Министерство образования и науки Российской Федерации
Государственное образовательное учреждение
высшего профессионального образования
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

НАУЧНАЯ СЕССИЯ ТУСУР–2011

Материалы
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2011»

4–6 мая 2011 г.

В шести частях

Часть 3

В-Спектр
2011

УДК 621.37/.39+681.518 (063)
ББК 32.84я431+32.988я431
Н 34

Н 34 **Научная сессия ТУСУР–2011:** Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 4–6 мая 2011 г. В 6 частях. – Ч. 3. – Томск: В-Спектр, 2011: – 356 с.

ISBN 978-5-91191-205-8
ISBN 978-5-91191-208-2 (Ч. 3)

Материалы 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, нанофотоники, физической, плазменной, квантовой, промышленной электроники, радиотехники, информационно-измеритель-ных приборов и устройств, распределенных информационных технологий, вычислительного интеллекта, автоматизации технологических процессов, в частности в системах управления и проектирования, информационной безопасности и защите информации. Представлены статьи по математическому моделированию в технике, экономике и менеджменте, антикризисному управлению, автоматизации управления в технике и образовании, а также работы, касающиеся социокультурных проблем современности, экологии, мониторинга окружающей среды и безопасности жизнедеятельности.

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

ISBN 978-5-91191-205-8
ISBN 978-5-91191-208-2 (Ч. 3)

Министерство образования и науки Российской Федерации
Государственное образовательное учреждение
высшего профессионального образования
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Всероссийская научно-техническая конференция студентов и молодых ученых «Научная сессия ТУСУР – 2011» 4–6 мая 2011 г.

ПРОГРАММНЫЙ КОМИТЕТ

- *Шурыгин Ю.А.* – председатель Программного комитета, ректор ТУСУРа, заслуженный деятель науки РФ, д.т.н., профессор;
- *Шелупанов А.А.* – сопредседатель Программного комитета, проректор по НР ТУСУРа, зав. каф. КИБЭВС ТУСУРа, д.т.н., профессор;
- *Беляев Б.А.*, зав. лабораторией электродинамики» Ин-та физики СО РАН, д.т.н., г. Красноярск;
- *Ворошилин Е.П.*, зав. каф. ТОР, к.т.н.;
- *Голиков А.М.*, доцент каф. РТС, к.т.н.;
- *Грик Н.А.*, зав. каф. ИСР, д.ист.н., профессор;
- *Давыдова Е.М.*, зам. зав. каф. КИБЭВС по УР, доцент каф. КИБЭВС, к.т.н.;
- *Дмитриев В.М.*, зав. каф. ТОЭ, д.т.н., профессор;
- *Еханин С.Г.*, профессор. каф. КУДР, д.ф.-м.н., доцент;
- *Ехлаков Ю.П.*, проректор по информатизации и управлению ТУСУРа, зав. каф. АОИ, д.т.н., профессор;
- *Зариковская Н.В.*, доцент каф. ФЭ, к.ф.-м.н.;
- *Карташев А.Г.*, профессор каф. РЭТЭМ, д.б.н.
- Катаев М.Ю., профессор каф. АСУ, д.т.н.;
- *Коцубинский В.П.*, зам. зав. каф. КСУП, доцент каф. КСУП, к.т.н.;
- *Лощилов А.Г.*, с.н.с. СКБ «Смена» ТУСУРа, к.т.н.;
- *Лукин В.П.*, директор отд. распространения волн Ин-та оптики атмосферы СО РАН, почетный член Американского оптического общества, д.ф.-м.н., профессор, г. Томск;
- *Малюк А.А.*, декан фак-та информационной безопасности МИФИ, к.т.н., г. Москва;
- *Малютин Н.Д.*, начальник НУ ТУСУРа, директор НОЦ «Нанотехнологии», д.т.н., профессор;

- *Мещеряков Р.В.*, зам. начальника НУ ТУСУРа, доцент, зам. зав. каф. КИБЭВС по НР, к.т.н.;
- *Мицель А.А.*, профессор, зам. зав. каф. АСУ, д.т.н.;
- *Осипов Ю.М.*, зав. отделением каф. ЮНЕСКО ТУСУРа, академик Международной академии информатизации, д.э.н., д.т.н., профессор;
- *Пустынский И.Н.*, зав. каф. ТУ, заслуженный деятель науки и техники РФ, д.т.н., профессор;
- *Разинкин В.П.*, профессор, каф. ТОР НГТУ, д.т.н., г. Новосибирск;
- *Семиглазов А.М.*, профессор каф. ТУ, д.т.н., ;
- *Суслова Т.И.*, декан ГФ, зав. каф. КС, д.ф.н., доцент;
- *Титов А.А.*, профессор каф. РЗИ, д.т.н., доцент;
- *Троян П.Е.*, зав. каф. ФЭ, д.т.н., профессор;
- *Уваров А.Ф.*, проректор по инновационному развитию и международной деятельности ТУСУРа, зав. каф. УИ, к.э.н.;
- *Ходашинский И.А.*, профессор каф. АОИ, д.т.н.;
- *Черепанов О.И.,* профессор каф. ЭСАУ, д.ф.-м.н.;
- *Шарангович С.Н.*, профессор, зав. каф. СВЧиКР, к.ф.-м.н.;
- *Шарыгин Г.С.*, зав. каф. РТС, д.т.н., профессор;
- *Шостак А.С.*, профессор каф. КИПР, д.т.н.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

- *Шелупанов А.А.* – председатель Организационного комитета, проректор по НР ТУСУРа, зав. каф. КИБЭВС, д.т.н., профессор;
- *Ярымова И.А.* – зам. председателя Оргкомитета, зав. ОППО ТУСУРа, к.б.н.;
- *Юрченкова Е.А.* – секретарь Оргкомитета, инженер ОППО ТУСУРа, к.х.н.

СЕКЦИИ КОНФЕРЕНЦИИ

Секция 1. Радиотехнические системы и распространение радиоволн. Председатель секции – Шарыгин Герман Сергеевич, зав. каф. РТС, д.т.н., проф.; зам. председателя – Тисленко Владимир Ильич, проф. каф. РТС, д.т.н., доцент.

Секция 2. Защищенные телекоммуникационные системы. Председатель секции – Голиков Александр Михайлович, доцент каф. РТС, к.т.н.; зам. председателя – Бернгардт Александр Самуилович, доцент каф. РТС, к.т.н.

Секция 3. Аудиовизуальная техника, бытовая радиоэлектронная аппаратура и сервис. Председатель секции – Пустынский Иван

Николаевич, зав. каф. ТУ, д.т.н., проф.; зам. председателя – Костевич Анатолий Геннадьевич, с.н.с. каф. ТУ НИЧ, к.т.н.

Секция 4. Проектирование биомедицинской аппаратуры. Председатель секции – Еханин Сергей Георгиевич, проф. каф. КУДР, д.ф.-м.н., доцент; зам. председателя – Романовский Михаил Николаевич, доцент каф. КУДР, к.т.н.

Секция 5. Конструирование и технологии радиоэлектронных средств. Председатель секции – Лощилов Антон Геннадьевич, с.н.с. СКБ «Смена», к.т.н.; зам. председателя – Бомбизов Александр Александрович, м.н.с. СКБ «Смена».

Секция 6. Интегрированные информационно-управляющие системы. Председатель секции – Катаев Михаил Юрьевич, проф. каф. АСУ, д.т.н.; зам. председателя – Бойченко Иван Валентинович, доцент каф. АСУ, к.т.н.

Секция 7. Оптические информационные технологии, нанофотоника и оптоэлектроника. Председатель секции – Шарангович Сергей Николаевич, проф., зав. каф. СВЧиКР, к.ф.-м.н.; зам. председателя – Буримов Николай Иванович, зав. УНЛ каф. ЭП НИЧ, к.т.н.

Секция 8. Физическая и плазменная электроника. Председатель секции – Троян Павел Ефимович, зав. каф. ФЭ, д.т.н., проф.; зам. председателя – Смирнов Серафим Всеволодович, проф. каф. ФЭ, д.т.н.

Секция 9. Распределённые информационные технологии и системы. Председатель секции – Ехлаков Юрий Поликарпович, проректор по информатизации и управлению ТУСУРа, зав. каф. АОИ, д.т.н., проф.; зам. председателя – Сенченко Павел Васильевич, декан ФСУ, доцент каф. АОИ, к.т.н.

Подсекция 9.1. Распределённые информационные технологии и системы. Председатель секции – Ехлаков Юрий Поликарпович, проректор по информатизации и управлению ТУСУРа, зав. каф. АОИ, д.т.н., проф.; зам. председателя – Сенченко Павел Васильевич, декан ФСУ, доцент каф. АОИ, к.т.н.

Подсекция 9.2. Современные библиотечные технологии. Председатель секции – Абдрахманова Марина Викторовна, зав. библиотекой ТУСУРа; зам. председателя – Карауш Александр Сергеевич, доцент каф. РЗИ, к.т.н.

Секция 10. Вычислительный интеллект. Председатель секции – Ходашинский Илья Александрович, проф. каф. АОИ, д.т.н.; зам. председателя – Лавыгина Анна Владимировна, ст. преп. каф. АОИ, к.т.н.

Секция 11. Автоматизация технологических процессов. Председатель секции – Давыдова Елена Михайловна, доцент, зам. зав. каф. КИБЭВС по УР, к.т.н.; зам. председателя – Зыков Дмитрий Дмитриевич, доцент каф. КИБЭВС, к.т.н.

Секция 12. Аппаратно-программные средства в системах управления и проектирования. Председатель секции – Шурыгин Юрий Алексеевич, ректор ТУСУРа, зав. каф. КСУП, д.т.н., проф.; зам. председателя – Коцубинский Владислав Петрович, доцент каф. КСУП, к.т.н.

Подсекция 12.1. Интеллектуальные системы проектирования технических устройств. Председатель секции – Черкашин Михаил Владимирович, декан ФВС, доцент каф. КСУП, к.т.н.

Подсекция 12.2. Адаптация математических моделей для имитации сложных технических систем. Председатель секции – Коцубинский Владислав Петрович, доцент каф. КСУП, к.т.н.

Подсекция 12.3. Инструментальные средства поддержки сложного процесса. Председатель секции – Хабибуллина Надежда Юрьевна, доцент каф. КСУП, к.т.н.

Подсекция 12.4. Автоматизация проектирования в AutoCAD и КОМПАС. Председатель секции – Дорофеев Сергей Юрьевич, ассистент каф. КСУП.

Секция 13. Радиотехника. Председатель секции – Титов Александр Анатольевич, проф. каф. РЗИ, д.т.н., доцент; зам. председателя – Семенов Эдуард Валерьевич, доцент каф. РЗИ, к.т.н.

Секция 14. Методы и системы защиты информации. Информационная безопасность. Председатель секции – Шелупанов Александр Александрович, проректор по НР ТУСУР, зав. каф. КИБЭВС, д.т.н., проф.; зам. председателя – Мещеряков Роман Валерьевич, зам. начальника НУ ТУСУР, доцент, зам. зав. каф. КИБЭВС по НР, к.т.н.

