым каналам связи для повышения защищенности передаваемой информации, используя в качестве механизма защиты сам способ передачи.

Для решения задачи транспортировки важных конфиденциальных сведений имеет смысл обратить внимание на способы транспортировки важных персон охранными фирмами или личными телохранителями. Одним из методов обеспечения личной безопасности при транспортировке человека являет выбор случайного маршрута следования из точки А в точку Б. Маршруты могут отличаться по точкам следования, по типу используемого транспорта и по времени прохождения отдельных участков (рисунок).

Наземную транспортную инфраструктуру можно сравнить с открытыми каналами связи, которыми связаны участники сети Интернет. А важной персоной в данном случае будет являться передаваемый конверт.

При постоянной смене маршрута следования трудоемкость перехвата информации сильно увеличивается вследствие того, что злоумышленнику неизвестно местоположение передаваемого или транспортируемого объекта в определенный момент времени. Но, если

местоположение становится известно, то время на подготовку мероприятий для перехвата становится неприемлемо мало для его осуществления. Это обстоятельство позволяет закончить транспортировку и вывести транспортируемый объект из открытой (недоверенной, неохраняемой) среды до того, как злоумышленник сможет предпринять эффективные действия по осуществлению перехвата.



Построение случайного маршрута для противодействия перехвату информационного конверта злоумышленником

Если при транспортировке персоны (человека) выбирается один маршрут следования из точки А в точку Б, то при транспортировке составных грузов возможно использование нескольких случайных маршрутов, т.е. груз перед отправлением разбивается на несколько частей, которые транспортируются до точки назначения независимо друг от друга. Таким образом, возможно достичь более высокого уровня защищенности всего информационного пакета, так как злоумышленнику потребуется среагировать на несколько событий отправки одновременно или в какой-либо неопределенный для него промежуток времени, чтобы осуществить полный перехват транспортируемого груза. Этот же принцип справедлив для передачи информационных пакетов по открытым каналам связи.

Использование случайного маршрута следования снижает вероятность события, при наступлении которого передаваемый пакет будет

перехвачен на пути следования. Вследствие этого повышается защищенность передаваемых внутри системы сообщений, так как для того, чтобы ознакомиться с информацией и/или модифицировать ее, злоумышленнику потребуется «перехватить» передаваемый пакет.

ЛИТЕРАТУРА

1. *Мельниченко П.А.* Обзор подсистем транспорта российских систем защищенного обмена электронными документами. 2006.

2. *Мельниченко П.А., Петрова Г.В.* Пассивный перехват трафика. Сб. Научная сессия ТУСУР-2005. Томск: ТУСУР, 2005.

ТРАНСПОРТНЫЕ ПОДСИСТЕМЫ. ПРОБЛЕМЫ И ПУТИ РАЗВИТИЯ

П.А. Мельниченко, аспирант каф. КИБЭВС, ТУСУР

г. Томск, mpa@udcs.ru

В настоящее время на территории Российской Федерации, как и во всем мире, все большее количество коммерческих и государственных структур разного уровня переходят на электронную форму работы с документами. Условие наличия развитой системы электронного документооборота в некоторых государственных ведомствах, например в таможне, является обязательным при вступлении страны во Всемирную торговую организацию. Это говорит о заинтересованности мирового сообщества во внедрении средств обработки и передачи документов в электронном виде.

Системы электронного документооборота могут различаться в зависимости от поставленных перед ними целей и решаемых задач. Если это система для ведения внутренней бухгалтерии, учета приказов или электронная канцелярия, то задачами, которые решаются данной системой, являются оптимизированное хранение документов, обеспечение доступности и распределение прав доступа к документам. В отдельный класс выделяются системы, основной задачей которых является гарантированно конфиденциальная передача электронных документов от одной организации или частного лица к другой.

Архитектура построения и принцип действия таких систем в корне отличаются от систем предыдущего класса, так как здесь упор делается именно на то, что передача конфиденциальной информации будет производиться через агрессивную среду (открытые каналы связи). Обычно системы данного класса узкоспециализированны для формирования документов определенного типа и их последующей передачи в другую организацию, например, ФНС России, ПФР и др.

Проектирование и разработка такой системы должны учитывать специфику ее использования. И если система предназначена для работы в агрессивной среде (такой, как сеть Интернет), то наиболее остро встает проблема защиты информации при ее передаче через агрессивную среду (открытые каналы связи, сеть Интернет).

Для решения задачи защиты информации в системах защищенного электронного документооборота используются средства криптографической защиты информации (СКЗИ) в совокупности с принципами, описанными в Федеральном законе 10.01.2002 N 1-ФЗ «Об электронной цифровой подписи» [1].

Использование средств СКЗИ для защиты от несанкционированного доступа подразумевает под собой наличие третьего доверенного лица в системе передачи данных – Удостоверяющего центра. Но отслеживание времени приема/передачи сообщений, разрешения спорных ситуаций в данном вопросе требует привлечения еще одного участника информационного обмена – 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. Это определение актуально только для ФНС России, но отражает базовые функции этого элемента системы передачи конфиденциальных документов.

Фактически специализированный оператор связи берет на себя функции транспортировки, являясь своего рода аналогом курьера при передаче информации от одной организации или частного лица другой стороне.

Таким образом, расширив рамки использования систем передачи конфиденциальной информации, можно выделить такой компонент, как подсистема транспорта, которая несет ответственность за передачу информационных конвертов внутри системы. Данный компонент является, как было сказано выше, своего рода курьером, который должен быть достаточно надежным, чтобы иметь право на транспортировку информационных конвертов любой важности.

Также транспортная подсистема может быть выделена в самостоятельную систему, которая может использоваться вместо, например, электронной почты. Стоит оговориться, что использование обычных общедоступных серверов электронной почты возможно, так как защита от несанкционированного доступа и модификации информации может осуществляться при помощи СКЗИ. Таким образом, возникает проблема

с соблюдением срока доставки, гарантированности доставки, возможности отправки, совместимости со специализированными программными средствами, возможности интеграции в состав более сложных систем.

Принципы современной электронной почты не позволяют использовать ее в тех случаях, когда требуется доставка конвертов в строго определенный срок. Наличие некоторого количества промежуточных звеньев – серверов-ретрансляторов – подразумевает под собой передачу конверта через несколько независимых друг от друга «рук», каждые из которых могут не доставить конверт или задержать его доставку.

Это не единственное ограничение, из-за которого использование общедоступной электронной почты проблематично при транспортировке конвертов особой важности.

Если путь прохождения письма возможно определить по заголовкам, добавляемым в конверт сообщения, то отследить реальное местоположения конверта в определенный момент времени не представляется возможным. Это требуется в тех случаях, когда по какой-либо причине дальнейшая транспортировка конверта невозможна или канал для передачи недоступен в данный момент. Принципы электронной почты не позволяют отследить данную ситуацию. Конверт будет либо потерян, либо возвращен отправителю с ошибочным результатом доставки.

Еще одна проблема заключается в обеспечении возможности подключения к серверу, который осуществляет доставку. Все большее количество корпоративных, домашних и других сетей снабжают маршрутизаторы межсетевыми экранами для возможности блокировки нежелательного трафика. Очень часто блокируется и возможность использования электронной почты по протоколам, специально разработанным для передачи сообщений (SMTP, POP3, IMAP). Это делается из соображений безопасности, так как по электронной почте очень часто приходят вредоносные программы или другая нежелательная информация. Но, несмотря на это, транспортная система или подсистема должна быть доступна. Поэтому требуется либо перенастраивать межсетевые экраны, установленные в сети, либо переходить на протоколы и порты для подключений, разрешенные в данной сети [2–4].

Для возможности работы на «слабых» каналах связи, при использовании которых возможны частые обрывы соединений и искажение передаваемой информации, современные протоколы электронной почты не смогут обеспечить гарантированную передачу конвертов от отправителя к серверу, отвечающему за доставку. Требуется использование протокола, в котором бы была возможность восстанавливать разорванное подключение при минимальных затратах времени и количестве пе-

редаваемой информации. Также требуется производить контроль целостности переданной информации. Примером может служить протокол FTP (RFC-959 – File Transfer Protocol), который поддерживает «докачку» файлов при обрыве соединения. Но для установления соединения и начала передачи данных по данному протоколу требуется передать довольно большое количество служебной информации, что нежелательно при использовании «слабых» каналов.

Таким образом, использование распространенных протоколов, таких как SMTP, POP3, IMAP, FTP, HTTP, возможно при отсутствии внутренних сетевых ограничений участников информационного обмена и ограничений на канал передачи данных. Для того, чтобы сделать транспортную систему универсальной с точки зрения используемых протоколов, требуется объединить широко распространенные протоколы и добавить возможность использования протоколов для «слабых» линий связи.

Возможность интеграции данного решения в другие системы может быть достигнута использованием протоколов более высокого уровня, таких как XML, HTML, SOAP и другие. Использование стандартизированных приемов инкапсуляции передаваемых данных делает возможность простого использования транспортной системы из приложений сторонних разработчиков [5–8].

ЛИТЕРАТУРА

1. *Федеральный* закон 10.01.2002 N 1-ФЗ «Об электронной цифровой подписи».

2. *Общее* описание продуктов «КриптоПро».

3. *Приказ* МНС России от 02.04.2002 № БГ-3-32/169 «Порядок представления налоговой декларации в электронном виде по телекоммуникационным каналам связи.

4. *Типовые* решения по организации обмена информацией в электронном виде по телекоммуникационным каналам между ФНС России и сторонними организациям.

5. http://osu.cctpu.edu.ru/edu/tech/internet/email/func.html – Принципы организации электронной почты (E-mail.

6. http://www.rhd.ru / docs / manuals / enterprise / RHEL-AS-2.1-Manual / install-guide / s1-firewallconfig.html – Настройка межсетевого экран.

7. http://lib.align.ru/rfc/0959.html – FILE TRANSFER PROTOCOL (FTP.

8. http://www.void.ru/content/832 – Уязвимости виртуальных частных сетей (VPN) (обзор).

РАЗРАБОТКА ЗАЩИЩЕННОЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА СИСТЕМЫ IP-ТЕЛЕФОНИИ, ФУНКЦИОНИРУЮЩЕЙ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS

С.В. Нопин, аспирант

ОмГТУ, Россия, т. 65-85-60. E-mail: work800@yandex.ru

В современном обществе информация является одной из главных ценностей. По этой причине возможны попытки злоумышленников получить несанкционированный доступ (НСД) к информации, циркулирующей в общедоступных вычислительных сетях, в частности, к оцифрованной речи, передающейся через общедоступные вычислительные сети. Необходимость сохранности этой информации делает актуальной разработку способов ее защиты от НСД. Использование ПЭВМ с установленными ОС Windows и IP-сетей для организации речевых переговоров в защищенном режиме предъявляет особые требования как к организации сжатия и передачи речи, так и к системам ее защиты. В научной литературе в последние годы вышли десятки статей, книг и монографий, посвященных защите информации с помощью криптографических преобразований и компрессии речевого сигнала. Однако в основном это работы теоретического характера, и использование их результатов на практике затруднено. Остается слабо освещенным вопрос использования и анализа современных встроенных в операционные системы (ОС) криптографических и аудиоинтерфейсов.

Все современные операционные системы Microsoft содержат криптографические подсистемы, и ключевую роль в их реализации играют интерфейс Microsoft Cryptographic Application Programming Interface (CryptoAPI), а также специальные интерфейсы, предназначенные как для ввода-вывода звука, так и для преобразования форматов (компрессии/декомпрессии) звуковых данных. Одним из интерфейсов ввода-вывода звука является DirectSound ОС Windows [2]. Интерфейс преобразования форматов звуковых данных называется (ACM) Audio Compression Manager (диспетчер сжатия звука). Целью исследования явился анализ возможностей разработки систем передачи речи через компьютерные сети в защищенном режиме, используя интерфейсы CriptoAPI, DirectSound и ACM.

Предложенные способы получения и преобразования данных были использованы в программе VoiceOverNet – системе передачи речи через компьютерные сети в защищенном режиме, использующей возможности интерфейсов CriptoAPI, DirectSound и ACM, а также соответствую-

щие модули ОС Windows. Для разработки программы использовалась среда разработки приложений C++Builder 6.0 [1].

Разработанное программное обеспечение имеет технические особенности и позволяет осуществлять, в том числе в режиме реального времени: 1) определение криптографических характеристик и возможностей криптографических модулей и библиотек, установленных в ОС Windows; 2) выбор и настройку параметров алгоритмов компрессии / декомпрессии звука на основе аудиокодеков, установленных в ОС Windows; 3) выбор алгоритмов криптографических преобразований и настройку их параметров для защиты от НСД блоков звуковых данных; 4) ввод-вывод звука в один из звуковых адаптеров на основе интерфейсов DirectSound ОС Windows с разрядностью звука 8 бит, частотой дискретизации 8000 Гц; 5) компрессию / декомпрессию звуковых блоков данных с помощью выбранных пользователем аудиокодеков установленных в ОС Windows в режимах и с настройками заданных пользователем; 6) криптографическое преобразование (шифрация, дешифрация, хеширование) блоков звуковых данных с помощью выбранных пользователем криптографических модулей, установленных в ОС Windows в режимах и с настройками, заданными пользователем; 7) формирование и передачу через вычислительную сеть удаленному абоненту IP-пакетов со сжатыми и криптографически защищенными звуковыми данными.