Секция 15. Информационно-измерительные приборы и устройства. Председатель секции – Черепанов Олег Иванович, проф. каф. ЭСАУ, д.ф.-м.н.; зам. председателя – Шидловский Виктор Станиславович, доцент каф. ЭСАУ, к.т.н.

Секция 16. Промышленная электроника. Председатель секции – Михальченко Геннадий Яковлевич, директор НИИ ПрЭ, д.т.н., проф.; зам. председателя – Семенов Валерий Дмитриевич, проф., зам. зав. каф. ПрЭ по НР, к.т.н.

Секция 17. Математическое моделирование в технике, экономике и менеджменте. Председатель секции – Мицель Артур Александрович, проф. каф. АСУ, д.т.н.; зам. председателя – Зариковская Наталья Вячеславовна, доцент каф. ФЭ, к.ф.-м.н.

Подсекция 17.1. Моделирование в естественных и технических науках. Председатель секции – Зариковская Наталья Вячеславовна, доцент каф. ФЭ, к.ф.-м.н.

Подсекция 17.2. Моделирование, имитация и оптимизация в экономике. Председатель секции – Мицель Артур Александрович, проф. каф. АСУ, д.т.н.; зам. председателя – Кузьмина Елена Александровна, доцент каф. АСУ, к.т.н.

Секция 18. Экономика и управление. Председатель секции – Осипов Юрий Мирзоевич, зав. отделением каф. ЮНЕСКО, д.э.н., д.т.н., проф.; зам. председателя – Васильковская Наталья Борисовна, доцент каф. экономики, к.э.н.

Секция 19. Антикризисное управление. Председатель секции – Семиглазов Анатолий Михайлович, проф. каф. ТУ, д.т.н.; зам. председателя – Бут Олеся Анатольевна, ассистент каф. ТУ.

Секция 20. Экология и мониторинг окружающей среды. Безопасность жизнедеятельности. Председатель секции – Карташев Александр Георгиевич, проф. каф. РЭТЭМ, д.б.н.; зам. председателя – Смолина Татьяна Владимировна, доцент каф. РЭТЭМ, к.б.н.

Секция 21. Социокультурные проблемы современности. Председатель секции – Суслова Татьяна Ивановна декан ГФ, декан ГФ, зав. каф. КС, д.ф.н., доцент; зам. председателя – Грик Николай Антонович, зав. каф. ИСР, д.ист.н., проф.

Подсекция 21.1. Актуальные проблемы социальной работы в современном обществе. Председатель секции – Грик Николай Антонович, зав. каф. ИСР, д.ист.н., проф.; зам. председателя – Казакевич Людмила Ивановна, доцент каф. ИСР, к.ист.н.

Подсекция 21.2. Философия и специальная методология. Председатель секции – Московченко Александр Дмитриевич, зав. каф. философии, д.ф.н., проф.; зам. председателя – Раитина Маргарита Юрьвна, к.ф.н., доцент каф. философии.

Секция 22. Инновационные проекты, студенческие идеи и проекты. Председатель секции – Уваров Александр Фавстович, проректор по инновационному развитию и международной деятельности ТУСУР, к.э.н.; зам. председателя – Чекчеева Наталья Валерьевна, зам. директора Студенческого бизнес-инкубатора (СБИ), к.э.н.

Секция 23. Автоматизация управления в технике и образовании. Председатель секции – Дмитриев Вячеслав Михайлович, зав. каф. ТОЭ, д.т.н., проф.; зам. председателя – Ганджа Тарас Викторович, доцент ВКИЭМ, к.т.н.

Секция 24. Проектная деятельность школьников в сфере информационно-коммуникационных технологий. Председатель секции – Вьюгова Татьяна Сергеевна, руководитель отдела образовательных программ ОЦ «Школьный университет».

Секция 25. Системы и сети электро- и радиосвязи. Председатель секции – Ворошилин Евгений Павлович, зав. каф. ТОР, к.т.н.; зам. председателя – Белов Владимир Иванович, доцент каф. ТОР, к.т.н.

Секция 26. Проектирование и эксплуатация радиоэлектронных средств. Председатель секции – Шостак Аркадий Степанович, проф. каф. КИПР, д.т.н.; зам. председателя – Озёркин Денис Витальевич, декан РКФ, доцент каф. КИПР, к.т.н.

Адрес Оргкомитета:

634050, Россия, г. Томск,
пр. Ленина, 40, ГОУ ВПО «ТУСУР»,
Научное управление (НУ), к. 205
Тел.: 8-(3822)-701-524, 701-582
E-mail: nstusur@main.tusur.ru

1-й том – 1–7-я секции;
2-й том – 8–10, 13-я секции;
3-й том – 11-я, 14-я секции;
4-й том – 12, 15, 19-я секции;
5-й том – 16–18, 20-я секции;
6-й том – 21–26-я секции.

СЕКЦИЯ 11

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

*Председатель секции – **Давыдова Е.М.**, доцент,*
зам. зав. каф. КИБЭВС по УР, к.т.н.;
*зам. председателя – **Зыков Д.Д.**, доцент каф. КИБЭВС, к.т.н.*

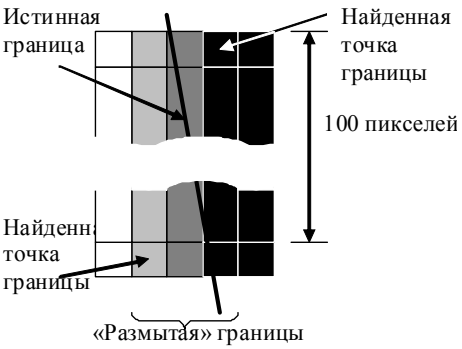
ИЗМЕРЕНИЕ УГЛА ГРАНИЦЫ ОБЪЕКТА НА ВИДЕОКАДРЕ НИЗКОГО РАЗРЕШЕНИЯ С ИСПОЛЬЗОВАНИЕМ АПРИОРНОЙ ИНФОРМАЦИИ

С.М. Алфёров, каф. АСУ, программист
г. Томск, ТУСУР, alhoresm@sibmail.com

При автоматизации технологических процессов в производстве часто требуется определять положение объекта. Одним из параметров положения является угол наклона прямой границы объекта, так, на ОАО «Манотомь» в процессе модернизации производственного процесса возникла задача: измерение угла наклона прямой границы объекта с точностью ±0,5° при помощи видеокамеры разрешением 320×240.

Для выделения границ объекта удобно использовать популярный фильтр Собела [1]. Но данный фильтр выделяет границу недостаточно точно и требует большого количества вычислений.

Самый простой метод: измерение угла по двум точкам границы. Граница объекта на кадре никогда не бывает четкой, кроме того, возникают помехи (не идеально белый фон, появление возле границы объекта, других мелких объектов, дающих тень, и т.д.), в результате погрешность измерения координат граничной точки достигает 3 пикселей при использовании предложенной видеокамеры. Таким образом, при расстоянии между найденными граничными точками 100 пикселей, погрешность измеренного угла составит ±0,03 рад

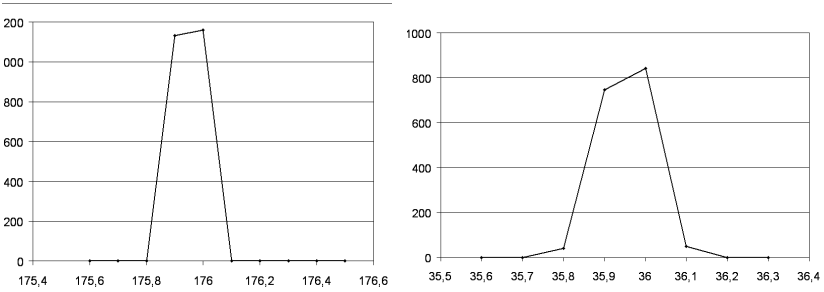


или ±1,7° (Рис. 1). Рис. 1. Погрешность измерения угла

Результаты работы

Были проведены два эксперимента с использованием видеокамеры разрешением 320×240, длина границы объекта на кадре примерно 100 пикселей. В ходе экспериментов для двух различных положений объекта были получены результаты, приведенные на Рис. 2 и в таблице.

Точки на графиках показывают количество измерений (ось ординат), попавших в интервалы размером 0,1 град, и измеренные значения углов (ось абсцисс).



Опыт №1 Опыт №2

Рис. 2. Гистограмма измерений

Результаты экспериментов

№ опыта	Количество измерений углов ψ*	Оценка истинного значения	Погрешность	Примечание
1	2293	175,95°	0,15° или 9'	Черный объект на белом фоне
2	1677	35,95°	0,25° или 15'	Черный объект на фоне стального механизма

Заключение

В результате работы построен и реализован алгоритм определения угла наклона объекта с достаточной точностью, данный алгоритм применяется в производстве на ОАО «Манотомь». Алгоритм хоть и даёт увеличение ошибки в два раза при незначительном изменении характера фона, тем не менее ошибка остаётся в допустимых пределах.

ЛИТЕРАТУРА

1. *Хорн Б.К.* Зрение роботов: пер. с англ. М.: Мир, 1989. 487 с.

ИССЛЕДОВАНИЕ ПОДХОДА К СЕГМЕНТАЦИИ РЕЧЕВОГО СИГНАЛА

И.Г. Андреева, студентка 5-го курса каф. КИБЭВС
г. Томск, ТУСУР, ФВС, genkavna@rambler.ru

Наиболее распространенным подходом к построению параметрического описания речевого сигнала является применение одного и того же алгоритма для всех классов звуков. Это упрощает предварительную обработку сигнала, исключает использование предварительной сегментации [1].

Слуховая система человека обладает эффектом одновременной маскировки частот. После одновременной маскировки сигнал имеет структуру, представленную на рис. 1 [2].

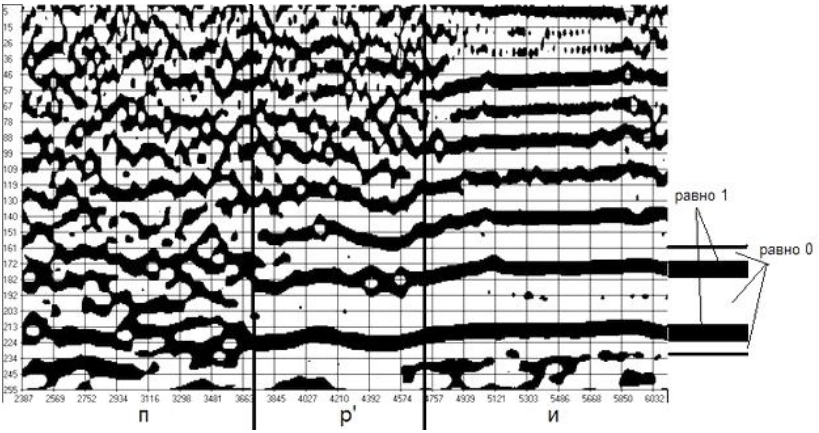


Рис. 1. Структура речевого сигнала после одновременной маскировки

В работе [3] приводится созданный на основе полученной структуры алгоритм определения вокализованности текущего временного отсчета.

Принятие решения о вокализации включает в себя определение меры различия d между сигналом и каждой из масок при помощи свёртки вида (1):

$$d(i,t)=\sum_{k} F(k,i)\oplus x(k,t)\,. \qquad (1)$$

Исследование подхода к сегментации речевого сигнала проводилось на основе программного комплекса, включающего разработанный алгоритм. В ходе работы было исследовано 2 фразы 8 дикторов, из них 4 женских и 4 мужских. Исследование проводилось с помощью приложения Sr.

Диктор – мужчина (1), фраза (7), слово «Скайлс» (С к Атм й’ л с), согласный глухой звук «С».

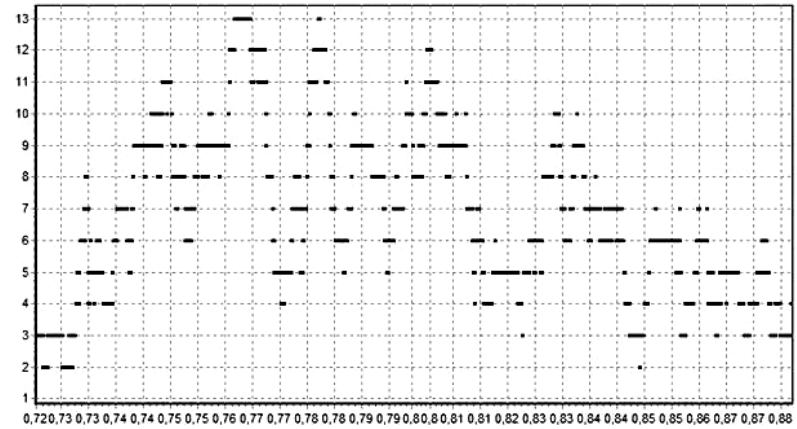


Рис. 2. Звук «С»

Диктор – мужчина (1), фраза (7), слово «Скайлс» (С к Атм й’ л с), ударный гласный звук «А».

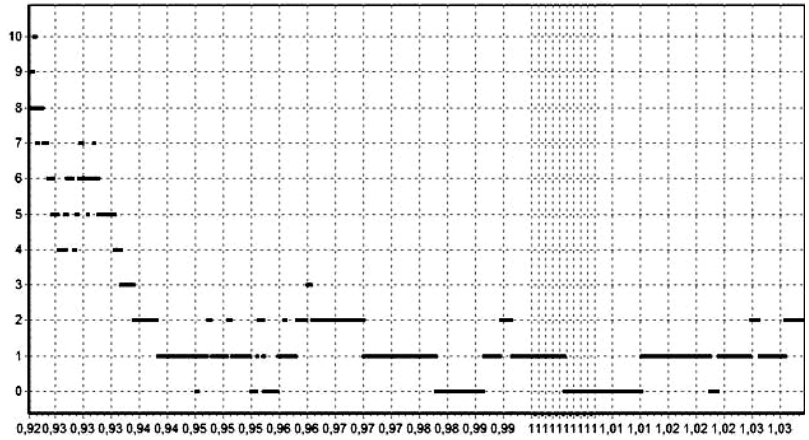


Рис. 3. Звук «Атм»

Диктор – женщина (53), фраза (44), слово «Щеки» (Щ’ Омм к’ им2), безударный гласный звук «И».

Исследование невокализованных звуков показало, что значение меры различия *d* находится примерно в интервале от 3 до 10. Исследование ударных гласных звуков показало, что значение меры различия было от 0 до 3. Исследование безударных гласных звуков показало,

что значение меры различия выше, чем у ударных звуков, и находится в районе от 2 до 6.

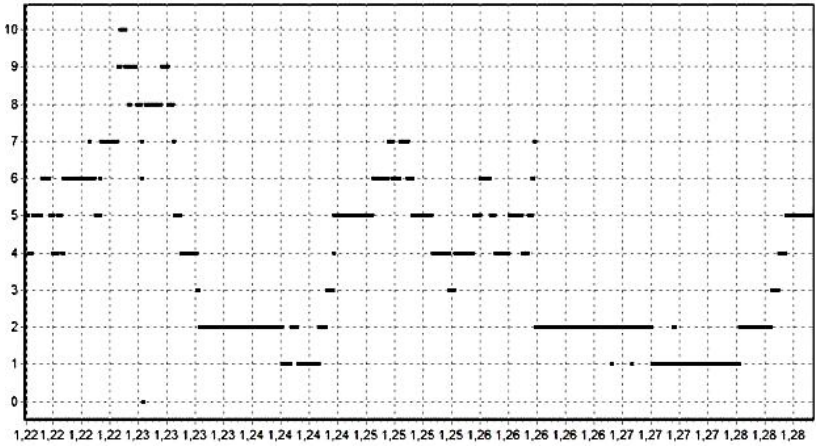


Рис. 4. Звук «Им2»

Полученные значения для разных классов звуков отличаются друг от друга. По полученным данным можно сделать вывод, что рассмотренный подход можно использовать для дальнейшей сегментации речевого сигнала.

ЛИТЕРАТУРА

1. *Конев А.А., Мещеряков Р.В., Тиунов С.Д. и др.* Параметрическое описание ударных гласных звуков // Сб. тр. XXII сессии Российского акустического общества. Т. 3. М.: ГЕОС, 2010. С. 41–45.

2. *Конев А.А., Мещеряков Р.В., Жевуров С.В., Хлебников В.С.* Сегментация вокализованных участков речевого сигнала // Сб. тр. XXII сессии Российского акустического общества. Т. 3. М.: ГЕОС, 2010. С. 45–48.

3. *Бондаренко В.П., Конев А.А., Мещеряков Р.В.* Обработка речевых сигналов в задачах идентификации // Изв. вузов. Физика. 2006. Т. 49, №9. С. 207–210.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПРОВЕРКИ ПРАВИЛЬНОСТИ ПРОГРАММ

Е.А. Батеев, студент 2-го курса ФВС

Научный руководитель В.Н. Кирнос, доцент, к.ф.-м.н.

г. Томск, ТУСУР, каф. КИБЭВС, by9_11@mail.ru

Как известно, при начальном обучении программированию важно научить грамотно проводить тестирование программ. Иначе говоря,

должна быть (для каждой учебной задачи) разработана правильная система тестов, на которых и будет проверяться созданная студентом программа. При этом также важно автоматизировать данный процесс с тем, чтобы студент мог протестировать свою программу, а преподаватель – получить результаты тестирования для оценки знаний студентов.

Основные положения по тестированию (испытанию) компьютерных программ заложены в классических трудах [2–4]. В последнее время системы автоматизированного тестирования программ (САТП) очень часто используются для проверки учебных и олимпиадных задач по информатике. Например, система проверки программ используется при проведении международных олимпиад под эгидой Association for Computing Machinery (ACM) [5]. Программное обеспечение, использующееся на олимпиадах ACM, защищено авторским правом, поэтому для подготовки команд на студенческие олимпиады разработано несколько подобных систем, в частности «EJudge», «Олимпия» [6, 7].

Условием, без которого невозможен процесс АТП, является однозначное отображение множества входных данных {X} в соответствующий набор выходных данных {Y} :

$$G: \{X\} \rightarrow \{Y\}. \quad (1)$$

Закон отображения определяется алгоритмом испытуемой программы. На вход САТП подается внешнее воздействие. На вход тестируемой программы поступает вектор входных данных $x=\{x_1,...x_n\}$. На выходе программы по закону (1) получаем результаты работы тестируемой программы $y=\{y_1,... y_m\}$, подающиеся на САТП, где они и обрабатываются. В САТП задан алгоритм *H* однозначного отображения множества {X} в {Z} :

$$H: \{X\} \rightarrow \{Z\}. \quad (2)$$

Будем считать, что условием верности работы программы является условие

$$G: \{X\} \rightarrow \{Y\} = H: \{X\} \rightarrow \{Z\}, \text{т.е. } \{Y\} = \{Z\}. \quad (3)$$

Таким образом, тестируемую программу можно рассматривать как модель идеальной программы, действующей по закону (2). Успехом тестирования программного кода будет являться истинность этой модели.

Такая модель (она описана в [8]) не полностью отражает исследуемый объект, но дает некоторое представление о простейшем случае АТП, используемого для предварительной проверки задач по программированию.

Итак, нами была поставлена задача: создать САТП с Windows-интерфейсом, который позволяет (пользователю):

а) выбрать задание из списка предлагаемых задач,

б) выбрать среду, в которой запрограммировано решение задачи,

в) отправить полученную программу-решение и получить результат проверки данной программы-решения на группе тестов.

При этом программный комплекс позволяет (администратору):

а) вносить в базу условия заданий,

б) формировать для каждого задания систему тестов,

в) на основе полученных от пользователей решений формировать таблицу результатов.

На настоящий момент такая САТП разработана частично: имеется собственно тестирующая программа, которая позволяет проверять программы, разработанные на языке Visual C++ (среда Microsoft Visual Studio 2005/2008), и в среде Borland Delphi 7. В дальнейшем предполагается предусмотреть тестирование программ, разработанных и в других средах (в т.ч. Turbo Pascal).

Предварительная проверка работы данной САТП в ходе занятий со студентами 1-го курса спец. 090105 и 210202 показала свою эффективность и значимость. Студенты могут самостоятельно проводить тестирование своих программ, зная, что проверка проводится на широкой группе тестов, и, соответственно, быть уверенными, что в результате ими создана вполне работоспособная программа. Преподаватель при этом может легко анализировать работоспособность созданных студентами программ и проводить быструю оценку их работы.

ЛИТЕРАТУРА

1. *Чупин Н.А.* Проведение олимпиад по информатике: учеб. пособие. Бийск: Изд-во БиГПИ, 1997.

2. *Ван Тассел Д.* Стиль, разработка, эффективность, отладка и испытание программ. М.: Мир, 1985.

3. *Грис Д.* Наука программирования. М.: Мир, 1984.

4. *Майерс Г.* Искусство тестирования программ. М.: Финансы и статистика, 1982.

5. *Васильев В.Н., Парфенов В.Г.* Командный чемпионат мира по программированию ACM 1998/1999. СПб: СПбГИТМО(ТУ), 1998. 112 с.

6. *Цымблер М.Л.* Система автоматической проверки решений задач по программированию, использующая сетевые технологии / М.Л. Цымблер, М.М. Арсламбеков // Телематика'99: Тез. докл. Всерос. науч.-метод. конф. (8–11 июня 1998 г., Санкт-Петербург). СПб.: Вузтелекомцентр, 1999.

7. *Меньшиков Ф.В.* Олимпиадные задачи по программированию. СПб.: Питер, 2006.

8. *Веретенников М.В.* Автоматизация проверки компьютерных программ в технических дисциплинах // Сб. науч. тр. «Дистанционные образовательные технологии». Вып. 1. Пути реализации. М., 2004.