Были получены следующие результаты: в режиме дуплексной связи было получено хорошее качество речи (разборчивость звуков по требованиям ГОСТ 16600-72 больше 90%) в следующих режимах работы программы VoiceOverNet: 1) без компрессии, без шифрации и хеширования; 2) с компрессией, шифрацией и хешированием; 3) с компрессией, шифрацией, без хеширования; 4) с компрессией, без шифрации, с хешированием; 5) без компрессии, с шифрацией и хешированием; 6) без компрессии, с шифрацией, без хеширования; 7) без компрессии, без шифрации, с хешированием. Из алгоритмов компрессии звука были успешно применены в составе программы следующие аудиокодеки (в скобках битовая скорость, кбит/с): GSM 6.10 (13), DSP Group TrueSpeech™ (8,5), IMA ADPCM (32,4), Microsoft ADPCM (32,7), Alex AC3 Audio (4,9; 5,9; 7,9). Также были успешно использованы следующие алгоритмы шифрования (в скобках указана длина ключа в битах): RC2 (40-128), RC4 (40-128), DES (56), Two Key Triple DES (112), Three Key Triple DES (168), American Encryption Standard (128, 192, 256), ГОСТ Р 28147-89 (256). Среди алгоритмов хеширования были работоспособны алгоритмы SHA-1, MD2, MD4, MD5, HMAC, ГОСТ Р 34.11-94. Шифрование успешно было протестировано в трех из четырех режимов: а) режим гаммирования с обратной связью (Cipher Feedback Mode, CFB); б) шифр простой

замены с зацеплением (Cipher Block Chaining Mode, CBC); в) шифр простой замены (Electronic CodeBook Mode, ECB).

В ходе экспериментов в локальной сети была получена статистическая информация о вкладе в задержку пакетов со звуковыми данными времени на передачу пакета. Сопоставляя эту составляющую (менее 2 мс) с функциональной задержкой кодека либо с обычной буферизацией перед передачей пакета (>= 80 мс), можно сделать вывод, что для высокоскоростных локальных сетей она играет небольшую роль (ее вклад менее 2%). Полученные данные о необходимом времени на компрессию и шифрацию пакетов звука в результате других экспериментов показывает, что даже для самых медленных алгоритмов вклад обеих этих составляющих также не превышал 1,5 мс для пакета длиной 1000 байт (125 мс для частоты дискретизации 8000 Гц).

Апробация разработанной программы VoiceOverNet показала эффективность применения технологий DirectSound, ACM, CriptoAPI ОС Windows при реализации защищенной от несанкционированного доступа системы IP телефонии. Сертифицированные ФСБ РФ криптомодули могут применяться в системах IP телефонии, защищенных от НСД силовыми ведомствами, органами власти и управления.

Разработанная программа VoiceOverNet, технологии Microsoft DirectSound, ACM для компрессии / декомпрессии и CriptoAPI для криптографической защиты информации могут быть использованы при компьютерном моделировании защиты систем IP телефонии от НСД и для реального закрытия речи, передаваемой по компьютерным сетям от потенциальных нарушителей. С помощью программы можно определять типы, параметры криптоалгоритмов и модулей, осуществляющих компрессию/декомпрессию звука, установленных в системе. Кроме того, возможность интеграции в программное обеспечение криптографических и аудиокомпонент, разрабатываемых различными производителями, позволяет сократить время разработки, увеличить эффективность и качество программного продукта, решить проблемы его модернизации.

ЛИТЕРАТУРА

1. *Архангельский А.Я.* C++Builder 6: Справочное пособие. Книга 1. Язык C++. М.: Бином-Пресс, 2002. 544 с.

2. *Гордеев О.* Программирование звука в Windows. Руководство для профессионалов. СПб.: BHV – Санкт-Петербург, 1999. 364 с.

КЛАССИФИКАЦИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Г.В. Петрова, ассистент каф. КИБЭВС, Р.В. Силиненко ст. 4 курса
ТУСУР, г. Томск, т. 414-476, pgv@keva.tusur.ru

В связи с ростом числа инцидентов, связанных с компьютерной безопасностью, а так же с все ускоряющейся популяризацией Internet и локальных сетей, организации все чаще прибегают к услугам программно-аппаратных комплексов, реализующих функции мониторинга информационной защищенности предприятия.

Эти комплексы, обычно называемые системами обнаружения вторжений (IDS[1]), являются предметом исследования данной работы. В работе приводится базовая классификация IDS [1].

Системы обнаружения вторжений – это системы защиты, которые детектируют подозрительную активность в сети.

Основные задачи IDS:

1) обнаружение и по возможности предотвращение попыток компрометации системы безопасности предприятия или отдельного пользователя;

2) выявление активных попыток нападения на систему на самой ранней стадии – сборе информации, например, сканирования портов.

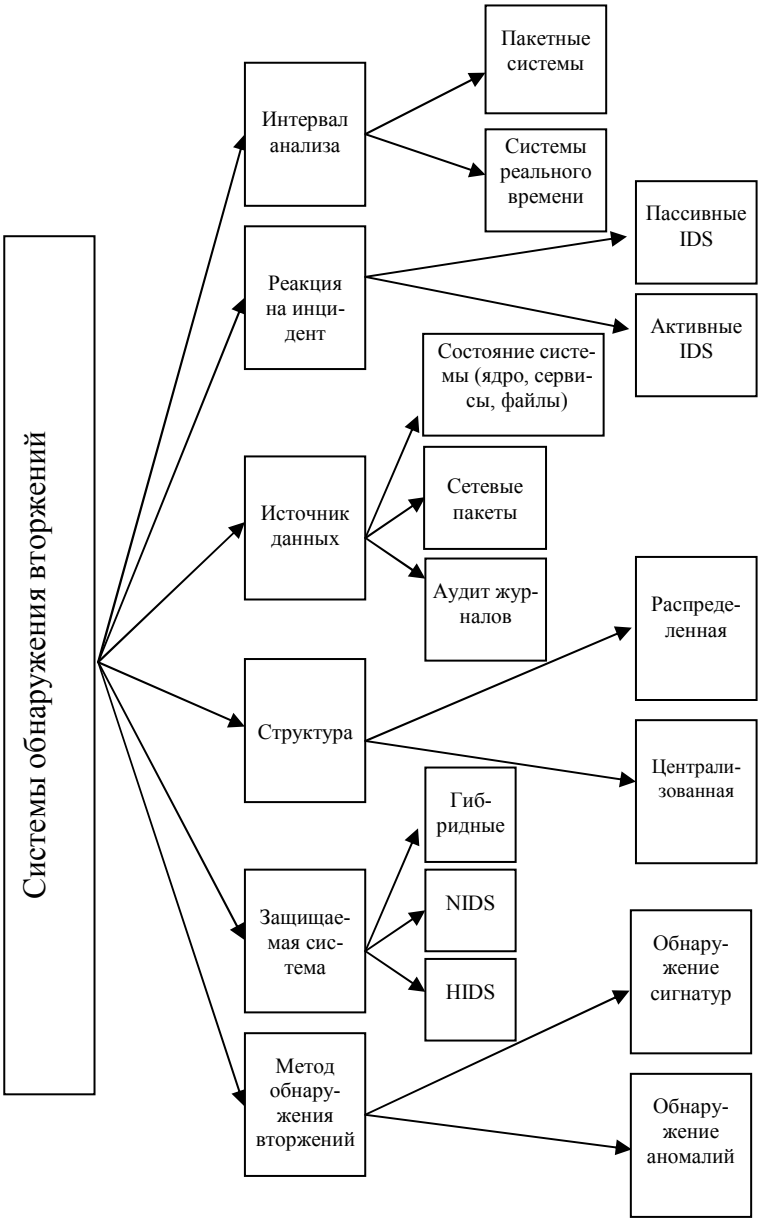
Одна из ключевых особенностей IDS – это их способность обнаруживать нестандартную активность и информировать об этом администраторов и блокировать подозрительное соединение. Кроме того, IDS способны различать инсайдерские атаки и атаки, производимые снаружи защищаемой системы.

Таким образом, обнаружение вторжения – это процесс идентификации и реагирования на зловредную активность, направленную на компьютерные и сетевые ресурсы.

IDS ищет так называемые сигнатуры, представляющие собой специфичные образцы сетевой активности, которая обычно проявляется при попытках произвести зловредные действия. Есть и другой тип систем, источником данных для которых служит статистическая информация, собираемая на основе анализируемого сетевого трафика.

Если IDS ищет сигнатуры или собирает статистику о сетевом трафике через включенный особым образом сетевой интерфейс, то такая система называется Network Based IDS или NIDS (русский аналог термина не известен). NIDS обычно устанавливают на активных сетевых элементах, например на маршрутизаторах. Если система проверяет ресурсы, локальные для конкретной машины, например, журналы, файло-

[1] Intrusion Detection System.



Классификация систем обнаружения вторжений

вую активность, сетевой трафик, предназначенный для этой машины, то такая система называется Host Based IDS (русский аналог термина не известен). Итак, по области действия выделяются Network Based IDS и Host Based IDS [2–5].

По структуре IDS делятся на системы с централизованной архитектурой и интегрированные приложения, создающие распределенную систему так называемых агентов, располагающихся на разных машинах и следящих за своей частью сети. Большим преимуществом такой архитектуры является возможность агентов следить именно за некоторой частью сети, а не только за отдельной машиной. Таким образом, ореалы действия разных агентов могут перекрываться, что позволяет коррелировать распределенную информацию.

Еще один критерий деления IDS – по способу реагирования. По этому критерию все системы можно разделить на пассивные и активные. Пассивные системы просто генерируют сообщения, предупреждающие о возможной атаке, тогда как активные системы могут отвечать на атаки, пробовать проследить атакующего, получить дополнительную информацию о методиках, обновить программное обеспечение, заблокировать сетевую активность с машины атакующего и т.д.

Последний существенный параметр, по которому можно разделить IDS, – это время реагирования. В этом плане выделяются системы реального времени (обычно это NIDS) и системы пакетной обработки, проводящие анализ через определенные промежутки времени (чаще это HIDS).

В заключении сведем все вышесказанное в классифицирующую схему, наглядно иллюстрирующую разнообразие принципов построения систем обнаружения вторжений.

ЛИТЕРАТУРА

1. *Przemyslaw Kazienko, Piotr Dorosz.* WindowsSecurity.com: Intrusion Detection Systems (IDS) Parts 1, 2, 3

2. WindowsSecurity.com : Intrusion Detection within a Secured Network.

3. How To Guide – Intrusion Detection Systems Internet Security Systems.

4. Running A World Class Intrusion Detection System. J.D. Aupperle March 2, 2004.

5. *Лапонина О.Р.* CitForum.ru : Intrusion Detection Systems: Лекция из курса «Межсетевое экранирование»

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ХАРАКТЕРИСТИК ТЕКСТА НА РЕЗУЛЬТАТИВНОСТЬ ОПРЕДЕЛЕНИЯ АВТОРСТВА НЕИЗВЕСТНОГО ТЕКСТА

А.С. Романов, студент 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 64-41-34, ras@ms.tusur.ru.

В настоящее время активно развиваются методы определения авторства текста на основе различных подходов. Однако недостаточно внимания уделяется оценкам собственно характеристик текста для определения автора. Очевидно, что некоторые базовые характеристики являются зависимыми друг от друга и не должны быть использованы в качестве альтернативных.

Состоятельность характеристик может быть определена только экспериментально. Вместе с тем, актуальным остается вопрос автоматизации определения авторства текста.

Для анализа информативности характеристик текста, применяемых для определения авторства текста можно использовать несколько способов:

1. Анализ статистической информации, собранной на основе текстов различных авторов.

Для удобства анализа информация может представляться в виде графиков.

Критерии характеристики оцениваются следующими ключевыми правилами.

а) характеристика должна быть устойчива к изменению стиля внутри произведений одного и того же автора, ее колебания могут быть признаны несущественными;

б) характеристика должна быть чувствительна к авторскому стилю как таковому, т.е. предоставлять возможность статистически разделить двух авторов с заданной точностью;

в) характеристика не может контролироваться автором сознательно.

2. Анализ результата работы обученной нейронной сети.

В надежде на избирательность нейронных сетей используется более широкий набор характеристик, не обязательно удовлетворяющий вышеперечисленным правилам. Нейронная сеть обучается на некотором наборе подобных характеристик текстов разных авторов. Затем на вход обученной нейронной сети подаются аналогичные характеристики текста, не участвовавшего в обучении нейронной сети, автором которого является один из авторов, участвовавших в обучении. В результате на выходе нейронной сети формируется вектор принадлежности тому или иному автору. Автор, получивший наибольший результат (в идеальном

случае единицу), является предполагаемым автором неизвестного текста. Затем берется текст следующего автора, тексты которого использованы в обучении и т.д. Изменяя набор характеристик, необходимо добиться результата, как можно более близкого к единице для каждого истинного автора в каждом из опытов.

Недостатком использования данного подхода является то, что судить о влиянии характеристик можно лишь по входам и выходам нейронной сети. Сам процесс принятия решения и критерии, использующиеся при этом, остаются неизвестными.

Для исследований будет использован программный продукт на основе нейронных сетей, структура которого описана в [1].

На данном этапе работы программа позволяет автоматизировать сбор статистической информации об исследуемых текстах, а также проводить с ее помощью предварительный анализ влияния конкретных характеристик текста на результативность определения авторства с выдачей результатов в виде графиков (рис. 1).