КОМПЬЮТЕРНЫЙ ОСЦИЛЛОГРАФ «ПРОГРАММНАЯ ЧАСТЬ»

Д.В. Березин, Д.А. Вольф, студенты, каф. КИБЭВС
Научный руководитель Е.Д. Головин, зам. директора филиала ТУСУРа в г. Сургуте, доцент, к.т.н.
г. Сургут, филиал ТУСУРа, atrayder@rambler.ru

В филиале ТУСУРа в г. Сургуте для проведения лабораторного практикума по дисциплине «Общая электротехника и электроника» разработана аппаратная часть компьютерного осциллографа. Необходимо написать программную часть к устройству, способную к получению цифровых данных по шине USB на ПК для последующей дополнительной обработки, пересчета масштаба, коррекции нуля и отображения в графическом виде.

Исходя из требований, предъявляемых к качеству работы компьютерного осциллографа, нельзя не отметить, что его эффективная работа всецело зависит от качества программного обеспечения, его функциональной насыщенности и наглядности.

Входные данные от аппаратной части «компьютерного осциллографа» поступают по интерфейсу USB со скоростью 60000 точек в секунду. Глубина дискретизации каждого временного интервала составляет 8 бит. Частота измеряемого сигнала изменяется в пределах от 1 Гц до 1,7 кГц, максимальная амплитуда по напряжению 2 В, две формы сигнала: гармоническая и прямоугольная.

Интерфейс программного обеспечения должен иметь: главное меню, рабочую область для изображения сигнала, курсор, который позволит отмечать точки графика для точного определения их координат. С помощью главного меню можно управлять развёрткой осциллографа, производить сравнение графиков различных осциллограмм, останавливать развертку осциллограммы для отображения значения минимума и максимума построенной функции, производить очистку дисплея, выбор требуемого канала ввода, предусмотреть сохранение осциллограммы в виде графического изображения, а также по координатам в текстовый файл для последующей обработки результатов измерений.

Для раскрытия всех потенциальных возможностей, которые несет в себе использование компьютерного осциллографа, необходимо применить в работе комплекс программных и аппаратных средств, максимально соответствующий программам обучения.

В результате проведенного анализа и исследования предметной области подтверждена актуальность разработки и изготовления программно-аппаратного комплекса. Главной отличительной особенно-

стью разработанного комплекса является возможность одновременного измерения нескольких каналов, при этом стоимость комплекса существенно ниже существующих аналогов.

При этом студенты, помимо программы обучения, получают необходимые средства для обеспечения диалога человек – ЭВМ, которые помогают на практике видеть, измерять параметры сигнала и проводить расчеты на основании полученных данных. Программная часть компьютерного осциллографа создаётся при помощи бесплатного программного обеспечения, что является экономически выгодно, а также способствует дальнейшему совершенствованию программной части комплекса.

ЛИТЕРАТУРА

1. Pico Technology Limited [сайт]. URL: http://www.picotech.com/
2. Компания СИГНАЛ [сайт]. URL: http://www.signal.ru/
3. ЗАО «Руднев-Шиляев» [сайт]. URL: http://www.rudshel.ru/
4. Научно-производственная компания АУРИС [сайт]. URL: http://auris.ru/

ОБЗОР ГРАФОПОСТРОИТЕЛЬНЫХ СИСТЕМ

Д.С. Бронников, студент 5-го курса,
П.Н. Коваленко, инженер, к.т.н., В.А. Бейнарович, проф., д.т.н.
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, intesa@sibmail.com

Графопостроитель – устройство для автоматического вычерчивания с большой точностью рисунков, схем, сложных чертежей, карт и другой графической информации. Применяется как устройство вывода графической информации в ЭВМ, автоматизированных системах проектирования, информационно-измерительных системах, в картографии и т.д.

Основными техническими характеристиками графопостроителей являются:

1) размер чертежной поверхности (мм);
2) быстродействие перемещения исп. орг. (10–300 мм/с);
3) разрешающая способность (0,4–0,0025 мм);

Графопостроители различаются по типу размещения носителя: планшетные и барабанные (таблица). В планшетных графопостроителях носитель неподвижно закреплён на плоском столе. В графопостроителях барабанного типа носитель закреплен на вращающемся цилиндре.

Графопостроитель широкоформатный «ГШ-2200»

Предназначен для построения чертежей в различных САПР (MCAD, ADEM, КОМПАС, TurboCAD), применяется в машиностроении, легкой промышленности, картографии, архитектуре и др. Графопостроитель позволяет производить вычерчивание в натуральную величину раскладок лекал для тканей.

Основные показатели:

- максимальные размеры рабочей поверхности – до 2,2 м;
- управляющая ЭВМ на базе процессора «Pentium»;
- наличие автоматической системы самодиагностики;
- максимальная скорость перемещения исполнительного органа – 500 мм/с;

Графопостроитель «ГР-1600»

Предназначен для маркировки, вычерчивания и вырезки лекал. В качестве рабочего инструмента могут выступать вибрационный механический нож, шариковый узел или фломастер. Материалом для вырезки может служить листовой электротехнический картон.

Графопостроитель «ГР-1600» на основании информации, поступающей от ЭВМ, производит вырезку фигур заданной формы и может наносить на эти фигуры метки и надписи.

По конструктивному исполнению графопостроитель представляет собой координатное устройство, в котором движение по оси Y осуществляется за счет перемещения рабочего материала, а движение по оси X – перемещением каретки, несущей на себе режущий и пишущий инструмент. Используется в САПР таких производителей, как «Mastercam», «Ассоль».

Основные показатели:

- максимальные размеры рабочей поверхности – 900×1600 мм;
- управляющая ЭВМ на базе процессора «Pentium»;
- толщина обрабатываемого картона – 0,2–2,0 мм;
- максимальная скорость черчения – 450 мм/с;
- максимальная скорость резки – 300 мм/с.

Координатный стол с ЧПУ «Рапид»

Координатный стол с ЧПУ для лазерных, плазменных, термических и раскройных комплексов. Промышленное исполнение, стальное основание, сервопривод постоянного тока с обратной связью по положению и по скорости.

Предназначен для построения чертежей в различных САПР (Eleandr CAPP, Comtense, КОМПАС).

Используется в аэрокосмической и легкой промышленности для вычерчивания раскладок элементов изделия при оптимизации раскроя и вырезания лекал (при оснащении лазерной раскройной системой).

Сравнительные показатели графопостроителей

Характеристики	Графопостроитель ГШ-2200	Графопостроитель ГР-1600	Координатный стол Рапид	Графопостроитель ШД-5Д1М
Размер чертежной поверхности,мм	2200×2200	900×1600	6800×1600	297×210
Минимальный программируемый шаг, мм	0,025	0,025	0,01	0,01
Статистическая погрешность, мм	±(0,2+0,05%L)	±(0,2+0,05%L)	$(1–2)\times10^{-3}$	±(0,4+0,05%L)
Тип размещения носителя	Планшетный	Барабанный	Планшетный	Барабанный
Применение в САПР	MCAD, ADEM, КОМПАС, TurboCAD	Mastercam, Ассоль	Eleandr CAPP, Comtense, КОМПАС	--------

Примечание. L – длина перемещения.

Основные показатели:

- максимальные размеры рабочей поверхности – 6800×1600 мм;
- максимальная скорость перемещения исполнительного органа– 500 мм/с;
- управляющая ЭВМ на базе процессора «Pentium»;

Графопостроитель «ШД-5Д1М»

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

Графопостроитель «ШД-5Д1М» преобразует вращение ротора шагового двигателя в линейное перемещение исполнительного органа.

Основные показатели:

- максимальные размеры рабочей поверхности – 297×210 мм;
- управляющая ЭВМ на базе процессора Intel 486;

• максимальная скорость перемещения исполнительного органа – 40 мм/с.

Графопостроитель «ШД-5Д1М» по ряду показателей уступает современным промышленным образцам (скорость перемещения исполнительного органа, максимальные размеры рабочей поверхности, отсутствие работы с САПР). Однако он обладает небольшой массой и габаритами – 500×400×300 (мм), что позволяет использовать для изучения принципов автоматизированного управления в качестве лабораторного стенда по таким дисциплинам, как «Гибкие автоматизированные системы и робототехника», «Системы автоматизированного управления».

ЛИТЕРАТУРА

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

2. Шаговый двигатель, или сервопривод? http://woodstanki.ru/info/shagservo

3. Координатные столы. http://www.fedal.spb.ru/production_ks.asp

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ КОСМИЧЕСКОЙ АППАРАТУРЫ «XPHOENIX»

Э.К. Данилин, аспирант

Научный руководитель Р.М. Мещеряков, доцент, к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, EddyKain@Gmail.com

Создание программного обеспечения для контрольно-провероч-ной аппаратуры – достаточно трудоёмкая задача, из-за многих факторов:

• ограничение времени на программный проект (времени выделяется гораздо меньше, чем на время проектирование аппаратных частей, также малое количество времени на работу с оборудованием);

• сложность проекта (в большинстве случаев не позволяет произвести полное тестирование программного обеспечения);

• постоянное изменение параметров и команд приборов;

• периодическая модернизация как программного, так и аппаратного обеспечения.

Вследствие этого возникает необходимость в более практичном и более надёжном подходе. На смену стандартному программному обеспечению появилась необходимость в создании системы, которая полностью заменит стандартный подход. Такая система должна отвечать следующим требованиям:

• надёжность (стабильность системы, неповторимость компонентов);

- изменяемость (возможность «на ходу» изменять интерфейс и изменять функциональность системы);
- расширяемость (возможность добавлять нестандартную функциональность);
- простота (возможность создания интерфейса и написания программ проверок низкоквалифицированным персоналом в области создания программного обеспечения и со слабыми знаниями английского языка);
- информативность (максимально возможное сохранение данных, для исследования аварий и других ошибок);
- защищённость (ограничение доступа и распределение полномочий).

Из этих требований можно вывести заключение, что необходимо создать комплекс программного обеспечения, отвечающий этим требованиям.

Надёжность можно повысить применяемостью системы, чем больше проектов производится, тем больше вероятность обнаружения ошибок, и вследствие этого – устранение недостатков системы во всех проектах одновременно. Также необходимо применять протоколы обмена, хорошо себя зарекомендовавшие в использовании, такие как «ModBus», «BSAP» и т.п. для оборудования, «LOTOS», «LOTOS2», «XNetwork» (основой которого является XML) и т.п. для компьютеров, чтобы повысить надёжность интерфейсов. Также надёжность можно повысить, изменяя принцип построения программного обеспечения, переход от стандартного программирования с зависимыми деревьями к независимым модулям связанных на основе графов.

Расширяемость приложения достигается за счёт модульности и поддержки встроенных средств программирования, что также позволит изменять систему «на ходу», создавая или уничтожая элементы управления, сетевые соединения, сигналы, команды и связи между этими элементами в рабочем режиме, чем и достигается изменяемость. Описание проекта на основе XML позволит редактировать проект без специальных средств и пользоваться системой контроля версий, к примеру SVN.

Для упрощения создания проекта необходим редактор, который позволит редактировать систему в рабочем режиме, используя «Drag and drop» (перетаскивание элементов на рабочую область при помощи мыши). Кроме того, необходим язык программирования, встроенный в среду, для задания специфических действий, а также написания программ тестирования проверяемого оборудования. Язык программирования должен отвечать следующим параметрам: возможность написания программ на родном языке (в нашем случае русский), поддержка ООП, для работы с элементами управления, сетевыми соединениями, шаблонами отчётов, сложными аппаратными частями. Примером тако-

го языка является Паскаль, который хорошо зарекомендовал себя для обучения программированию, только для XPhoenix потребуется использование его на русском языке. Также хорошим примером является язык LISP, который по своей структуре напоминает XML и удобен для хранения и воспроизведения в форме дерева, что быстро позволит создавать графическое представление, и наоборот.

Под информативностью понимается база данных, которая позволяет просматривать хронологию использования тех или других ресурсов. Так как связь элементов системы динамична и есть возможность отделения некоторых ПК от основного, то база должна иметь возможность производить периодическую сборку информации со всей системы.

Защищённость системы подразумевает возможность создания учётных записей, разграничение прав, ограничение от несанкционированного доступа, к примеру, редактирование системы или попадание вируса, т.е. в системе должна находиться база данных пользователей, которая хранит параметры доступа и пароли, а также CRC суммы для отслеживания изменений проекта и двоичных файлов.

Такая система позволит создавать системы распределённо, быстро, с меньшим количеством ошибок, что позволит производить большее количество проектов за то же время, что и обычным способом. Кроме того, часть проекта возможно передавать разработчикам аппаратной части проекта.

ЛИТЕРАТУРА

1. *Баженова И.Ю.* Delphi 5. Самоучитель программиста. М.: КУДИЦ–ОБРАЗ, 2001. 336 с.

2. *Фаронов В.В.* Искусство создания компонентов Delphi. Библиотека программиста. СПб.: Питер, 2005. 463 с.

3. *Ельманова Н., Трепалин С., Тенцер А.* Delphi и технологии COM. Мастер-класс. СПб.: Питер, 2003. 698 с.

СИНТЕЗ СИСТЕМЫ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ ТЕМПЕРАТУРОЙ ЖИДКОСТИ С ОБРАТНОЙ СВЯЗЬЮ ПО ТЕПЛОСОДЕРЖАНИЮ

В.А. Данилушкин, к.т.н., ассистент, П.И. Рубан, аспирант, каф. электроснабжения промышленных предприятий

Самарский гос. технический университет, epp@samgtu.ru

Рассматривается проблема управления процессом нагрева вязких жидкостей в проходном индукционном нагревателе. Исследуемый объект относится к объектам с распределенными параметрами. Задача реализации систем управления объектами с распределенными пара-

метрами значительно усложняется по сравнению с системами с сосредоточенными параметрами как за счет необходимости осуществления пространственно-распределенного контроля состояния объекта, так и за счет необходимости построения регуляторов с пространственно-распределенными управляющими воздействиями.

При транспортировке вязких жидкостей поток жидкости носит ламинарный характер. В зависимости от физических характеристик жидкости (теплопроводности, вязкости) и требований к точности стабилизации температуры закон регулирования может быть сформирован на основании информации о температуре трубы, либо по информации о средней температуре потока жидкости на выходе из теплообменника, либо по теплосодержанию жидкости на выходе из нагревателя. Однако реализация системы автоматического управления с обратной связью по температуре стенки трубы возможна лишь в случае турбулентного течения жидкости. При ламинарном течении жидкости, которое имеет место в исследуемой установке, система с обратной связью по температуре трубы не обеспечивает требуемой точности стабилизации температуры потока.

Система с обратной связью по средней температуре жидкости дает удовлетворительные результаты в тех случаях, когда можно пренебречь неравномерностью распределения скорости по сечению потока. Однако, как следует из выполненных авторами расчетов, при нагреве высоковязких жидкостей пренебрежение этим фактором может привести к значительной погрешности. Более высокую точность позволит обеспечить система регулирования, замкнутая по выходному теплосодержанию.

Для реализации системы автоматического регулирования с обратной связью по теплосодержанию сечение потока жидкости делится на несколько условных кольцевых зон, в пределах каждой из которых температуру жидкости и скорость можно считать постоянной. Количество зон, или число точек измерения температуры по сечению потока, определяется требованиями к точности поддержания теплосодержания на выходе из нагревателя, вязкостью жидкости, теплопроводностью и рядом других факторов. Теплосодержание жидкости на выходе из нагревателя при известной температуре определится простым суммированием теплосодержаний всех зон, т.е.

$$\sum_n Q_n = Q_1 + Q_2 + ... + Q_n = c_1 m_1 T_1 + c_2 m_2 T_2 + ... + c_n m_n T_n ,$$

где c_n, m_n, T_n – соответственно удельные значения теплоемкости, массы и температуры жидкости в n-м сечении потока.

Контроль температурного распределения в идеальном варианте предполагает использование датчиков температуры, распределенных по всему сечению. Однако на практике такой контроль осуществить не представляется возможным. В реальной ситуации контроль температуры потока жидкости осуществляется с помощью термопар, установленных на выходе из нагревателя в дискретных точках по сечению потока. Как показывают эксперименты, для оценки температурного распределения и теплосодержания жидкости достаточно иметь четыре установленных на различном расстоянии от стенки трубы датчика температуры жидкости. Система автоматического регулирования включает ПИ-регулятор с обратной связью по теплосодержанию в выходном сечении нагревателя. С этой целью в цепь обратной связи вводится дополнительно вычислительный блок, в который поступает информация о температуре жидкости в каждом сечении потока, скорости и сведения о константах, таких, как плотность жидкости, теплоемкость, температура жидкости на входе в нагреватель.

Для моделирования системы управления использовались возможности среды технологических расчётов – Matlab®, а также сопутствующей системы для моделирования динамических нелинейных систем – Simulink®. Температурное поле как функцию распределения внутренних теплоисточников можно рассчитать, используя инструментарий Matlab для решения дифференциальных уравнений в частных производных – PDE Toolbox (Partial Differential Equation Toolbox). Проведен анализ качественных показателей работы предложенной системы регулирования при отработке возмущающих воздействий по различным каналам воздействий. Результаты анализа свидетельствуют об удовлетворительных качественных показателях работы системы.

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ КОНСТРУИРОВАНИЯ 3D-ИЗОБРАЖЕНИЯ СЕРДЦА ПО ТОМОГРАФИЧЕСКИМ СНИМКАМ

А.Н. Дымченко, студент 3-го курса

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, mailagentrus@mail.ru

Для повышения качества диагностики нарушений ритма и патологий сердца, при проведении операций с использованием рентгеновских установок и систем навигации внутрисердечных электродов необходимо знать точную структуру сердца, информацию о которой наглядно демонстрирует 3D-модель. Трехмерная модель сердца может быть составлена по набору томографических снимков. Компьютерная томография является одним из основных способов клинической диагности-

ки пациентов с сердечными заболеваниями. В результате обследования человека с помощью компьютерного томографа получают серию изображений. Томография внутренних органов человека завоевала популярность благодаря высокой точности, информативности.

Целью данной работы является создание программного комплекса для конструирования 3D-модели сердца из последовательности срезов томографических изображений.

Для построения 3D-модели из множества плоских изображений слоев, полученных при компьютерной томографии или магнитно-резонансной томографии, используется алгоритм марширующих кубов [1].

Трехмерная модель, составленная из дискретного набора томографических снимков, улучшает качество восприятия информационного поля хирурга: дает более полные знания о его структуре перед встречей с пациентом, перед проведением операции и во время нее.

Каждый слой сохранен в формате DICOM. DICOM-файл – объектный файл с теговой организацией для представления кадра изображения (или серии кадров) и сопровождающей/управляющей информации в виде DICOM тегов [2].

Слои имеют равную толщину (например, фотографируется один слой на миллиметр) и равное количество пикселей на каждый слой.

Таким образом, входными данными является регулярная сетка вокселей. Воксель – элемент объёмного изображения, содержащий значение элемента растра в трёхмерном пространстве. Воксели являются аналогами пикселей для трехмёрного пространства (рис. 1).

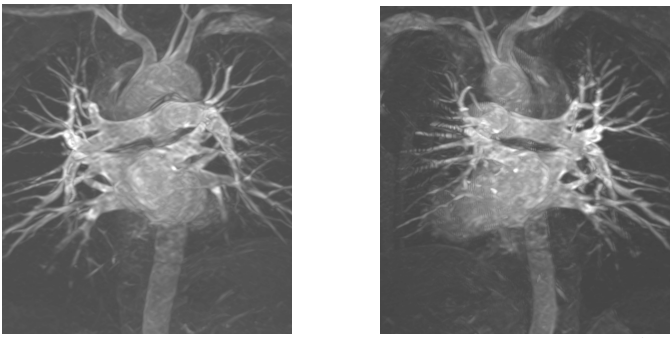


Рис. 1. Результат построения 3D-изображения сердца по 32 томографическим снимкам с использованием алгоритма марширующих кубов. Слева фронтальная проекция, справа – 135°

Алгоритм марширующих кубов используется для преобразования набора вокселей в полигональную модель. Реализованный алгоритм Marching Cubes анализирует скалярное поле (сетку вокселей), на каж-

дой итерации просматривая 8 соседних позиций (вершины куба, параллельного осям координат), и определяет полигоны, необходимые для представления части изоповерхности, проходящей через данный куб. Далее на экран выводятся полигоны, образующие заданную изоповерхность.

Результатом данной работы является разработанный программный комплекс, основными возможностями которого являются:

- возможность чтения и редактирования результатов томографического обследования;
- пакетная обработка томографических снимков;
- построение 3D-модели по набору срезов.

Основное достоинство программного комплекса – высокая скорость работы. Построение 3D-модели по 32 томографическим снимкам с разрешением 512×512 занимает не более 3 с на компьютере с тактовой частотой процессора 1,8 GHz.

Трехмерная модель может быть экспортирована в файл формата raw.

ЛИТЕРАТУРА

1. *Lorensen W.E. and Cline H.E.* Marching Cubes: A high Resolution 3D-surface Construction Algorithm. 1987. ACM Siggraph. С. 163–169.

2. National Electrical Manufacturers Association . Digital Imaging and Communications in Medicine (DICOM). Part 1: Introduction and Overview. URL: ftp://medical.nema.org/medical/dicom/2009/08_01pu.pdf. Дата обращения: 22.02.2011.

СУЩЕСТВУЮЩИЕ ПОДХОДЫ К СЖАТИЮ ДАННЫХ РАЗЛИЧНОГО ТИПА

О.О. Евсютин, аспирант каф. КИБЭВС

Научный руководитель С.К. Росошек, доцент каф. КИБЭВС, к.ф.-м.н.

г. Томск, ТУСУР, ФВС, eoo@keva.tusur.ru

Под сжатием (компрессией) данных понимается их преобразование с целью уменьшения объема. Иногда по отношению к этому процессу используют термин «кодирование», поскольку при сжатии информации осуществляется переход от одного представления к другому, исходные коды заменяются новыми с меньшей средней длиной. Сжатие является возможным в том случае, если данные обладают избыточностью, максимальное устранение которой и является конечной целью рассматриваемого процесса [1].