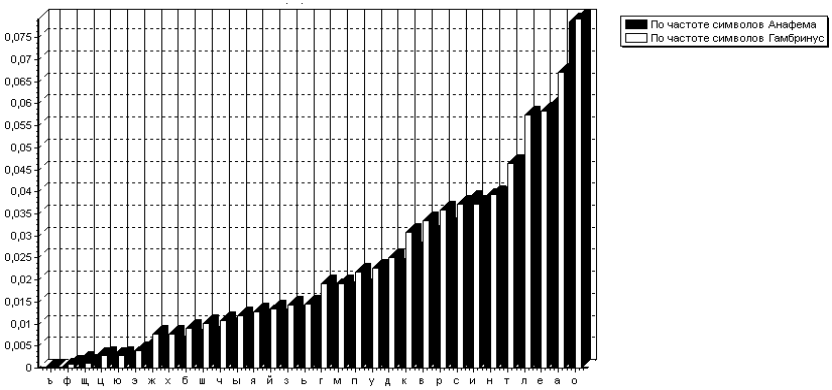


Рис. 1. Графики частот встречаемости строчных букв в двух текстах

Осуществляется сбор в базу данных (рис. 2) следующей информации о тексте: количество, частота встречаемости символов, двойных символов, слов, двойных слов предложений; длина, средняя длина, отклонение от средней длины слов, и предложений, морфологическая информация о словах (нормальная форма, часть речи, род, число, падеж, время и др.) и т.д.

В настоящее время ведется экспериментальное исследование различных характеристик текста и их комбинаций для выявления набора наиболее «информативных» в задаче определения авторства текста.

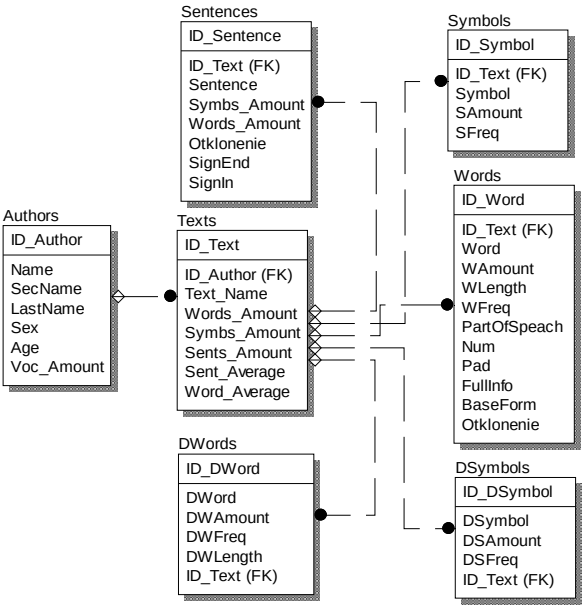


Рис. 2. Концептуальная модель базы данных

ЛИТЕРАТУРА

1. *Романов А.С., Мещеряков Р.В.* Структура программного обеспечения идентификации автора текста // Актуальные проблемы математики, механики, информатики: Материалы Международной научно-методической конференции, посвященной 90-летию высшего математического образования на Урале/ Перм. гос. ун-т; под ред. Л.Н. Лядовой, В.И. Яковлева, Л.Н. Ясницкого. Пермь, 2006. С. 210–211.

БЕЗОПАСНОСТЬ С ТОЧКИ ЗРЕНИЯ НАДЕЖНОСТИ ЭВМ

А.А. Русев, аспирант, ИФИ, ООО «Крипто-Про»
г. Москва, т. 7 (495) 933-1168, raa@cryptopro.ru

Считается, что вероятность ложной аутентификации не должна превышать 10^{-6} на попытку доступа [1]. Логично предположить, что вероятности ошибок при выполнении прочих критических операций (идентификации, проверки электронной цифровой подписи, контроля целостности криптографических модулей и др.) также не должны превышать эту величину. Предположим, что пользователь многопользовательской системы постоянно пытается получить доступ к файлам друго-

го пользователя, при этом происходит проверка соответствия его идентификатора владельцу, и доступ запрещается. При возникновении ошибки в функции проверки он получит доступ. Можно простроить еще ряд рассуждений, приводящих к тому, что следует говорить о вероятности возникновения ошибки в течение некоторого длительного периода времени.

Причиной ошибки выполнения программы может быть сбой аппаратуры. Таким образом, необходимо оценить вероятность этого сбоя.

При оценке надежности функционирования ЭВМ используется стандартная модель с экспоненциальным распределением времени между отказами и последовательным соединением элементов в силу шинной архитектуры:

- центральный процессор,
- оперативное запоминающее устройство (ОЗУ),
- шина ЭВМ,
- контроллеры ЭВМ,
- жесткий магнитный диск с контроллером,
- блок питания.

Данные по надежности отдельных устройств и блоков импортной вычислительной техники в общедоступных официальных источниках отражены неполно, поэтому используются данные, опубликованные в [2–6], которые сведены в таблицу.

Характеристики надежности ЭВМ и ее узлов

Устройство	Характеристика надежности
Центральный процессор	Интенсивность отказов на чип: $\lambda=10^{-1}$ (1/ч), Надежность микропроцессора Pentium (коэффициент сложности 32): $\lambda = 1\cdot32\cdot0.018\cdot10^{-6} = 0.576\cdot10^{-6}$ (1/ч).
ОЗУ	Коэффициент сложности 8, коэффициент корпуса 3, количество корпусов – до 16: $\lambda = 3\cdot16\cdot8\cdot0.05\cdot10^{-6}=1.9\cdot10^{-5}$ (1/ч)
Материнская плата	Надежность 3000 паек: $\lambda=2.1\cdot10^{-6}$ (1/ч)
Контроллер	$\lambda = 10^{-9}$ (1/ч)
Жесткий диск	Время наработки на отказ 500000 ч
Блок питания	Время наработки на отказ 40000–60000 ч
Сервер SunUltra	Время наработки на отказ 40000 ч

Применяется следующая методика расчета надежности блока ЭВМ, состоящего из однотипных элементов:

$$\lambda = n\, k_{\text{сл}}\, k_{\text{корп}}\, \lambda_0, \qquad (1)$$

где n – число однотипных элементов в блоке; $k_{сл}$ – коэффициент сложности, равный отношению числа транзисторов на один чип импортной элементной базы к числу транзисторов на один чип отечественной элементной базы, принятой в справочнике за эталонную; $k_{корп}$ – коэффициент корпуса, равный отношению числа выводов на один чип импортной элементной базы к числу выводов на один чип отечественной элементной базы; λ_0 – интенсивность отказов чипа отечественной элементной базы, состоящего из 10^5 транзисторов.

Шинная архитектура ЭВМ обусловливает последовательное соединение элементов в эквивалентной схеме надежности, поэтому для оценки общей надежности интенсивности отказов входящих в нее устройств суммируются. В результате для ЭВМ на базе процессора Pentium получаем $\lambda = 2{,}5 \cdot 10^{-5}$ (1/ч), что соответствует значению времени наработки на отказ $T = 40\,000$ ч.

Другой подход к оценке надежности электронных блоков ЭВМ состоит к констатации факта, что с развитием элементной базы и повышением степени ее интеграции надежность отдельного чипа остается постоянной величиной и составляет $\lambda_{чипа} = 10^{-7}$ (1/ч). Надежность электронного блока определяется числом элементов (n), входящих в его состав, $\lambda = n \cdot 10^{-7}$ (1/ч) (без учета надежности блока питания). Такой оптимистичный подход приводит к показателям времени наработки на отказ в сотни тысяч часов.

С другой стороны, хорошо известны показатели надежности пайки оловом $\lambda_{пайки} = 2 \cdot 10^{-8}$ [7], и при количестве паек порядка 1000 общая надежность характеризуется крайне низкой величиной $\lambda = 10^{-5}$. Эта пессимистичная оценка должна корректироваться с учетом того, что современная пайка ведется другими материалами с лучшими характеристиками, однако численных показателей по ним не найдено.

Интенсивность сбоев в 5–10 раз превосходит интенсивность постоянных отказов. Посчитаем суточную вероятность сбоя по оптимистичному подходу в предположении, что в критических операциях участвуют только три чипа: процессор, один чип памяти и контроллер:

$$\lambda_{от} = 3 \cdot 10^{-7} \text{ (1/ч)} \quad (2)$$

$$\lambda_{сбоя} = \lambda_{от} \cdot 10 = 3 \cdot 10^{-6} \text{ (1/ч)} \quad (3)$$

$$P_{сбоя} = 1 - e^{-\lambda_{сбоя} \cdot 24} = 7{,}2 \cdot 10^{-5} \quad (4)$$

Итак, при наилучших предположениях суточная вероятность сбоя оказывается довольно высокой. Это говорит о том, что для надежной работы критических модулей должны применяться дополнительные меры: например, контроль целостности файлов при загрузке библиотеки, контроль целостности критических объектов в ОЗУ, периодический

тестовый контроль функций на предмет выявления сбоев в работе, а также дублирование как в аппаратуре, так и при выполнении программ.

ЛИТЕРАТУРА

1. *М.Р. Биктимиров, В.В. Засыпкина, А.Ю. Щербаков*. К вопросу о разработке требований к защите от несанкционированного доступа конфиденциальной информации // Безопасность информационных технологий. 2001. №1. С. 62–69.

2. *Горшков В.Н*. Надежность оперативных запоминающих устройств ЭВМ. Л.: Энергоатомиздат, 1987. 168 с.

3. *Надежность* электрорадиоизделий. Единый справочник. Т. 1. 1992. Российский НИИ Электростандарт.

4. *Методика* расчета надежности опытных образцов ПЭВМ ЕС-1841, Е11.700.012.РР4.2.

5. *Дополнение* к расчетам надежности опытных образцов ПЭВМ ЕС-1841 в части наработки на отказ. Е 11.700.012.РР2.

6. Designing Highly Available Architectures: A Methodology. Erik Vanden Meersch, Global Sales. Sun BluePrints™ OnLine – November 2002.

7. *Козлов Б.А., Ушаков И.А*. Справочник по расчету надежности аппаратуры радиоэлектроники и автоматики. М.: Сов. радио, 197–472 с.

КОМПЛЕКС ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕР БЕЗОПАСНОСТИ ОБЩЕЖИТИЙ ТУСУР

А.А. Самсонов, студент группы 522-2

ТУСУР, г. Томск, т. 89131103152, Anatoli111@mail.ru.

1. Введение

В распоряжение Томского государственного университета систем управления и радиоэлектронике отводиться пять студенческих общежитий (№ 2–6). Одно общежитие отдано для сотрудников (общежитие «№ 2»), а во все остальных проживают студенты (общежитие № 3–6). По своей конструкции все общежития различны, одни из них являются коридорного типа № 5 и 6, а другие, как № 4, секционного. В качестве примера разберем общежитие № 5.

С самого основания студенческого общежития № 5 в 1967 г. появились ряд проблем, связанных с безопасностью проживания студентов (например, пожарная безопасность и т.д.). Вот и были введены для студентов правила проживания в общежитии, как, например «положение проживания студентов в общежитиях Томского государственного университета систем управления и радиоэлектроники». А также описаны все положения, связанные с проживанием и деятельностью сотрудников общежития, и учтены организационно-технические меры безопасности общежития.

2. Основная часть

– Структура руководства общежития.

– Структура самоуправление общежития.

– Структура службы безопасности общежития.

– Организационно-технические меры безопасности проживания в общежитии ТУСУР.

3. Приложение

Приложение 1. Положение о студенческом общежитии.

Приложение 2. Правила проживания студентов в общежития ТУСУР.

Приложение 3. Положение о студенческом отряде охраны правопорядка ТУСУР.

Приложение 4. Рейтинговая система проживания в общежитии ТУСУР.

4. Заключение

В ходе проделанной работы были описаны организационные моменты по структуре общежития, где было показана структура руководства общежития, структура самоуправления студентов общежития, где была отражена правовая база по проживанию в студенческих общежитиях ТУСУР. Также показаны организационно-технические меры безопасности в общежитии, и даны рекомендации по повышению безопасности проживания в общежитие.

СИСТЕМА СБОРА ИНФОРМАЦИИ ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

М.В. Савчук, студент 5 курса каф. КИБЭВС

Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС

ТУСУР, г. Томск, e-mail: mehos@ngs.ru

В нашей предыдущей работе был описан комплекс, позволяющий внедрять произвольные методы аутентификации в приложения Windows. Более подробно об этом можно прочитать в сборнике докладов научной сессии ТУСУР от 2006 г. В ходе разработки был предложен ряд существенных дополнений.

Помимо штатных модулей получения и отображения данных, таких как текстовое поле, поле ввода пароля, надпись и картинка для использования более совершенных механизмов аутентификации (по клавиатурному подчерку, электронному ключу и т.д.), необходимо обеспечивать механизм встраивания дополнительных модулей получения информации от пользователей. Первоначально для реализации этих возможностей планировалось использовать технологию DCOM. Однако

использование такого подхода выявило ряд существенных недостатков, среди которых можно отметить следующие.

– привязка модулей только к одной платформе, в данном случае только Windows;

– невозможность использования в консольных приложениях.

Таким образом, оправданным решением проблемы является разделение модулей сбора информации с модулями аутентификации.

С одной стороны, появляется возможность для использования нескольких вариантов модулей сбора для осуществления единообразной аутентификации разнородных клиентов (веб-приложение, мобильный пользователь) а, с другой стороны, один и тот же модуль сбора может использоваться в нескольких механизмах аутентификации.