В общем случае, если речь идет о некоторых произвольных данных, избыточность заключается в наличии повторяющихся единиц

данных или групп единиц данных и называется статистической. К данным такого типа обычно относят тексты на естественном или искусственном языках, тогда единицами данных являются символы соответствующего алфавита. В качестве примера можно привести любое литературное произведение, текст которого представлен в электронном виде, а также тексты программ, представляющие собой последовательности команд языка программирования высокого уровня или машинных кодов.

Слово «произвольные» означает, что данные такого типа не обладают никакими особенностями, за исключением статистической избыточности, и воспринимаются как некий текст.

Основной подход к устранению статистической избыточности заключается в том, что часто встречающимся единицам данных, то есть символам алфавита, ставятся в соответствие короткие коды, а редко встречающимся – длинные, и такие методы сжатия называются статистическими [2].

Вариантом данного подхода являются словарные методы сжатия, когда короткие коды ставятся в соответствие часто встречающимся последовательностям символов – «словам», – а редко встречающиеся последовательности могут быть оставлены без изменений.

Когда по мере развития вычислительной техники начали активно использоваться цифровые изображения, возникла необходимость разработки алгоритмов, предназначенных для сжатия данных такого типа. Эта необходимость была обусловлена тем, что, несмотря на явное наличие избыточности в цифровых изображениях, статистические методы сжатия оказались для них абсолютно неприменимыми.

Между текстовой информацией и изображениями существует ряд важных с точки зрения сжатия отличий:

1. Множеством значений, которые могут принимать элементы изображения – пиксели, нельзя оперировать так же, как алфавитом, на котором строится текст. Во-первых, соседние символы алфавита никак не связаны между собой, в то время как пиксели с близкими значениями кажутся одинаковыми для человеческого глаза. Во-вторых, в случае изображений с большим количеством цветов (16- или 24-разрядных) невозможно работать со статистической таблицей такого объема.

2. Каждый язык, как естественный, так и искусственный, обладает определенными особенностями, однако при сжатии все эти особенности учесть невозможно, поэтому считается, что рядом расположенные символы текста никак не коррелируют между собой. Сжатие изображений опирается на противоположный принцип – предположение, что расположенные рядом пиксели совпадают или незначительно отлича-

ются друг от друга. Такая особенность изображений называется пространственной избыточностью. Следует отметить, что описанный тип пространственной избыточности характерен, прежде всего, для непрерывно-тоновых изображений. Кроме того, изображение в отличие от текста является двумерным, поэтому корреляция пикселей наблюдается как по горизонтали, так и по вертикали.

3. На сегодняшний момент лишь человек, но не компьютер может определить, какая часть текста является малозначимой и может быть удалена без ущерба для восприятия, кроме того, для большинства текстов такая операция вообще невозможна, в то время как, задав необходимый уровень качества, из изображения можно необратимо удалить часть информации, поэтому наиболее эффективными методами сжатия изображений являются методы сжатия с потерями.

Статистические методы, описанные выше, не применяются для сжатия изображений в явном виде. Единственным исключением являются монохроматические (двуцветные) изображения, типичные, к примеру, для факсимильной связи, которые сжимаются с помощью кодирования длин серий черных и белых пикселей (пелов). Методы сжатия изображения других типов (полутоновых, непрерывно-тоновых, дискретно-тоновых) основываются на устранении пространственной избыточности путем преобразования изображения к новому виду, подходящему для дальнейшего применения какого-либо из статистических алгоритмов сжатия [3].

Сжатие звука осуществляется аналогичным образом. Конечно, звук имеет свою собственную специфику, не характерную для изображений, однако общим является то, что из звукового файла, как и из изображения, можно удалить часть информации незаметно для человеческого восприятия. Существуют так называемые психоакустические модели, учитывающие особенности восприятия звука слуховым аппаратом человека, которые определяют, какие сэмплы могут быть безвозвратно удалены из оцифрованного звукового сигнала, и после соответствующего преобразования каким-либо из статистических алгоритмов производится сжатие оставшихся.

Наиболее сложным типом данных в рассматриваемой последовательности являются видеоизображения, которые сочетают в себе последовательность неподвижных изображений – кадров, и звуковое сопровождение. Однако при сжатии две эти составляющие не оказывают никакого влияния друг на друга, поэтому сжатие звукового ряда видеофайла ничем принципиально не отличается от сжатия обычного звукового файла.

Особенностью видеоизображений является временная избыточность – не только пиксели в пределах некоторой окрестности отдельно

взятого кадра могут принимать близкие значения, но и соседние кадры могут быть похожи друг на друга. Для устранения избыточности такого типа разрабатываются алгоритмы, осуществляющие поиск движения в следующих друг за другом кадрах, таким образом, если два соседних кадра содержат одинаковые блоки пикселей, смещенные один относительно другого на некоторое число позиций, достаточно осуществить сжатие выбранных блоков в первом кадре, который в этом случае называется опорным, а для второго блока записать соответствующие смещения.

ЛИТЕРАТУРА

1. *Ватолин Д., Ратушняк А., Смирнов М., Юкин В.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М.: ДИАЛОГ-МИФИ, 2002. 384 с.

2. *Сэломон Д.* Сжатие данных, изображений и звука. М.: Техносфера, 2004. 368 с.

3. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. М.: Техносфера, 2005. 1072 с.

СИСТЕМА РАЗРАБОТКИ ОБРАЗОВАТЕЛЬНОГО КОНТЕНТА

С.И. Франчук, Н.С. Савченко,
А.В. Титков, директор МСБИ «Дружба», к.т.н..
г. Томск, ТУСУР, ФЭТ, xcorter@mail.ru

Образование является одним из важнейших элементов профессиональной деятельности любого человека. Развитие информационных технологий позволяет говорить о непрерывном образовании, когда обучающийся имеет доступ к образовательным ресурсам 24 часа в сутки из любой точки мира. Вместе с тем роль печатных изданий в образовательном процессе все так же является одной из первостепенных. Образовательные учреждения стоят перед сложной задачей публикации своих образовательных ресурсов в различных форматах. Задача чрезвычайно сложная, т.к.:

1) видов образовательных ресурсов большое количество (учебные пособия, конспекты лекций, тесты, презентации и т.д.);

2) способов представления образовательных ресурсов огромное количество (печатное издание, электронное издание в виде файла (PDF, DOC, ODT, TeX), пособия в электронной библиотеке, курса в системе дистанционного обучения, пособия на CD и т.д.);

3) внешний вид образовательных ресурсов необходимо быстро изменять/адаптировать (обучающийся может заказать печатное издание в разных форматах – A4 или A5; для различных устройств, таких

как КПК, смартфон, нетбук и т.д., необходимо адаптировать внешний вид образовательных ресурсов).

В настоящее время решение задачи преобразования образовательных ресурсов в различные форматы производят в основном в ручном режиме, который является трудоемким, долгим и дорогостоящим процессом.

Кроме этого, перед образовательными учреждениями стоит множество других задач, связанных с образовательными ресурсами: управление образовательными ресурсами в рамках всего учреждения, разработка образовательных ресурсов, их поддержка и модификация.

В настоящее время не существует комплексного решения, которое решало бы все задачи, связанные с образовательными ресурсами.

Предлагаемая система разработки образовательного контента позволяет:

- организовать среду разработки и централизованного хранения образовательных ресурсов;
- обеспечить снижение сроков разработки учебных курсов и электронных изданий;
- разрабатывать электронные образовательные издания с учетом семантики контента как на основе уже существующих текстовых материалов, так и при разработке контента с нуля и представлять их в различных форматах.

Основные характеристики системы:

- система выполнена в виде Web-приложения, что делает её кроссплатформенной, для работы необходимо лишь наличие web-браузера;
- редактирование материалов происходит в режиме WYSIWYG;
- поддерживает работу с математическими формулами;
- поддерживает различные виды ресурсов (теоретический материал, вопросы, тесты, глоссарий и т.д.);
- позволяет импортировать ресурсы из различных форматов (MS Word, Open Office Writer, HTML, IMS Content Package, IMS QTI, SCORM, Moodle);
- позволяет экспортировать ресурсы в различные форматы (HTML, IMS Content Package, IMS QTI, SCORM, Moodle, TeX);
- унификация обеспечивает совместное многократное использование электронных ресурсов и их интероперабельность (независимость от технической и программной платформы), что существенно экономит время и материальные затраты при подготовке образовательных материалов и в ходе образовательного процесса.

В настоящее время система находится в стадии реализации.

Современные системы образования с каждым годом выдвигают все большие требования к методам обучения, поэтому система разработки образовательного контента сможет стать неотъемлемой частью любого образовательного учреждения, позволяя экономить время на разработку учебных курсов и увеличить качество обучения.

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ПУАРО

А.И. Гуляев, А.В. Ефремкин, Р.Р. Вильданов, студенты,
А.А. Шелупанов, проф., проректор по научной работе
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, gai@keva.tusur.ru

Комплекс MatLab очень разнообразен и функционален. Он включает в себя модули, не только помогающие в решении математических уравнений, но также и средства для построения нейронных сетей. А встроенный язык программирования еще больше расширяет функционал программы. Использование данной среды разработки для построения системы с принятием решений позволит автоматизировать процесс поиска и анализа больших объемов информации. А дополнительные алгоритмы анализа, такие как стеммер портера и определение тональности текста, позволят использовать информационные ресурсы оптимальным образом.

Принцип работы системы анализа и принятия решений

Выбор данной среды не случаен. В комплекс MatLab входит инструмент для создания нейронных сетей (Neural Network Toolbox), включающий в себя шаблоны простейших сетей, что позволяет освоить принципы их работы. Но прежде чем начать работать с нейронной сетью, ее нужно обучить. То есть задать набор входных и выходных данных. Данный процесс очень трудоемкий и долгий. Но его можно избежать, используя нейронные сети, которые обучаются сами – «без учителя». Для работы такой сети необходимы лишь некоторые начальные значения. Какие? В этом и заключается основная сложность систем с принятием решений. Перед нами встает сразу три задачи. Во-первых, необходимо представить входящую информацию (символьные строки) в числовой форме. Во-вторых, отсеять коэффициенты, значения которых минимально влияют на результат. В-третьих, необходимо учесть тональную окраску текста. То есть уметь определять те части текста, на которые обращает внимание сам автор. Например, выделенные курсивом слова и фразы помечать как имеющие больший приоритет (ранг). В первом случае мы можем воспользоваться ранжировани-

ем по частоте встречаемости слов в тексте, с применением так называемого «стеммера портера».

Стеммер портера – алгоритм нахождения основы слова для заданного языка и отсекания окончаний и суффиксов. Этот алгоритм необходим для более качественного отбора входных данных. Ведь разные падежи и склонения не меняют смысл слова, однако они влияют на количество слов и могут распознаваться системой как разные, что может исказить результаты анализа. Со второй проблемой справиться гораздо сложнее. Ведь слово, передающее весь смысл текста, может встретиться в нем всего несколько раз.