Клиентская часть, представляемая отдельной библиотекой, регистрирует приложение и транслирует передаваемую пользователем информацию в серверную часть, которая располагается либо на этом же компьютере, либо на специально оборудованном для этих целей. Если необходимый модуль сбора информации отсутствует либо поврежден (не соответствует контрольная сумма, либо модуль получен не из доверенного источника), то серверная часть, основываясь на данных о целевой платформе, передает необходимый модуль сбора клиентской части, которая исполняет его в адресном пространстве приложения.

Интерфейс для взаимодействия с модулями тривиален, что позволяет минимизировать неизбежные сложности при проектировании для использования на различных платформах. Существуют четыре основных функции: инициализация, установка значения, получение значения и финализация. Для текстовых модулей передаются нажатия клавиш на клавиатуре и мыши. Для модулей, исполняющихся в графическом режиме, сообщения, посылаемые системой, транслируются в модуль с использованием штатных средств, поставляемых с системой.

Следует использовать текстовый протокол обмена сообщениями без подключения механизмов бинарной сериализации объектов, поскольку модули в общем случае могут использовать различные объектные модели и разные версии компиляторов. Однако для специфичных модулей сбора информации, поставляющихся только в комплекте с основными, допустимо использование текстовой сериализации, внедренной в XML. При передаче информация с отдельных модулей упаковывается в текстовые фреймы, передаваемые ядру, которое их распаковывает, разделяет на отдельные потоки и передает на обработку соответствующим механизмам аутентификации [1–4].

Таким образом, разработанная архитектура позволяет обеспечивать широкий спектр механизмов аутентификации для различных целевых

платформ с возможностью многократного использования компонентов и их независимого обновления.

ЛИТЕРАТУРА

1. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. Наука и техника, 2004. 384 с.

2. *Щербаков Д.В*. Компьютерная безопасность. Введение в теорию и практику. НОЛИДЖ, 2003. 352 с.

3. *Александреску А.* Современное проектирование на C++. Питер Пресс, 2000. 420 с.

4. *Бек К.* Экстремальное программирование. Вильямс, 1999. 213 с.

АНАЛИЗ И СРАВНЕНИЕ СТАТИСТИЧЕСКОГО ПОДХОДА И ИСПОЛЬЗОВАНИЯ АППАРАТА НЕЙРОННЫХ СЕТЕЙ В РЕШЕНИИ ЗАДАЧИ ОПРЕДЕЛЕНИЯ АВТОРСТВА

В.Н. Щербаков, студент 5 курса КСУП
Р.В. Мещеряков, к.т.н., доцент

Целью проделанной работы являлось исследование существующих методов идентификации автора печатного текста. Сравнение результативности существующих методов при использовании статистического подхода и аппарата нейронных сетей.

Основное предположение, без которого невозможен программный анализ текстов для идентификации – существование характеристик, однозначно определяющих автора, которые вносятся автором бессознательно, не зависят от настроения автора и практически не изменяются с возрастом (авторский инвариант) [1].

Проанализировав все существующие методы, было принято решение исследовать тексты несколькими методами используя два вышеназванных подхода:

– метод опорных слов, в дальнейшем метод Фоменко (подсчет количества появления союзов, частиц и предлогов);

– синтаксический метод (подсчет знаков препинания, слов и предложений определенной длины);

– комбинированный (объединение метода Фоменко и синтаксического метода);

– экспериментальный метод (подсчет внешних и внутренних знаков препинания, гласных и согласных).

При статистическом подходе было решено подсчитывать отклонение каждого параметра исследуемого текста от параметров известного автора.

Полученные данные для неизвестного текста поочередно сравнивались с текстами из базы данных. Результаты отклонения на каждом параметре суммировались. После проверки всех параметров происходило сравнение со следующим автором. После подсчета отклонений всех параметров для каждого автора, известного базе данных, происходило сравнение всех сумм отклонений по каждому известному автору. Автор, сумма отклонений которого наименьшая, являлся предполагаемым автором исследуемого текста.

При использовании аппарата нейронных сетей полученные данные подавались на вход предварительно обученной нейронной сети. После работы сети фиксировались выходные данные. Автор, получивший наибольший результат (в идеальном случае единицу), являлся предполагаемым автором неизвестного текста.

При статистическом подходе метод Фоменко не оправдал себя даже на заведомо большей выборке (при выборке в 50000 слов правильно определено 6 авторов из 10). При использовании аппарата нейронных сетей результаты на выборке уже в 6000 слов (7 правильно идентифицированных авторов) лучше, чем при статистическом подходе на наибольшей выборке (табл. 1).

Таблица 1

Результаты исследования метода Фоменко

	Метод Фоменко	
	Статистический подход	Нейронные сети
6000	4	7
20000	5	9
50000	6	9

При статистическом подходе синтаксический метод показал не очень высокие, но достаточно стабильные результаты. На выборке в 50000 слов правильно определены всего 6 авторов из 10, но оставшиеся четыре автора вошли в тройку претендентов на авторство своих произведений. Использование аппарата нейронных сетей прошло более успешно по сравнению со статистическим подходом. На выборке в 50000 слов успешно распознаны уже все 10 авторов (табл. 2).

Таблица 2

Результаты исследования синтаксического метода

	Синтаксический метод	
	Статистический подход	Нейронные сети
6000	5	8
20000	6	7
50000	6	10

Наиболее результативным оказалось применение комбинированного метода (табл. 3) и экспериментального (табл. 4) с использованием аппарата нейронных сетей. Уже на выборке в 20000 слов получен результат 10 авторов из 10.

Таблица 3

Результаты исследования комбинированного метода

	Комбинированный метод	
	Статистический подход	Нейронные сети
6000	6	6
20000	8	10
50000	7	10

Таблица 4

Результаты исследования комбинированного метода

	Экспериментальный метод	
	Статистический подход	Нейронные сети
6000		6
20000		10
50000		10

По результатам исследования сделан вывод о неоспоримом преимуществе использования аппарата нейронных сетей по сравнению со статистическим подходом. Результаты идентификации при использовании нейронных сетей лучше результатов использования статистического подхода практически на всех методах, при любом размере выборки.

ЛИТЕРАТУРА

1. *Волевач В.К.* Проблема установления авторства в работах В. Кайзера и Ф. Шнейдера. // Вопросы текстологии. Вып. 2. М.: Изд. АН СССР, 1960. С. 256–274.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

М.А. Шабаловский, студент 5 курса, ФВС КИБЭВС
ТУСУР, г. Томск, max_fish_tysyr@rambler.ru

Особенность нынешнего периода развития общества является переход от индустриального общества к информационному, в котором информация становится более важным ресурсом, чем материальные или энергетические ресурсы. Инструментами решения ряда задач являются процедуры идентификации и аутентификации пользователей.

Идентификация – присвоение субъектам или объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Идентификация и аутентификация является основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание опознанных (именованных) субъектов.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова «аутентификация» иногда используют словосочетание «проверка подлинности».

Процесс аутентификации пользователя компьютером можно разделить на два этапа:

– подготовительный – выполняется при регистрации пользователя в системе. Именно тогда у пользователя запрашивается образец аутентификационной информации, например, пароль или контрольный отпечаток пальца, который будет рассматриваться системой как эталон при аутентификации;

– штатный – образец аутентификационной информации запрашивается у пользователя снова и сравнивается с хранящимся в системе эталоном. Если образец схож с эталоном с заданной точностью, то пользователь считается узнанным, в противном случае пользователь будет считаться чужим, результатом чего будет, скажем, отказ в доступе на компьютер.

Для аутентификации пользователя компьютер должен хранить некую таблицу имен пользователей и соответствующих им эталонов. В любом случае функция вычисления эталона из аутентификационной информации должна быть однонаправленной, т. е. легко рассчитываться, но представлять собой вычислительную проблему при попытке вычисления в обратном направлении.

ОЦЕНКА ВОЗМОЖНОСТИ АВТОМАТИЗАЦИИ МЕТОДОВ ЗАПУТЫВАЮЩИХ ПРЕОБРАЗОВАНИЙ

О.О. Шевцова, аспирант каф. КИБЭВС
Д.Н. Буинцев, к.т.н., инженер каф. КИБЭВС
ТУСУР, г. Томск, 513-600, studprof@tusur.ru

Метод защиты программного обеспечения при помощи запутывания программ является одним из основных и самых надежных среди способов физической защиты ПО. Обычно пытаются запутать сам код программы. Такие подходы в реализации различных видов преобразо-

ваний малоэффективны по отдельности. Необходимо осуществлять комплексное запутывание, используя реализацию всех преобразований в различном объеме для более эффективного запутывания с минимальным снижением работоспособности программы [2]. Процесс автоматизации при этом сводиться в большей степени к автоматизации графа потока управления. Реализовать такой алгоритм в настоящее время является довольно трудоемкой задачей.

Таким образом, задача автоматизации процесса запутывания сводится к автоматизации применений отдельных видов автоматизации на различных этапах перевода семантики программы в машинный код и его исполнение.

На рисунке представлены обобщенные этапы трансляции программы.

Некоторые запутывающие преобразования могут применяться на различных этапах транслятора.

Предварительный анализ методов запутывания показал, что наиболее эффективным методом является семантическое запутывание на этапе составления графа потока управления и его разрушения.

Этапы трансляции программы

Был проведен эксперименты по частичной автоматизации процесса запутывания. Рассмотрим преобразования потока управления на примере развертки циклов.

Для предварительного анализа защищенности программы с помощью этого метода предлагается рассмотреть некоторые действия, которые может совершать противник в отношении к данному программному продукту [1]:

– локальное внесение изменений;

– глобальное внесение изменений;

– обратная обработка, т.е. алгоритмическое понимание.

Кроме того, необходимо рассматривать противников в зависимости от того, какие инструменты они могут использовать и какими знаниями обладают. В связи с этим также можно рассмотреть, как противник

сможет наблюдать за действиями программы и какие изменения может вносить. Необходимо достижение уровня, на котором противник сможет совершить взлом программы и скопировать интеллектуальную часть кода программы, что потребует еще больше времени и будет соизмеримо или больше, чем написать собственный.

Таблица 1

Анализ возможности автоматизации процесса запутывания на этапе трансляции

Преобразования	Этап трансляции	Режим
Преобразования форматирования (лексические), которые изменяют только внешний вид программы.	Лексический анализатор	Автоматический
Преобразования структур данных, изменяющие структуру данных, с которыми работает программа.	Лексический анализатор	Автоматизированный
	Синтаксический анализатор	Автоматизированный
Преобразования потока управления, которые изменяют структуру графа потока управления программ.	Лексический анализатор	Автоматизированный
	Синтаксический анализатор	Автоматизированный
	Генерация машинного кода	Автоматизированный
Превентивные преобразования, нацелены против методов декомпиляции программ	Нет	Нет

Таблица 2

Автоматизация развертки циклов во время трансляции

	Этап трансляции	Действие	Режим
Преобразование потока управления	Лексический анализатор	Оценка количества выполняемых циклов и формирование нового типа циклов (либо избавление от цикла)	Автоматизированный
	Синтаксический анализатор	Прямое разворачивание цикла (перевод в линейный код, либо добавление условий)	Автоматизированный
	Генерация машинного кода	Формирование разнотипных машинных команд, заменяющих различные циклы	Автоматизированный

Заключение. В результате оценки возможности автоматизации методов запутывающих преобразований выявлено, что не все преобразования можно провести в автоматическом режиме. Предложен метод запутывания не только самого кода программы, а запутывания интерпретации программы. Таким образом, используя данный метод, можно повысить доверие к среде вычислительной системы, в которой выполняется программа.

ЛИТЕРАТУРА

1. *Симонова А.* Среда для запутанного интерпретирования (исполнения) программ. А. Аязян. // Обфускация программ: обзор, 2005. С. 17–20.

2. *Буинцев Д.Н.* Метод защиты программных средств на основе запутывающих преобразований. Диссертационная работа. 2006.

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛОВ TCP И UDP ДЛЯ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ ПО SSL-VPN ТУННЕЛЯМ

В.В. Шейда, аспирант ТУСУР

Эффективность ведения бизнеса современного предприятия зависит от возможности его сотрудников получать доступ к информационным ресурсам компании и от способности сотрудников передавать данные в компанию в любой момент времени, находясь в любой точке планеты.

Однако открытие ресурсов во вне приведет к тому, что они станут доступны не только сотрудникам компании, но и конкурентам. Поддержка модемного пула – достаточно дорогостоящее решение, так как, помимо затрат на оборудование, оно предполагает непосредственно оплату телефонных звонков, вместе с тем также возникают вопросы, касающиеся безопасности.

Альтернативное решение – это использование VPN-технологии, так как при обеспечении высокого уровня безопасности эта технология является наименее дорогостоящей и не вызывает сложностей в применении у конечных пользователей.

VPN-технология, помимо защищенного удаленного доступа для сотрудников, позволяет предприятиям объединять сети территориально разнесенных филиалов и организовывать защищенные видео- и аудиоконференции через Интернет.

На данный момент существует множество VPN-решений, однако, в связи с тем, что часто для обеспечения дополнительной безопасности системные администраторы корпоративных сетей закрывают все порты, кроме 80 и 443, использовать многие из них не представляется возмож-

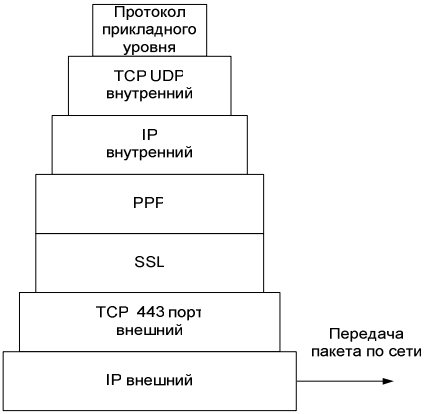
ным. Вместо этого используют SSL-VPN, для работы которого необходим только 443-й порт.

Очень важно обеспечить быструю и надежную работу VPN-сетей, так как от этого зависит оперативность информационного обмена между филиалами предприятия и его сотрудниками.

SSL-VPN обладает рядом недостатков, обусловленных используемыми протоколами, которые ограничивают применение SSL-VPN при передаче потокового вещания [1–3].

Целью работы является анализ технологии SSL-VPN и предложение оптимального решения для обеспечения наилучшей производительности.

Полный стэк протоколов, используемый в SSL-VPN, выглядит следующим образом.



Стандартный стек протоколов, применяемый в SSL

Существуют две основные проблемы такой реализации – «эффект таяния трафика» и трансопртировка UDP поверх TCP.

Протокол TCP – протокол с гарантированной доставкой сообщений. Это значит, что если пакет, содержащий некоторое сообщение, не был доставлен, то он будет поставлен в очередь для повторной отправки и отослан по истечению определенного интервала времени (retransmission timeout – тайм-аут повторной передачи). Если по какой-то причине пакет снова не был доставлен, то TCP использует механизм увеличения тайм-аута повторной передачи, т.е. времени перед следующей повторной отправкой пакета. Это было сделано, для того чтобы учесть возникшие в сети задержки или просто дать пакету, который по какой-то причине пошел по неоптимальному маршруту, больше времени чтобы дойти до получателя.

Однако при использовании протокола TCP поверх TCP увеличение тайм-аута повторной передачи внешнего TCP приводит к тому, что внутренний TCP не получает вовремя подтверждения о доставки пакета TCP, посланного по корпоративной сети, и начинает увеличивать свои тайм-ауты. Это приводит к лавинообразному увеличению суммарных задержек, т.е. снижению скорости передачи – «эффект таяния трафика».

Еще одна проблема, связанная с наличием у TCP механизма повторной передачи, возникает при транспортировке UDP-трафика, например, видео- или аудиоинформации.

В случае туннелирования UDP поверх TCP внешний TCP, если пакет не был доставлен, возобновит передачу этого пакета. Следовательно, пакеты, следующие за ним, вынуждены ждать, пока потерянный пакет будет доставлен, что приводит к большим задержкам потокового вещания. Если еще принять во внимание механизм увеличения тайм-аута повторной передачи, то задержки при передаче потоковой информации становятся абсолютно неприемлемыми.

Для решения вышеописанных проблем необходимо использовать оба протокола UDP и TCP. Выбор конкретного протокола зависит от типа туннелируемого трафика. В случае передачи TCP-данных в качестве внешнего транспортного протокола необходимо использовать TCP-протокол, а при передаче UDP-трафика – UDP. Информация об используемом внутреннем транспортном протоколе может быть получена из специального поля IP-заголовка внутреннего IP-пакета. Для гарантированного обмена ключами и установки SSL сессии необходимо использовать TCP-протокол. Для корректной расшифровки данных на стороне получателя в режиме Cipher Block Chaining (CBS) при туннелировании по UDP необходимо формировать IP-пакеты таким образом, чтобы зашифрованная информация, передаваемая в одном IP-пакете, не зависела от последующих посылок, тогда при потере одного или более IP-пакетов данные смогут быть расшифрованы [4].

ЛИТЕРАТУРА

1. *Мэтью Н., Стоунс Р.* Linux Programming – Wiley Publishing, Inc. 2004. 891 с.

2. *Семенов Ю.А.* Протоколы и ресурсы Internet M/: Радиосвязь, 1996.

3. *Сэтчел Стефен Т., Клиффорд Х.Б. Дж.* Linux IP Stacks в комментариях/Пер. с англ. К.: ДиаСофт, 2001. 288 с.

4. *Хетч Б., Колесников О.* Linux: Создание виртуальных частных сетей (VPN)/Пер. с англ. М.: КУДИЦ-ОБРАЗ, 2004. 464 с.

ОБЗОР ПРОГРАММНЫХ СРЕДСТВ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Р.В. Силиненко, студент 4 курса, ФВС

Целью статьи является обзор основных программных средств обнаружения вторжений в соответствии с классификацией, опубликованной в статье «Классификация систем обнаружения вторжений».

HIDS[2]

1. Dragon Squire

Dragon Squire – это система мониторинга системных журналов реального времени. Программа также производит наблюдение за важными системными файлами на предмет их изменения, мониторинг журналов брандмауэра, маршрутизаторов, Dragon Squire имеет в своем распоряжении базу данных сигнатур, с огромным количеством записей для широкого круга операционных систем. Программа может выступать в роли агента, если на предприятии запущена NIDS серии Dragon Sensor.

Из дополнительных преимуществ выделяется оптимизация работы с целью минимально увеличить нагрузку на защищаемую машину.

2. EMERALD eXpert-BSM™

Высокоуровневая, ориентированная на производительность система анализа, основанная на базе данных сигнатур eXpert (читается И-эксперт) – это одна из трех аналитических платформ, используемая в целом спектре компонентов обнаружения вторжений, начинающемся с простых систем обнаружения злоупотреблений на пользовательском уровне и, заканчивающемся основанными на TCP/IP распределенными сетевыми сенсорами. Система eXpert является системой реального времени, применяется на критичных серверах и рабочих станциях. В программу входят система сбора данных, анализ вторжений, управление оповещением, подробные директивы по ответным действиям.

– KFSensor

IDS-ловушка для Windows-платформ, KFSensor действуют как мышеловка, для того чтобы привлечь к себе внимание злоумышленников и червей, симулируя различные виды уязвимостей. Действуя как сервер-приманка, KFSensor отклоняет внимание злоумышленников от критически важных узлов сети, предоставляя вместе с тем более подробную информацию, чем брандмауэры. К плюсам программы относится ее поддержка баз данных сигнатур программы Snort.

1. NFR-HID

Предоставляет всестороннюю защиту серверов и рабочих станций. Предоставляет такие сервисы, как оценка уязвимости, анализ журналов,

[2] Host based Intrusion Detection System.

управление политикой безопасности, мониторинг вторжений. Предоставляет быстрое развертывание, настройку, и малотребователен ко времени обслуживания.

NIDS[3]

1. CISCO Secure IDS

IDS реального времени, основанная на базах данных сигнатур, состоит из двух основных частей – сенсоров и управляющей платформы. Сенсоры проводят мониторинг сети, а управляющая платформа предоставляет удобный графический интерфейс для управления всей системой отображения сообщений генерируемых сенсорами.

2. Dragon Sensor

Вместе с базами данных сигнатур данная IDS поддерживает анализ трафика на основе правил, базирующихся на политике безопасности, что позволяет выявлять новые, нестандартные атаки. Dragon Sensor (в отличие от большинства других NIDS, концентрирующих свое внимание на атаке или сканировании) может собирать достаточно информации, для того чтобы дать ответ на вопрос об успешности атаки. Эта возможность позволяет исключить ложные срабатывания и предоставить общую картину происходящего, что является большим плюсом в работе IDS. Dragon Sensor также ориентирован на максимальную производительность при минимальных затратах ресурсов.

3. Snort

Легенда в мире IDS-технологий, ставшая де-факто стандартом в обнаружении и предупреждении вторжений. Snort – это бесплатная программа с широкими возможностями, среди которых – журналирование пакетов, анализ трафика в реальном времени, анализ протоколов. Поиск сигнатур в пакетах может быть использован для обнаружения многих атак, таких как переполнение буфера, сканирование портов, CGI-атаки, определение установленной ОС. Snort независим от платформы. На основе Snort строятся более сложные программно-аппаратные системы, например Sourcefire Intrusion Sensor.

4. FireStorm

Высокопроизводительная NIDS, распространяющаяся по лицензии GPL, что является несомненным преимуществом в сравнении с коммерческими системами, стоимость которых иногда достигает более десятка тысяч долларов. Из основных характеристик можно выделить полную совместимость с правилами анализа Snort, систему обнаружения аномалий трафика, поддержку анализа более десятка сетевых протоколов, обработку трафика в реальном времени, не влияя на пропускную способность сети.

□

[3] Network based Intrusion Detection System

Hybrid IDS

5. Prelude

Гибридная IDS (т.е. сочетающая в себе возможности NIDS и HID), позволяющая объединить все приложения для защиты информации в одну централизованную систему. Для этого Prelude использует IDMEF-протокол обмена сообщениями, разработанный специально для систем обнаружения вторжений. Данная программа может объединять множество программ разных платформ, анализировать до тридцати типов файлов журналов [1–6].

В заключение следует отметить, что приведенные программные средства, являются лишь небольшой частью представленных на рынке систем IDS. Некоторые из приведенных программ используются для построения еще более сложных комплексов, включающих в себя наряду с программами аппаратную составляющую в виде маршрутизаторов, брандмауэров, управляемых свитчей.

ЛИТЕРАТУРА

1. www.prelude-ids.org
2. www.windowsecurity.com
3. www.securityfocus.com
4. www.informit.com
5. www.securitysolutions.com
6. www.sri.com

РАЗРАБОТКА ПОЛИТИКИ СЕТЕВОЙ БЕЗОПАСНОСТИ ДЛЯ ПРЕДПРИЯТИЯ

Д.А. Соломатов, студент группы 522-2
ТУСУР, г. Томск

Для разработки политики безопасности, помимо профессионального опыта, знания нормативной базы в области информационной безопасности, необходимо также учитывать основные факторы, влияющие на эффективность политики безопасности, и следовать основным принципам разработки ПБ, к числу которых относятся минимизация влияния на производительность труда, непрерывность обучения, контроль и реагирование на нарушения безопасности, поддержка руководства организации и постоянное совершенствование ПБ.

Разработка сетевой политики безопасности является частью общей политики безопасности предприятия.

На основании результатов аудита безопасности были определены основные условия, требования и базовая система мер по обеспечению

ИБ на предприятии, позволяющие уменьшить риски до приемлемой величины.

Разработка политики сетевой безопасности проводилась на основе стандарта ISO 17799, требований предприятия и других нормативно-правовых документов. В результате были написаны общие положения, инструкции по работе в сети.

Разработанная политика состоит из двух частей – общих принципов и конкретных правил работы.

Общие принципы определяют подход к безопасности в сети (это общее описание организации сетевой, локальной и физической безопасности).

Правила же определяют, что разрешено, а что – запрещено (это, например, правила парольной защиты, правила защиты от вирусов и злонамеренного ПО, правила осуществления удаленного доступа и т.д.). Правила дополняются конкретными процедурами и различными руководствами.

В сферу действия политики попадают все программные, аппаратные и информационные ресурсы, входящие в локальную сеть предприятия, которая ориентирована на пользователей, работающих с сетью.

Для того чтобы ПБ оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах ИБ и обучать их выполнению правил, предписываемых ПБ. Регулярный пересмотр и корректировка правил ПБ необходимы для поддержания ее в актуальном состоянии.

ОС LINUX КАК ОБЪЕКТ И ИНСТРУМЕНТ СУДЕБНОЙ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ

В.Н. Свердлова, А.С. Романов, студенты 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-906-199-90-95, vlada@ms.tusur.ru.

В настоящее время все более популярным среди пользователей ПК становится открытое программное обеспечение. Если до недавнего времени прерогативой таких операционных систем, как Linux или FreeBSD, были различные серверные станции, то с развитием графического пользовательского интерфейса X-Window эти операционные системы нашли свое распространение и на локальных машинах отдельных пользователей. Развитие POSIX-совместимых ОС, в частности Linux, вполне оправданно: они бесплатны, надежны и представляют собой гибкий инструмент в руках опытного пользователя.

Тем не менее в отечественных экспертно-криминалистических подразделениях не хватает достаточно квалифицированных специалистов в области операционных систем, альтернативных Windows. Программа обучения экспертов по направлению «Исследование компьютерной информации» также практически не затрагивает этих вопросов. Таким образом, все больше повышается актуальность создания методик криминалистического исследования Linux.

Очевидно, что тот инструментарий, который используется для исследования Windows (кроме достаточно дорогих специализированных программных комплексов), не подходит для Linux. Но здесь инструментом исследования может выступать сама операционная система. В этом плане Linux имеет следующие возможности:

– поддержка большого числа файловых систем (ext2fs, ext3fs, VFAT, FAT, ISO9660, NTFS, UFS, NFS и др.);

– штатные средства создания образа носителя, поиска, восстановления, хэширования данных;

– возможность манипулировать носителями как файлами, устанавливать разные режимы монтирования;

– возможность монтировать образ носителя как файловую систему;

– возможность исследования работающей системы с использованием live CD или специально сформированного диска с необходимым инструментарием[1].

Кроме того, основная масса существующих специализированных комплексов для криминалистического исследования Linux (The Coroners Toolkit, TSK&Autopsy) и различных полезных утилит также является открытым программным обеспечением и распространяется бесплатно. Отсюда явное преимущество исследования Linux в среде этой же операционной системы, ведь тогда появляется возможность использовать бесплатные и эффективные именно для этой системы инструменты, работу которых можно проанализировать на основе открытого исходного кода.

Однако не все утилиты, предназначенные для поиска или восстановления данных, подходят для экспертов. Поэтому встает вопрос о таком наборе инструментов, который позволял бы с максимальной эффективностью решать эти тривиальные задачи.