Чтобы найти решение для данной проблемы, целесообразно использовать метод Зипфа. Третья проблема только на первый взгляд кажется наименее важной. Однако часто оказывается, что автор самостоятельно выделяет из текста все наиболее важные аспекты, нахождение которых поможет значительно улучшить результаты анализа. Данный метод основан на утверждении, что слова, содержащие большее количество букв, встречаются в тексте реже коротких. Исходя из этого, Зипф вывел два универсальных закона: «ранг – частота» и «количество – частота». Для первого закона необходимо найти количество вхождений каждого слова в тексте. Далее каждому слову необходимо присвоить ранг. Слова, которые встречаются чаще других, будут иметь ранг 1, а самые редкие – n. Если слова имеют одинаковый ранг, то они группируются, и в дальнейших расчетах используется любое из этой группы. Далее, если умножить частоту вхождения слова в тексте на ранг частоты и поделить на общее количество слов, то получившаяся величина приблизительно постоянна! Из этого следует, что если самое популярное слово встречается в тексте, например, 100 раз, то следующее по популярности не будет встречаться 99 раз. Следующее после самого популярного встретится около 50 раз. Значение коэффициента для разных языков отличается. Для английского это примерно 0,1, а для русского языка – 0,6–0,7.

Второй закон Зипфа «встречаемость – частота» опирается на тот факт, что разные слова входят в текст с одинаковой частотой. Частота и количество слов, входящих в текст с этой частотой, тоже связаны между собой. Если построить график, отложив по одной оси (оси X) частоту вхождения слова, а по другой (оси Y) – количество слов в данной частоте, то получившаяся кривая будет сохранять свои параметры для всех без исключения созданных человеком текстов (рис. 1).

Из графика видно, что значимые слова располагаются в центре. Значит, самые популярные и редкие слова не несут в себе смысловой нагрузки, и их можно отсеять. Однако если мы возьмем слишком маленький интервал значимых слов, то можем получить слишком мало

информации, а если интервал будет большой, то в результате окажется слишком много лишнего.

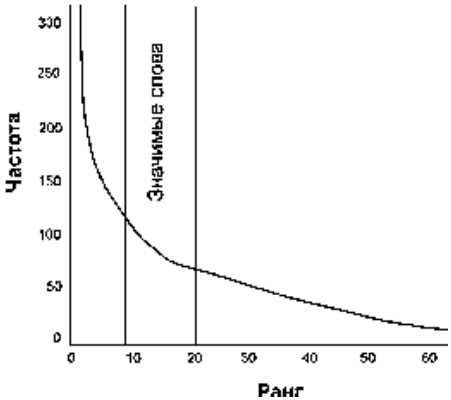


Рис. 1. График зависимости ранга от частоты

Вернемся к нейронным сетям. Не всю информацию можно связать друг с другом напрямую, нейронные сети без учителя позволяют находить такие связи, так как имеют запрограммированные начальные значения. В качестве примера можно привести нейронные сети Кохонена. Они являются сетью без учителя [1]. Также одним из вариантов сети, являются самоорганизующиеся карты Кохонена, основной задачей которых является классификация и последующая кластеризация. Задача классификации представляет собой задачу отнесения образца к одному из нескольких попарно не пересекающихся множеств. То есть мы разделяем информацию об объекте на куски. Далее каждый кусок, по выбранным критериям, соотносится к определенному классу, после чего можно получить информацию о принадлежности объекта к определенному классу (кластеризация). Примером может послужить задача нахождения наиболее выгодного партнера для бизнеса или поиск наиболее выгодных условий для получения кредита в банке. При использовании среды MatLab можно в наглядной форме получить информацию о результатах работы нейронной сети.

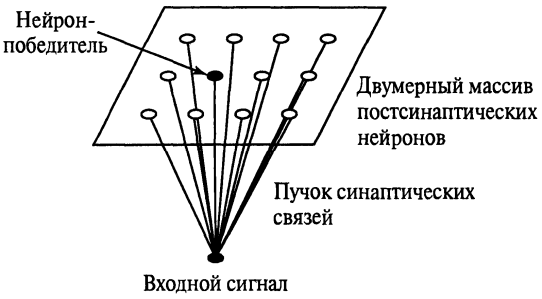


Рис. 2. Самоорганизующаяся карта признаков (модель Кохонена)

Данный процесс является кластеризацией, так как он соответствует основным его критериям схожести объектов в рамках одного кластера и их различия между кластерами. Большим преимуществом является то, что система может изначально не знать, сколько кластеров потребуется, и по мере надобности она сама создаст необходимые разделы. Данный метод позволяет системе работать максимально приближенно к человеческому мозгу, проводя самостоятельный анализ полученных данных и фактов [2]. На выходе возможно будет получить наглядные данные, которыми может воспользоваться аналитик или лицо, принимающее решения.

Таким образом, применение MatLab для кластерного анализа на нейронных сетях является оправданным для вопросов, связанных с принятием решений. Однако можно получить систему, которая может обрабатывать почти любые данные не только в рамках поставленной задачи. Данная особенность позволяет расширить спектр использования данной системы не только в системах продержки принятия решений, но и во многих других областях.

ЛИТЕРАТУРА

1. *Хайкин С.* Нейронные сети. Москва; Санкт-Петербург; Киев: Вильямс, 2006.

2. *Рутковская Д.* Нейронные сети, генетические алгоритмы и нечеткие системы. М.: Горячая линия – Телеком, 2006.

3. *Медведев В.* Нейронные сети. MATLAB 6. М.: ДИАЛОГ-МИФИ, 2002.

ФОТОИМПУЛЬСНЫЙ ДАТЧИК ОБРАТНОЙ СВЯЗИ

Г.В. Ильичев, студент 5-го курса, П.Н. Коваленко, инженер, к.т.н., В.А. Бейнарович, проф., д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, ФВС igv@sibmail.com

В системах автоматизированного управления особое внимание уделяют механизмам и принципам обратной связи. Одним из видов регулируемого электропривода является тиристорный электрический привод. В совокупности с электродвигателем постоянного тока этот привод является основным средством преобразования электрической энергии в механическую. Система числового программного управления электроприводом «КЕМЕК» предназначена для управления текущим угловым положением вала двигателя в соответствии с управляющей программой. Управляющая ЭВМ последовательно посылает команды управления и принимает текущее положение двигателя для оп-

ределения ошибки позиционирования. Данная система используется в учебной лабораторной установке, на которой студенты изучают вопросы программирования, наладки и эксплуатации реальных систем ЧПУ. Для определения положения ротора двигателя в пространстве применяют различные способы слежения. В системах числового программного управления (ЧПУ) наибольшее распространение получили фотоэлектрические средства обратной связи [1]. Одним из таких средств является фотоимпульсный датчик (ФИД), описание и принцип работы которого рассмотрен в проделанной преддипломной практике и изложен в данной работе.

Фотоимпульсный датчик служит для получения информации о положении ротора относительно осей фазных обмоток статора. Датчик состоит из трёх основных частей: механической, оптической и электронной. Механическая часть обеспечивает вращение вала датчика относительно корпуса. В основе датчика лежит диск, который соосно соединяется с валом двигателя.

Оптическая часть содержит светодиод с линзой, растровую индикаторную пластину, растровый диск и фотодиоды. Растровый диск и растровая индикаторная пластина в паре создают растровое сопряжение. На индикаторной пластине растры расположены в два сектора, сдвинутые один относительно другого на 1/4 шага растров. Два фотодиода, установленные над каждым из секторов растровой пластины и сопрягаемыми с ними растрами диска, выдают несформированные сигналы $U_а$ и $U_в$, как показано на рис. 1, 2. Фотодиод, расположенный в центральной части растрового диска, выдает несформированный нулевой сигнал $U_к$.

Схема согласования сигналов фотоимпульсного датчика осуществляет питание датчика напряжением 5 В и согласование сигналов микроконтроллера и ФИД. Преобразование двухфазных импульсных сигналов в цифровую форму и синхронизация оцифрованной величины нулевым сигналом осуществляется программным обеспечением микроконтроллера [2]. При оцифровке определяется направление вращения и положение ротора в пространстве.

При вращении импульсного диска меняются световые потоки от источников света (ИС1) и (ИС2), которые воспринимаются чувствительными элементами (ЧЭ1) и (ЧЭ2). Они преобразуют световые сигналы в электрические импульсы. Логическая схема формирования импульсов отработки (СФИО) формирует две последовательности импульсов, каждая из которых сдвинута относительно другой на 90° и синхронизирована со статорными обмотками. Структурная схема фотоимпульсного датчика изображена на рис. 3.

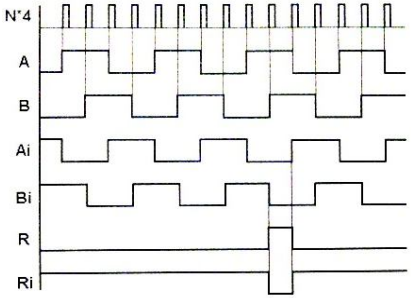


Рис. 1. Вращение вала против часовой стрелки

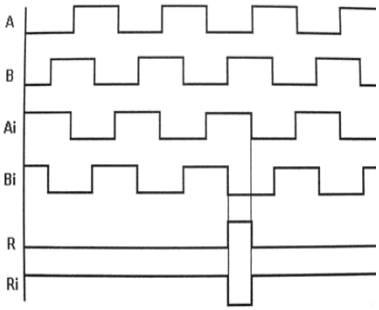
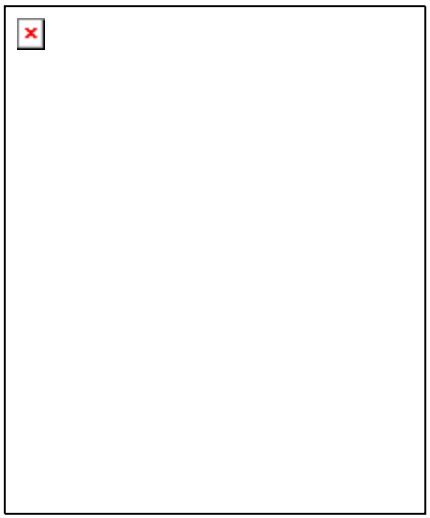


Рис. 2. Вращение вала по часовой стрелке



Фотоимпульсный датчик подключён к ротору электродвигателя через муфту, которая имеет коэффициент передачи 4. На периферии диска выполнено на 2500 делений. Таким образом, дискретность отсчёта перемещений фото импульсным датчиком равна:

$$1:2500\times4 = 1:10000 = 0{,}036°.$$

Рис. 3. Структурная схема фотоимпульсного датчика

Таким образом, рассмотренная конструкция фотоимпульсного датчика применяется в системе обратной связи по определению пространственного положения ротора электродвигателя в системе числового программного управления в составе комплекса «КЕМЕК», который успешно используется при выполнении лабораторных работ по дисциплине «Теория автоматического управления».

ЛИТЕРАТУРА

1. *Чернов Е.А., Кузьмин В.П.* Комплектные электроприводы станков с ЧПУ: Справ. пособие. Горький: Волго-Вятское кн. изд-во, 1989. 320 с.

2. Исследование системы ЧПУ оборудованием с приводом постоянного тока и датчиками положения: руководство к лаб. работам. Томск, 2003. 40 с.