Рассмотрим задачу восстановления данных.

Приведем данные по результатам испытаний программ восстановления данных на файловых системах ext2fs и ext3fs. Для сравнительного анализа были выбраны foremost, TSK&Autopsy, R-Stidio (как платный аналог для Windows). Для проверки работы программ был выделен отформатированный раздел размером 1 Гб. С разделом осуществлялись следующие действия.

1. Форматирование в файловой системе ext3fs.

2. Запись и последующее удаление некоторого количества файлов, большинство из которых находилось в каталоге DELETED, 5 файлов – отдельно в корне. Для удаления использовалась команда $ rm –rf <directory>.

3. Создание образа раздела с помощью утилиты dd.

4. Восстановление данных тремя разными программами.

5. То же самое для файловой системы ext2fs.

Результаты испытаний приведены на рисунке 1.

Рассмотрим подробнее результаты работы foremost. По результатам испытания можно сделать вывод, что foremost – одна из наиболее эффективных программ для восстановления данных в файловых системах ext2fs и ext3fs. Htm-страницы и .rar-архивы восстанавливаются полностью. Была восстановлена половина удаленных документов формата MSWord. Несколько некорректно происходит восстановление графических файлов. Кроме того, можно задавать параметры восстановления, и результаты выдаются в удобном виде – файлы рассортированы по папкам. Генерируемый программой файл аудита восстановления можно включать в отчет об экспертизе.

Результаты, полученные R-Studio для файловой системы ext2fs, возможно анализировать только в среде Linux. Отличное качество восстановления графических файлов (формата .gif). Htm– страницы тоже восстанавливаются, но не все из числа удаленных. В целом восстановление файлов менее эффективное, нежели у foremost, учитывая тот факт, что в ext3fs R-Studio восстанавливает только имена и атрибуты файлов. Тем не менее, программа может быть полезна для исследования в комплексе с другими инструментами.

В разрабатываемых методиках должны быть описаны принципы решения и подходящий инструментарий для каждой определенной исследовательской задачи. При этом использование Linux в качестве среды исследования дает не только вышеописанные преимущества, но и формирует мышление эксперта, способствуя лучшему пониманию устройства исследуемой системы.

ЛИТЕРАТУРА

1. *Thomas Rude*, CISSP. Next Generation Data Forensics & Linux // www.e-evidence.info

СИСТЕМА ТЕСТИРОВАНИЯ СТУДЕНТОВ И МОДУЛИ ЗАЩИТЫ

А.В. Забелин, студент 5 курса, ФВС КИБЭВС
ТУСУР, г. Томск, ga-fsb@mail.ru

Целью практической работы являются изучение криптографических методов защиты информации, создание клиентского приложения и разработка модулей защиты.

В ходе работы были изучены особенности алгоритмов с открытым ключом, и на основании полученных знаний был программно реализован модуль криптографической защиты баз данных.

Создано насколько приложений, позволяющих создавать и редактировать базы данных вопросника, а также использовать созданные базы данных с целью тестирования студентов:

– Liber TEST (программа для создания баз данных с вопросами и шифрования);

– Tester (непосредственно сам программа которая производит тестирование);

– TESTER.dll (криптографический модуль защиты).

В данный момент разрабатывается модуль защиты от дизассемблера, система контроля целостности баз данных и созданных приложений. Также разрабатываются новые функции и возможности программ: liberTEST, при помощи которой собственно и происходит создание базы данных вопросника, и программы TESTER, при помощи которой происходит тестирование студентов. Планируется, добавление еще нескольких алгоритмов шифрования в модуль защиты TESTER.dll.

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

О.В. Жувагин, студент 4 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-913-102-8042, mave@ctb.rk..tusur.ru

В данной статье описывается классификация компьютерных преступлений в зависимости от способа их совершения. Основные способы совершения компьютерных преступлений можно объединить в три основные группы: методы перехвата, методы несанкционированного доступа и методы манипуляции.

1. Методы перехвата.

Непосредственный перехват осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом

объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи и специальные системы правительственной связи.

Электромагнитный перехват. Перехват информации осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Может осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.

2. Методы несанкционированного доступа.

Метод следования «за дураком». Имеет целью несанкционированное проникновение в пространственные и электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним.

Метод «за хвост». Используя этот метод, можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе.

Метод «неспешного выбора». В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости.

Метод «мистификация». Используется при случайном подключении «чужой» системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

Метод «аварийный». Этот прием основан на использовании того обстоятельства, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ. Такая программа – мощный и опасный инструмент в руках злоумышленника.

Метод «склад без стен». Несанкционированный доступ осуществляется в результате системной поломки, т.е если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных.

3. Методы манипуляции.

Сущность методов манипуляции состоит в **подмене данных**, которая осуществляется, как правило, при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

Манипуляция с пультом управления. Манипуляция с пультом управления относится к злоупотреблению механическими элементами управления ЭВМ. Характеристика манипуляции с вычислительной техникой заключается в том, что в результате механического воздействия на технические средства машины создаются возможности манипуляции данными.

«Троянский конь» – способ, состоящий в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

«Логическая бомба» – тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

«Асинхронная атака» состоит в смешивании команд двух или нескольких пользователей, чьи команды компьютерная система выполняет одновременно.

Реверсивная модель. Существо метода заключается в следующем. Создается модель конкретной системы. В нее вводятся реальные исходные данные, и учитываются планируемые действия. Затем, исходя из полученных правильных результатов, подбираются правдоподобные желательные результаты. Затем модель прогоняется назад, к исходной точке, и становится ясно, какие манипуляции с входными данными нужно проводить. В принципе прокручивание модели «вперед-назад» может проходить не один раз, чтобы через несколько итераций добиться желаемого. После этого остается только осуществить задуманное.

«Воздушный змей». В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз до тех пор, пока на счете не оказывается приличная сумма (фактически, она постоянно «перескакивает» с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и владелец счетов скрывается.

Манипулирование данными осуществляется также и самими руководителями коммерческих структур с целью нанесения ущерба государству.

Заключение. По оценкам отечественных специалистов, уже сейчас хищения с применением компьютерной техники и средств электронного

платежа представляют серьезную угрозу для безопасности России. В ближайшем будущем прогнозируются значительный рост преступности в данной сфере и увеличение ее доли в общем количестве преступлений [1].

В целях борьбы с компьютерной преступностью российским законодательством (глава 28 УК РФ) предусмотрена уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ) [2].

ЛИТЕРАТУРА

1. *Бекряшев А.К.* Экономическая преступность / Теневая экономика и экономическая преступность: Электронный учебник.
< http://newasp.omskreg.ru/bekryash/ >.

2. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (принят ГД ФС РФ 24.05.1996).

ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В.Д. Зыков, студент 5 курса; М.А. Сопов, инженер;
П.А. Мельниченко, аспирант
ТУСУР, г. Томск, zvd@udcs.ru

Эффективная работа современной организации в настоящее время связана с организацией электронного документооборота. Работа с документами в электронной форме позволяет быстро и удобно хранить, обрабатывать и передавать документы в информационной системе организации. Однако электронные документы могут быть потенциально подвержены следующим информационным атакам:

– нарушение конфиденциальности при передаче электронных документов;

– несанкционированное искажение электронных документов;

– отправка ложного электронного документа от имени легального пользователя системы.

При принятии решения об автоматизации делопроизводства организация сталкивается с проблемой выбора системы защищенного электронного документооборота (СЗЭДО), которая смогла бы с наибольшим успехом решать поставленные задачи, противодействовать информационным угрозам и оправдала бы инвестиции на внедрение [1]. Для выбо-

ра СЗЭДО в первую очередь необходимо определить список требований к системе.

Предлагается разделить требования к системам защищенного электронного документооборота на следующие группы и подгруппы:

Эксплуатационные требования:

– возможности для работы с документами,
– стандартизация и автоматизация документооборота,
– организация хранилища документов,
– возможности модификации системы,
– удобство в использовании,

Требования к архитектуре системы:

– масштабируемость,
– распределенность,
– модульность,
– открытость,

Аппаратно-программные требования и требования к сопровождению системы:

– операционная система,
– СУБД,
– зависимость от сторонних продуктов,
– аппаратное обеспечение,
– требования к сопровождению системы,

Требования безопасности:

– идентификация и аутентификация пользователей,
– разграничение прав доступа к документам,
– контроль целостности документов,

Применение технологий электронной цифровой подписи и инфраструктуры отрытых ключей для создания систем защищенного электронного документооборота [2].

Введение в действие Федерального закона от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» позволило рассматривать электронный документ с электронной цифровой подписью (ЭЦП) как аналог традиционного бумажного документа с подписью и печатью.

Для реализации ЭЦП в информационной системе предприятия применяется технология инфраструктуры открытых ключей PKI (Public Key Infrastructure). Эта технология предусматривает возможность использования асимметричных криптографических алгоритмов для защиты информации пользователей на уровне электронных документов. Асимметричное шифрование предполагает наличие двух различных криптографических ключей – открытого и закрытого.

Для обеспечения безопасного обмена открытыми ключами между пользователями системы используются цифровые сертификаты. Сертификат представляет собой структуру данных, которая содержит открытый ключ владельца сертификата и подписана электронной цифровой подписью его издателя. Таким образом, выдавая сертификат, издатель удостоверяет подлинность связи между открытым ключом субъекта и информацией, его идентифицирующей. В качестве издателей сертификатов выступают специальные удостоверяющие центры.

Конфиденциальность документов достигается путем их шифрования, а достоверность и целостность – использованием электронной цифровой подписи (ЭЦП).

В общем виде система защищенного документооборота показана на рисунке.

Система защищенного документооборота

Выводы. В настоящее время при создании систем защищенного электронного документооборота наиболее распространенными компонентами являются технология электронной цифровой подписи и инфраструктура открытых ключей. Данные технологии позволяют существенно повысить оперативность обработки документов и обеспечивают такие важные свойства систем документооборота как неотрекаемость, конфиденциальность и целостность. При этом электронный документооборот при соблюдении условий, определяемых Российским законодательством может быть равнозначным по степени юридической значимости с традиционным бумажным документооборотом [3].

Таким образом, использование инфраструктуры открытых ключей является эффективным комплексным решением ряда важнейших требований к системам защищенного электронного документооборота.

ЛИТЕРАТУРА

1. *Выбор* системы документооборота. Независимый ресурс Всероссийского сообщества CIO, 2003.

2. *Кравец М.А.* Электронные системы управления документооборотом. Воронеж. ИММИФ, 2004.

3. *Пахчанян А.* Обзор систем электронного документооборота // Директор ИС №8, 2001.

ПРОТОКОЛ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ КЛЮЧАМИ ПСЕВДОСЛУЧАЙНОГО ГЕНЕРАТОРА

А.В. Архангельская; С.В. Запечников, к.т.н, доц.

МИФИ, г. Москва, тел. (495) 324-73-34, kaf42@mephi.ru

Современные средства криптографической защиты информации характеризуются высокой стойкостью применяемых в них криптографических алгоритмов, в связи с чем нарушение безопасности средств и систем защиты информации посредством криптоаналитических атак маловероятно. Основными источниками уязвимостей являются слабости методов аутентификации, управления и генерации ключей. В связи с этим становится актуальной проблема разработки методологических основ создания криптосистем, стойких к компрометации части ключей. Один из перспективных путей совершенствования процедур управления ключами связан с применением защищенных криптографических модулей с замкнутым жизненным циклом персональных секретных ключей пользователя. Однако с внедрением таких устройств связана проблема дистанционного выполнения криптографических операций. В целях обеспечения высокой стойкости криптосистем секретные ключи в течение всего своего жизненного цикла не должны покидать пределов защищенного модуля, поэтому для выполнения операций на внешних устройствах могут быть применены лишь производные от них ключи. Авторами поставлена и решена задача проектирования криптографического протокола для дистанционного управления секретными ключами генератора псевдослучайных последовательностей.

Основным критерием качества псевдослучайного генератора считается невозможность за полиномиальное время отличить его выходную последовательность от истинно случайной двоичной строки. Другим желательным свойством криптографически стойкого генератора является совершенная опережающая безопасность, т.е. невозможность при известном состоянии генератора в некоторый момент времени отличить выработанные им ранее выходные последовательности от истинно случайных. Пусть $G:\{0,1\}^k \to \{0,1\}^{b+k}$ – криптографически стойкий псевдо-

случайный генератор. Известен типовой способ преобразования стойкого псевдослучайного генератора G в генератор GEN=<GEN.key, GEN.next>, обладающий свойством совершенной опережающей безопасности [1]. Для этого конструируются алгоритм ввода ключа генератора GEN.key $\{ s \leftarrow \{0,1\}^k$; Return s$\}$ и алгоритм очередного шага работы генератора GEN.next(St_{i-1}) $\{ r \leftarrow G(St_{i-1})$; Return $Out_i = [r]_{1\ldots b}$, $St_i = [r]_{b+1\ldots b+k}$ $\}$. Здесь St_{i-1} – входной ключ для *i*-го шага работы генератора; Out_i – выходная последовательность на *i*-м шаге; St_i – часть выходной последовательности, полученной на *i*-м шаге, которая служит ключом для следующего шага. В то же время для такого генератора остается возможным при известном его состоянии в некоторый момент времени отличить выработанные позднее выходные последовательности от истинно случайных.

Пусть *T* – защищенное устройство, обладающее памятью для хранения секретных ключей и аппаратно реализующее некоторые криптографические алгоритмы (например, смарт-карта). Однако объем памяти и производительность криптографического сопроцессора смарт-карты существенно ограничены, поэтому другие криптографические операции выполняются на внешних по отношению к смарт-карте устройствах, например, программно реализуются на компьютере, к которому присоединяется считыватель смарт-карт.

Один из способов выполнения криптографических операций на внешних устройствах без вывода секретного ключа за пределы *T* заключается в применении криптосхем с изоляцией ключа [2, 3]. Такие схемы предназначаются для асимметричных криптосхем главным образом схем цифровой подписи и схем открытого шифрования и отличаются высокой сложностью. В рассматриваемой задаче необходимости применения асимметричных криптосхем нет, поэтому в предлагаемом ниже протоколе можно воспользоваться более простой схемой управления ключами. Идея этой схемы весьма близка к методу Лампорта аутентификации по одноразовым паролям [4], но используется для других целей.

Пусть *K* – секретный ключ псевдослучайного генератора, который хранится в защищенном криптографическом модуле *T;* $y = f(x)$ – однонаправленная функция, описание которой общеизвестно, например, функция вида $y = E_x(M_0)$, где *E* – криптографически стойкий блочный шифр, например, ГОСТ 28147-89. Перед началом работы схемы выбирается параметр *t* – количество периодов, на которые разбивается время работы схемы, и определяется продолжительность каждого периода.

Полагают $s_0 = K$, после чего вычисляется последовательность значений $s_i = f(s_{i-1})$ для всех $i = 1,2,...,t$. Последний элемент вычисленной цепочки s_t вводится в псевдослучайный генератор со свойством совершенной опережающей безопасности GEN=<GEN.key, GEN.next> в качестве его начального ключа St_0. После этого начинается 1-й период работы схемы. Далее для генерации очередного отрезка псевдослучайной двоичной последовательности применяется алгоритм GEN.next, но при окончании каждого периода времени работы схемы выполняется специальный протокол модификации ключа псевдослучайного генератора.

В конце каждого *i*-го периода времени защищенное устройство *T* пересылает программному модулю, реализующему псевдослучайный генератор, величину $s_{t-i}, i = \overline{1,t-1}$. Программа осуществляет проверку $f(s_{t-i}) \stackrel{?}{=} s_{t-i+1}$. В случае выполнения равенства старое значение s_{t-i+1} уничтожается, после чего вычисляется новый ключ генератора $St_{i-1} := St_{i-1} \oplus s_{t-i}$. Далее для выработки очередных фрагментов псевдослучайной последовательности запускается алгоритм GEN.next до тех пор, пока не завершится *i*-й период времени работы схемы.

Если в течение *i*-го периода времени секретный ключ St_{i-1} станет известен противнику, вычислить псевдослучайные последовательности, полученные генератором с 1-го по (i-1)-й период времени, он не может в силу свойства совершенной опережающей безопасности, а вычислить последовательности, которые будут получены с (*i*+1)-го по *t*-й периоды времени он также не может, так как для этого ему пришлось бы научиться обращать однонаправленную функцию, что является вычислительно сложной задачей. Таким образом, предложенный протокол дистанционного управления ключами псевдослучайного генератора позволяет добиться усиления его криптографической стойкости.

ЛИТЕРАТУРА

1. *Bellare M., Yee B.* Forward security in private-key cryptography – http://eprint.iacr.org/2001/035.

2. *Dodis Y., Katz J., Xu S., Yung M.* Key-insulated public key cryptosystems // Adv. in cryptology – Proc. of Eurocrypt'2002, LNCS Vol. 2332, Springer-Verlag, 2002. Pp. 65–82.

3. *Dodis Y., Katz J., Xu S., Yung M.* Strong key-insulated signature schemes // Adv. in cryptology – Proc. of PKC'2003, LNCS Vol. 2567, Springer-Verlag, 2003. P. 130–144.

4. *Lamport L.* Password authentication with insecure communication // Communications of the ACM. 1981. No. 24. P. 770–772.

ПРОБЛЕМЫ РЕАЛИЗАЦИИ RSA В СРЕДЕ BORLAND DELPHI 7. ФУНКЦИЯ ШИФРОВАНИЯ.

Д.Т. Ибатулин, М.С. Касьянов, студенты 4 курса
ОГАУ, г. Оренбург, т. (3532)72-40-52, asoi@mail.ru

При создании программы, реализующей работу данной шифрсистемы, были обнаружены некоторые трудности. Для шифрования текста в RSA используется следующий принцип: $C = M^e \pmod n$, где M – блок открытого текста; C – соответствующий блок шифрованного текста. При использовании компонентов ключа, удовлетворяющих условиям криптостойкости, становится невозможным вычисление данного выражения в связи с тем, что значение M^e выходит за рамки разрядной сетки, с которой работает среда Borland Delphi 7. Это не позволяет использовать штатную функцию Delphi из модуля Math для вычисления степени числа – IntPower. Для решения этой проблемы предлагается следующий алгоритм проведения расчетов: степень, в которую возводится число необходимо разложить на сумму степеней двойки и воспользоваться правилом, что $M^e \pmod n = ((M^a \pmod n)*(M^b \pmod n))\pmod n$, где $e = a + b$. Данный алгоритм был взят за основу при написании программного кода собственной функции, осуществляющей вычисление значения выражения $C = M^e \pmod n$.

```
function Modul(m, ed, n: integer): integer;
var
  m0, j:                          integer;
  m1, m_1, a, i, ced:   real;
begin
  ced:= ed;
  j:=1;
  m_1:= m mod n;
  a:= 1;
  repeat
    repeat
      m0:= 1 shl j ;
      m1:= round(sqr(m_1)) mod n;
      m_1:= m1;
      a:= round(a*m1) mod n;
      ced:= ced - m0;
      inc(j);
    until  1 shl j > ced;
    m_1:= m mod n;
    j:= 1;
```

```
  until ced <= 1;
  If ced = 1 then a:= round(a * m) mod n;
  result:= round(a);
end;
```

В функцию передаются 3 параметра *m*, *ed* и *n*, возвращаемый результат соответствует значению выражения $m^{ed} \pmod{n}$.

При написании данного программного кода были обнаружены и устранены еще 2 трудности: искажение результатов вычислений при работе с достаточно большими числами и относительно низкая скорость работы.

Первая проблема обусловлена особенностями работы среды Borland Delphi 7 с большими целыми числами (тип integer). Решение связано с переводом части используемых переменных в тип real.

Вторая проблема стала результатом использования функции для вычисления степени числа – IntPower. Так как данная функция использовалась для возведения в степень числа 2, то было принято решение заменить её функцией shl, осуществляющей сдвиг двоичных порядков влево, т.е. умножение числа на 2 в определенной степени, в результате чего скорость возросла в полтора раза. Полученный прирост скорости позволил отказаться от дальнейшей оптимизации кода. Кроме того, это решение позволило избавиться от зависимости функции от модуля Math.

Таким образом, можно сделать вывод об актуальности данной работы в связи с ее направленностью на устранение основного недостатка самой распространенной асимметричной шифрсистемы RSA – низкой скорости шифрования [1].

ЛИТЕРАТУРА

1. *Л.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин.* Основы криптографии. М.: Гелиос АРВ, 2001.

ТРАНСПОРТНЫЕ ПОДСИСТЕМЫ НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ ПРОГРАММНЫХ КОМПЛЕКСОВ ПРЕДОСТАВЛЕНИЯ ОТЧЕТНОСТИ НА ТЕРРИТОРИИ РФ

П. А. Мельниченко, аспирант каф. КИБЭВС, ТУСУР
г. Томск, mpa@udcs.ru

В Российской Федерации наиболее распространенными и широко используемыми системами передачи конфиденциальной информации являются системы сдачи налоговой и пенсионной отчетности. Для того,

чтобы разработанная кем-либо система могла использоваться для данной цели, она должна пройти тестирование и сертификацию в ГНИВЦ ФНС РФ – для налоговых органов – и в ПФР – для пенсионного фонда.

Данные системы подвергаются детальному тестированию на наличие уязвимостей и возможностей перехвата и модификации конфиденциальной информации. К этим системам предъявляется требование наличия такого элемента, как специализированный оператор связи, на который возлагается роль третьей стороны при разрешении конфликтных ситуаций при возникновении разногласий между налогоплательщиком и налоговыми органами.

Специализированный оператор выполняет также и транспортную функцию в данной системе. Другими словами, этот элемент системы должен иметь сервер для приема и временного хранения передаваемых сообщений, генерировать подтверждения приема сообщений и отвечать требованию доступности.

1. Технология фирмы «Taxcom»

Технология передачи налоговой отчетности, разработанная фирмой «Taxcom», использует в качестве транспортной составляющей сервер «ДИОНИС», разработанный НПП «Фактор-ТС». В качестве клиентской программы используется клиент защищенной электронной почты DiPost, разработан также НПП «Фактор-ТС». По открытым каналам связи информация передается в зашифрованном виде с контролем целостности. Шифрование и проставление ЭЦП производятся программой DiPost в соответствие с алгоритмами, стандартизированными в Российской Федерации. Формирование подтверждений осуществляет отдельное программное обеспечение – X-Monitor, на основе логов сервера «Дионис».

Из плюсов данной организации обмена конфиденциальной информацией можно выделить модульность системы и возможность замены ее отдельных частей, таких как сервер, клиентская часть и ПО для формирования подтверждений оператора связи.

Но данная технология обладает всеми минусами обычной электронной почты, описанными выше, так как сервер работает по протоколам SMTP и POP3 с возможностью переключения на собственный протокол, который сохраняет свойства предыдущих.

Так же в связке DiPost – «Дионис» не проработан механизм аутентификации клиента на сервере. Это дает возможность злоумышленнику как собрать большое количество косвенной информации о документообороте внутри системы (количество передаваемой информации от каждого абонента, время передачи конвертов, отправитель и получатель конвертов), так и вывести из строя или нарушить работу почтового сервера.

Это возможно из-за того, что передача информации для аутентификации клиента передается стороне сервера в открытом (незашифрованном) виде, т.е. возможен перехват данной информации злоумышленником с дальнейшим ее использованием для аутентификации на сервере. Это, в свою очередь, может нарушить регламент обмена сообщениями, привести к потере передаваемой информации и так далее. Причем при возникновении подобной ситуации, скорее всего, дискредитированным будет именно абонент системы, так как с точки зрения сервера и программы, отвечающей за выработку подтверждений, сообщения будут доставлены без ошибок.

Снижение уровня угрозы данной уязвимости могло бы быть достигнуто привязкой каждого конкретного клиента к статичному ip-адресу или другому идентификатору, но сделать этого не позволяет сервер «ДИОНИС». Тем не менее факт подключения абонента с определенными данными для аутентификации возможно зафиксировать по логам сервера «ДИОНИС». Но это обстоятельство ничего не меняет с точки зрения соблюдения регламента.

2. Технология фирмы «Комита»

В системе «Комита-отчет» для обмена сообщениями между налогоплательщиками, кредитными организациями и налоговыми органами используется специализированный сервер, использующий транспортный протокол близкий к стандартным SMTP/POP3.

Однако сервер реализован практически с «нуля» для решения специфических задач организации электронного документооборота под требования налоговых органов.

К особенностям сервера обмена документами относятся:

1. Обмен документами между сервером и рабочими местами (АРМ Налогоплательщика, АРМ инспекции, АРМ банковские счета) осуществляется напрямую. Использование транзитных серверов допустимо (при соблюдении ряда условий), но не рекомендуется.
2. Инициатором обмена может выступать только рабочее место (в режиме оператора или в автоматическом режиме).
3. Все документы, которые были отправлены/получены с использованием сервера хранятся в архиве сообщений.
4. Все сообщения (за исключением сообщений об ошибках шифрования/расшифровывания) передаются только в зашифрованном виде.
5. Квитанции специализированного оператора связи формируются сервером в режиме реального времени.

Экземпляр системы «Комита-отчет», развернутый в Санкт-Петербурге, показывает следующие результаты (по данным приема отчетности 19–20 июня 2006 г.):

1. Время после отправки отчета, через которое квитанция специализированного оператора связи становится доступной для загрузки налогоплательщиком/налоговым органом – 1 мин.

2. Период опроса сервера обмена документами приемным рабочим местом налогового органа 2 мин.

3. Время после отправки отчета, через которое квитанции налогового органа становится доступной для загрузки налогоплательщиком 5–7 мин в зависимости от загрузки сервера;

4. Время, после отправки отчета, через которое протокол входного контроля становится доступен для загрузки налогоплательщиком – 8–15 мин, в зависимости от загрузки сервера.

5. Общее число отправленных документов за 48 ч больше 2400 файлов отчетности (не считая неформализованные сообщения, сообщения кредитных организаций и т.д.).

Как поясняют авторы, протоколы, близкие к стандартным SMTP/POP3, – это те же протоколы только с ограниченным набором функций.

Возможности серверной части системы «Комита-отчет» и ее описание позволяют сделать вывод, что транспортная подсистема представляет собой специализированный почтовый сервер, основной отличительной особенностью которого является возможность формирования подтверждений. Плюсом данной технологии является только совместимость со всеми клиентами электронной почты. Минусы использования сервера электронной почты описаны выше.

Тем не менее транспортная подсистема системы «Комита-отчет» является высоко производительной в сравнении с технологией фирмы «Taxcom». Так как непосредственно сами разработки недоступны для проведения анализа, то можно только предположить, что производительность достигнута путем оптимизации системы под задачи быстрого транспорта сообщений без использования транзитных серверов.

3. Технологии фирмы «Калуга-Астрал» и фирмы «Тензор»

Эти две технологии схожи по организации транспортной подсистемы. В обеих технологиях в качестве серверной части используется почтовый сервер. Отличие состоит только в криптографической защите передаваемых данных.

В технологии «Калуга-Астрал» используется криптопровайдер фирмы «InfoTecs» – «ДоменК», тогда как в технологии «Тензор» используется самый распространенный на территории Российской Федерации криптопровайдер «КриптоПро» версии 2.0 (по данным на сентябрь 2006 г.).

В ходе анализа технологии «Тензор» выявлены те же недостатки, что и остальных технологий на базе почтовых серверов. Эти недостатки

описаны выше. К тому же выявлен еще один недостаток, связанный с распознаванием внутрисистемных сообщений.

Дело в том, что данная технология жестко привязана к стандартам электронной почты и использует в качестве идентификационной информации для зашифрованного сообщения заголовки конверта электронной почты, т.е. распознавание сообщения системой ведется по полям конверта. При наличии каких-либо нерегламентированных полей заголовка или отсутствии требуемых полей сообщение считается не принадлежащим регламентированному документообороту. Это, в свою очередь, является препятствием масштабируетмости системы, так как почтовые серверы для фиксации маршрута прохождения сообщения добавляют в конверт заголовки, идентифицирующие каждый почтовый сервер-ретранслятор в цепи передачи сообщения. Отсутствие данной информации возможно, но не желательно, а наличие является фактором, который влияет на распознавание сообщения системой.

Таким образом, в данной системе проблемно использование промежуточных серверов-ретрансляторов для передачи сообщений. Как следствие этого требуется наличие прямого подключения к серверу электронной почты системы у клиента для возможности участия в электронном документообороте. А использование протоколов SMPT/POP3 является небезопасным вследствие их спецификации, согласно которой информация для аутентификации пользователей передается в открытом виде по открытым каналам связи.

4. «Служба гарантированной доставки» от СКБ «Контур»

«Служба Гарантированной Доставки» (СГД) – собственная разработка СКБ «Контур». Она представляет собой протокол обмена сообщениями, реализованный над протоколом HTTPS, т.е. шифрование передаваемой информации осуществляется на более низком уровне, что позволяет скрыть служебную информацию протокола.

Данный протокол соответствует следующим требованиям:

– архивирование передаваемых сообщений;

– шифрование циркулирующей информации;

– инициализация информационного обмена только со стороны клиента;

– автоматическое отслеживание ошибок;

– гарантированность доставки сообщений.

Причем последние 2 пункта выполняются, исходя из свойств протокола.

Исходя из того, что данный протокол реализован над протоколом HTTPS, можно сделать вывод, что он не поддерживает сессионность в чистом виде, так как протокол HTTPS, как и HTTP, не предоставляет

возможность работы по сессиям. Это значит, что каждый последующий запрос является независимым по отношению к предыдущему, что не совсем удобно при необходимости аутентификации при обмене информацией.

Использование данного протокола делает затруднительным его использование на «слабых» линиях связи, так как отсутствует возможность быстрого восстановления утерянного подключения.

Так как информация о спецификации СГД недоступна, то детально проанализировать его работу не предоставляется возможным.

СУДЕБНАЯ КОМПЬЮТЕРНАЯ ЭКСПЕРТИЗА

В.Н. Свердлова, А.С. Романов, студенты 5 курса каф. КИБЭВС
ТУСУР, г. Томск, т. 8-906-199-90-95, vlada@ms.tusur.ru.

Компьютерная экспертиза представляет собой комплексное исследование основных (обеспечивающих) компонентов любого компьютерного средства – аппаратного, программного и информационного обеспечения [1].

Материалами, предоставляемыми для проведения компьютерной экспертизы, обычно являются системные блоки, жесткие диски (НМЖД), гибкие диски (НМГД), оптические диски, другие носители.

Процедура проведения компьютерной экспертизы не регламентируется соответствующим уголовно-процессуальным законодательством, не существует также и какой бы то ни было универсальной схемы (только методические рекомендации). Поэтому все зависит исключительно от вопросов в постановлении на экспертизу и творческой деятельности квалифицированного эксперта.

Важно отметить, что в первую очередь должны применяться методики, не связанные с видоизменением, разрушением или расходованием объектов исследования [2].

Как правило, процедура проведения компьютерной экспертизы включает в себя:

–установление признаков аппаратных средств, таких как тип (вид, модель), форм-фактор и геометрические размеры, наличие или отсутствие серийного номера, кода, наклейки, характерные надписи, повреждения и т.п.;

–создание копии (образа) исследуемого носителя;

–проверка корректности копирования путем сравнения хэш-кодов данных носителя и образа;

–установление структуры данных на носителе (файловая система, распределение информации по секторам и кластерам, объем данных, формат данных);

–восстановление удаленных файлов (либо на файле образа, либо на носителе, защищенном от записи);

–непосредственно исследование согласно вопросам в постановлении на экспертизу;

–документирование всех действий (когда осуществлялись, сколько продолжались) и их результатов;

–представление результатов исследования в виде заключения и формулирование выводов.

Исследование может проводиться по следующим направлениям:

–исследование программного обеспечения, изучение его функционального предназначения, характеристик, структурных особенностей, текущего состояния;

–изучение программных и аппаратных средств, предназначенных для реализации сетевых компьютерных технологий, в том числе работы в сети Internet;

–исследование информации (данных), установление характеристик физического и логического размещения данных на носителе, их формат, атрибуты, тип доступа, содержание.

При проведении компьютерной экспертизы эксперты обычно используют различные программно-технические средства. Существует ряд специализированных программно-аппаратных и программных комплексов зарубежного производства, предназначенных для проведения компьютерных экспертиз, таких как EnCase Forensic Edition, ILOOK Investigator и др. [3]. Тем не менее, инструментарий каждый эксперт подбирает сам, основываясь на финансовых возможностях экспертно-криминалистического учреждения и на собственных предпочтениях. При этом важно понимание экспертом того, как работают используемые программы, чтобы иметь возможность в суде обосновать результаты, полученные в ходе экспертизы. В случае использования специализированных программных комплексов, прошедших соответствующую аттестацию, результаты экспертизы в потенциале гораздо реже могут быть подвергнуты сомнению.

Остается добавить, что непосредственно сама процедура проведения компьютерной экспертизы, ее грамотность и эффективность зависит исключительно от соответствующей методической литературы и уровня подготовленности экспертов. В этом направлении ведется активная работа: выпускают пособия, методические рекомендации, подготавливают программы обучения экспертов по соответствующей специальности.

Тем не менее в отечественной литературе практически не затронута тема криминалистического исследования среды иных операционных систем, нежели Windows. В связи с растущей популярностью POSIX-совместимых операционных систем, в частности Linux, которые исполь-

зуются уже не только на серверах, актуальным становится вопрос о разработке методик проведения компьютерной экспертизы для этой операционной системы.

ЛИТЕРАТУРА

1. *Усов А.И.* Основы методического обеспечения судебно-экспертного исследования компьютерных средств и систем (учебно-практическое пособие)/ Под ред. проф. Е.Р. Россинской. М.: Право и закон , 2002 384 с.

2. *Приказ* МВД РФ от 29 июня 2005 г. N 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации».

3. http://computer-forensics-lab.org – сайт, посвященный компьютерно–технической экспертизе и средствам ее проведения.

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ПОЧТОВОГО СЕРВЕРА DIONIS

О.В. Жувагин, студент 4 курса каф .КИБЭВС

ТУСУР, г. Томск, т. 8-913-102-8042, mave@ctb.rk..tusur.ru

В данной статье рассматривается изучение уязвимых мест системы Dionis, возможные действия потенциального злоумышленника. Анализ уязвимостей системы носит чрезвычайно актуальный характер, так как анализируемые уязвимости являются угрозой в профессиональной деятельности организаций, занимающихся защитой информации.

Dionis – это электронный центр коммуникационных услуг, являющийся многопользовательским программно-техническим комплексом, представляющий абонентам современный коммуникационный сервис – эл. почту, БД, пересылку файлов, компьютерные конференции и т.д. [1].

Технология Dionis является полностью отечественной разработкой, не имеет прямых аналогов в России и за рубежом и отвечает требованиям Доктрины информационной безопасности в плане замещения импортных технических и программных средств в российских СПД (систем передачи данных), а также обеспечения комплексной защиты систем и средств сбора, обработки, хранения и передачи информации от несанкционированного доступа (используемые средства криптографической защиты и сетевой безопасности сертифицированы ФАПСИ и Гостехкомиссией России) [1].

Наиболее распространенные угрозы – сканирование портов и перехват пароля.

Сканирование портов используется злоумышленником для установления вредоносных программ («Трояны», «Вирусы»). Такой тип позволяет потенциальному злоумышленнику понять, какие типы атак на дан-

ный компьютер могут оказаться удачными, а какие заведомо обречены на провал. По полученной информации опытный злоумышленник может догадаться о типе установленной на ПК пользователя операционной системы. А это, в свою очередь, еще сильнее увеличивает круг потенциально удачных атак, а также позволяет попытаться использовать специфические для данной ОС уязвимости.

Перехват пароля и имени пользователя делает доступным для потенциального злоумышленника работу на сервере, т.е. от имени законного пользователя злоумышленник может произвести действия, не желательные как для пользователя, так и для самой системы в целом. И как следствие, – нанесение ущерба, который может исчисляться далеко не маленькими цифрами.

Удручает тот факт, что программное обеспечение, необходимое для обнаружения таких уязвимостей, находится в широком распространении в сети Internet, т.е может использоваться не только администратором сети, но и злоумышленником. Такие программы, как License Agreement v2.0, GFI LANguard Network7.0, легко это демонстрируют. Поэтому для снижения вероятности использования этих уязвимостей необходимо произвести усиление защиты.

Использование терминального доступа (режим постоянного диалога – постоянно выбираются необходимые команды, для управления процессом) [2].

На усмотрение пользователя, можно произвести усиление аутентификации на входе в Dionis следующим образом: после ввода пароля необходимо ответить на вопрос, а затем продолжать работу в системе.

При использовании такой системы необходимо помнить:

– при изменении какого-нибудь состояния компании (например, смене номера телефона, места расположения, смене руководителя и т.д.) ответ на вопрос тоже меняется;

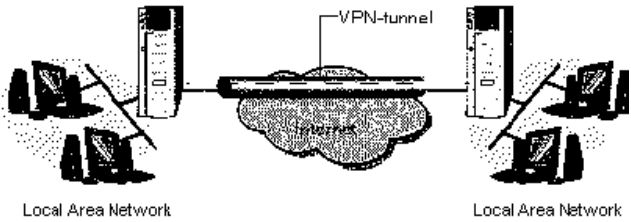
– использовать сможет только квалифицированный сотрудник (системный администратор, программист), т.е. такая система накладывает определённые ограничения на уровень пользователя.

Таким образом, проходим к выводу, что использование такой системы целесообразно только в больших компаниях, где существует должность системного администратора. Поэтому необходимо иметь альтернативные способы усиления защиты, и одним из таких способов является VPN(Virtual Private Network) – виртуальная частная локальная сеть.

Возможность использования VPN происходит в любой ОС Windows 98 и выше.

Необходимо использовать сервер ,который будет использоваться как точка соединения с клиентом, на котором будут запущены службы маршрутизации. Необходимо настроить брандмауэр так как наш сервер VPN принимает (будет принимать) соединения из внешней сети, но это

не значит, что внешняя сеть должна иметь полный доступ к нашему серверу VPN (рисунок).



Использование VPN-соединения

Поэтому мы должны использовать брандмауэр для того, чтобы блокировать неиспользуемые порты. Если используется виртуальный тунель (VPN-tunnel) для присоединения к сети VPN, то важным решением является выбор протокола. Самым совместимым(относительно ОС) является протокол PPTP (Point to Point Tunneling Protocol), но также возможно использовать L2TP (Layer 2 Tunneling Protocol) протокол [3, 4].

В заключение надо сказать, что при выборе способов и средств защиты информации необходимо четко решить:

– для чего будет применяться средство?

– от каких угроз это средство будет ограждать и в какой степени?

– какие правила работы с информационными ресурсами могут быть реализованы?

– сколько финансовых средств надо потратить для достижения необходимых результатов?

ЛИТЕРАТУРА

1. www.factor-ts.ru

2. *Технология* «Дионис», межсетевой экран, Москва 2001

3. *Необходимост*ь применения VPN Николай Прокофьев // КомпьютерПресс. 5. 2001.

4. www.Cyber-Crimes.ru

СОДЕРЖАНИЕ

СЕКЦИЯ 9

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

СЕКЦИЯ 11

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Научное издание

Научная сессия ТУСУР-2007

Материалы
Всероссийской научно-технической конференции
студентов, аспирантов и молодых специалистов
3–5 мая 2007 года, Томск, Россия
В пяти частях

Часть 3

Корректор – **Н.М. Шпагина**

Верстка **В.М. Бочкаревой**

Дизайн обложки **В.Глушко**

Издательство «В-Спектр»
Сдано на верстку 20.03.2007. Подписано к печати 05.04.2007.
Формат $60\times84^{1}/_{16}$. Печать трафаретная.
Печ. л. 14,56. Усл. печ. 13,5. Уч.-изд. л. 14,5.
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