ПОЛУЧЕНИЕ ДАННЫХ С УСТРОЙСТВ СЕТИ, ИХ ОБРАБОТКА И ПРЕДСТАВЛЕНИЕ

С.Ю. Исхаков, аспирант;
Н.С. Козыренко, А.О. Шумская, студенты 3-го курса
г. Томск, ТУСУР, каф. КИБЭВС, frosty@ssmu.ru, anastasia91@sibmail.com, nattyk@sibmail.com

Сегодня практически каждая организация имеет свою локальную сеть, зачастую она имеет сложную структуру, включающую несколько подсетей. Чем крупнее компьютерная сеть, тем труднее организовать в ней управление и контроль над протекающими процессами. На базе локально-вычислительной сети СибГМУ [1] разрабатывается система управлению сетью (СУС).

Задачами разрабатываемой СУС являются:

- управление конфигурацией сети и именованием ее элементов;
- обработка ошибок;
- анализ производительности и надежности;
- управление безопасностью;
- учет работы сети.

Первичной задачей для реализации СУС стала организация получения данных о работе устройств сети. Существует концепция TMN (Telecommunication Management Network) [2], принятая для интегрированного управления сетями. Основная ее идея – обеспечение сетевой структуры для взаимодействия различных типов управляющих устройств и телекоммуникационного оборудования, использующих стандартные протоколы.

На основе этой концепции можно выделить два протокола, позволяющих осуществить получение данных с устройств сети: SNMP (Simple Network Management Protocol) и CMIP (Common Management Information Protocol) [2]. Последний является более гибким и масштабным, но вместе с тем требует ряд вспомогательных служб, объектов и баз данных объектов. И хотя он способен выполнять задачи, недоступные в SNMP, его применение является нецелесообразным из-за сложности протокольных данных и отсутствия необходимости в выполнении громоздких функций на практике.

Таким образом, для сбора информации был выбран протокол SNMP, работающий по схеме [3] взаимодействия между агентами, установленными непосредственно на устройствах сети, и менеджером управления, в качестве которого выступает сервер СУС. С помощью SNMP можно получить все необходимые данные для анализа производительности сети, учета работы аппаратных средств.

На рис. 1 схематично показана концепция работы SNMP по получению данных – взаимодействие агента и менеджера на основании моделей управляемых ресурсов, которые включают параметры, необходимые для контроля работы аппаратных средств. К примеру, модели управляемых ресурсов маршрутизатора и сервера будут отличаться, так как они выполняют разные задачи, и об их функционировании можно судить по различающимся показателям.

Рис. 1. Схема получения данных с помощью протокола SNMP

Разрабатываемая СУС основана на веб-интерфейсе, поэтому формы представления получаемых данных могут быть разнообразными. Был выбран способ графического представления в виде графиков.

Рынок предлагает ряд готовых программных продуктов, в том числе со свободной лицензией, способных собирать данные с устройств сети и представлять их в виде графиков. В их числе Cacti, SNM, Munin, aNTG. В основе большинства из них лежит утилита MRTG (The Multi Router Traffic Grapher), её прямой потомок RRDTool. Таким образом, выбор MRTG [4] или RRDTool [4] позволит внедрить в СУС гибкое средство визуализации данных, настраиваемое под изменяющиеся требования контроля сети.

RRDTool и MRTG доступны под GNU General Public License [4], кроссплатформенны и не отличаются по функционалу. Однако по ряду причин предпочтение было отдано RRDTool. В большей мере это связано со способом хранения результатов утилитой. RRDTool работает с Round Robin Databases (кольцевыми базами данных), что исключает переполнение жесткого диска сервера с установленной системой мониторинга, поскольку размеры БД четко фиксированы. В отличие от MRTG, RRDTool самостоятельно не помещает в архивы все устаревшие данные – сохраняет те, что были затребованы при проектировании базы, что также освободит сервер от хранения лишней информации.

Кроме удобства хранения данных, RRDTool обладает гибкой системой описания хранимой и отображаемой информации.

Выбранное средство позволяет хранить и отображать любые изменяющиеся во времени данные. В конкретной разрабатываемой СУС будут визуализироваться следующие параметры:

– загруженность канала (входящий, исходящий, максимальный, минимальный, средний трафик);

– использование процессоров, жестких дисков серверов.

Работа с RRDTool предполагает создание кольцевой базы, её наполнение, построение графиков на основе данных, хранимых в базе. Регулярный сбор необходимых показателей (через SNMP), их обработка и формирование на их основе графиков переложены на скрипты, написанные на языке Perl, который включает библиотеки для работы с RRDTool. Регулярное выполнение скриптов обеспечивается через планировщик заданий операционной системы.

В дальнейшем планируется описать модели управляемых ресурсов для всех типов устройств сети, развить систему оповещения администраторов при достижении контролируемыми параметрами установленных критических значений (обозначенных на графиках). Также в перспективе разработка и описание алгоритмов, унифицирующих действия администраторов при настройке утилит RDTool и SNMP на выполнение новых задач.

Выполнено в рамках проекта ГПО КИБЭВС-1002 – «Построение автоматизированной системы администрирования локально-вычислительных сетей».

ЛИТЕРАТУРА

1. *Исхаков С.Ю.* Анализ структуры сети учреждения здравоохранения // Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2010», Томск, 4–7 мая 2010 г. Томск: В-Спектр, 2010. Ч. 3. С. 40–42.

2. *Гребешков А.Ю.* Управление сетями электросвязи по стандарту TMN: учеб. пособие. М.: Радио и связь, 2004. С. 88–111.

3. *Кунегин С.В.* Архитектуры систем управления сетями. Протокол управления сетью SNMP [Электронный ресурс]. URL: http://kunegin. narod.ru /ref3/snmp/file0.htm

4. *Alex van den Bogaerdt.* RRDtool tutorial [Электронный ресурс]. URL: http://www.mrtg.org/rrdtool/tut/rrdtutorial.en.html

ОБЗОР СИСТЕМ УПРАВЛЕНИЯ СЕТЬЮ

С.Ю. Исхаков, аспирант
г. Томск, ТУСУР, каф. КИБЭВС, frosty@ssmu.ru
Научный руководитель А.А. Шелупанов, проректор по научной работе, проф., д.т.н.

Развитие систем управления сетью (СУС) [1] началось в конце 80-х гг. прошлого столетия. Одной из первых СУС был продукт SunNet Manager, ориентированный на управление коммуникационным оборудованием и контроль трафика сети. Международным союзом электросвязи (International Telecommunication Union, ITU) [1] разработана и утверждена концепция TMN (Telecommunication Management Network, TMN) [2]. Она определяет принципы создания СУС для сетей разных масштабов, независимо от объекта управления.

В соответствии с концепцией TMN процесс управления сетью включает в себя следующие функции управления:

1) управление конфигурацией сети и именованием;
2) обработка ошибок;
3) анализ производительности и надежности;
4) управление безопасностью;
5) учет работы сети.

Кроме разделения задач управления на группы, можно выделить уровни управления в соответствии с иерархией сети.

Нижний уровень определяется элементами сети (компьютеры, каналы передачи данных и т.д.). Элементы могут содержать встроенные средства для поддержки управления, а могут и требовать разработки специального устройства.

Следующий – уровень управления элементами сети. Это элементарные системы управления отдельными элементами сети, отделяющие СУС от особенностей управления конкретным оборудованием и моделирующие его поведение.

Над ним располагается уровень управления сетью. Он координирует работу элементарных систем управления, определяет работу сети как единого целого.

Далее расположен уровень управления услугами. В задачи уровня входят фиксация в базе данных параметров услуги, выдача уровню управления сетью задания на конфигурирование оборудования.

Последним является уровень бизнес-управления. Занимается долговременным планированием сети с учетом финансовой деятельности организации.

На каждом уровне иерархии модели TMN решаются задачи одних и тех же пяти функциональных групп, рассмотренных выше. Однако

на каждом уровне эти задачи имеют свою специфику. Модель TMN упрощенно можно представить в виде рис. 1 [3].

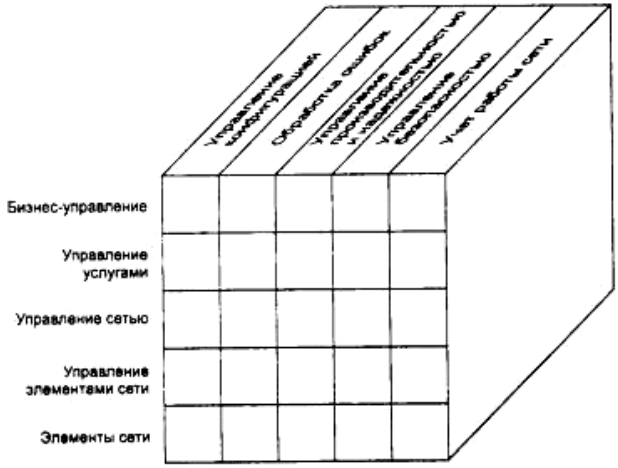


Рис. 1. Многоуровневое представление задач управления

Таким образом, СУС – это набор программных продуктов, предназначенных для решения перечисленных задач. Это могут быть продукты разных производителей, никак не связанные между собой. В зависимости от масштабов сети, типов устройств, используемых в ней и степени унификации можно выделить три типа СУС (таблица).

Классификация систем сетью

Тип	Описание
1	В управлении сетью применяются отдельные программные продукты для каждого сетеобразующего устройства. Примеры: Cisco ASDM, Esafe Security Center
2	Архитектура ПО для управления различными сетевыми устройствами и механизм управления ими похожи. Существует платформа, предоставляющая стандартный набор сервисов для множества модулей управления различными сетевыми устройствами и приложений для решения задач управления. Примеры: HP OpenView, IBM NetView, CiscoWorks
3	Аналогичен типу 2, но отличается наличием единого централизованного управления в рамках подхода к управлению информационными ресурсами. Примеры: Spectrum Enterprise Manager, Solstice Enterprise Manager, Cisco MARS

Недостатки СУС 1 типа очевидны: при большом количестве оборудования различных производителей применяется много различных программных продуктов. Успешное применение данного типа СУС возможно при преобладании в сети оборудования какого-либо производителя.

Одним из существенных недостатков СУС 2-го и 3-го типов является то, что при наличии в сети оборудования других производителей их типы определяются неверно. Кроме того, при управлении такими устройствами не поддерживаются специфические функции, отличающие данное оборудование от остальных.

К недостаткам СУС 3-го типа можно добавить еще некоторые:

1) Использование централизованного мониторинга не дает возможности анализировать состояние сети из любой ее точки. Представление о состоянии сети в данном случае получается неполным.

2) Диагностика доступности устройств и тестирование портов дают информацию только об активности устройства, но не отражают его производительности.

3) СУС предоставляют администраторам подробные отчеты о состоянии сети, количестве коллизий и т.д. Но все отчеты строятся на базе статистических данных. Отсутствие возможности анализа текущего трафика не дает возможности оценить текущее состояние и предотвратить сбои в сети.

В связи с вышеприведенной классификацией СУС возникает понятие платформы управления [1], которая складывается из трех составляющих: набора базовых компонентов, образующих ядро; совокупности принципов комплектования системы управления на данной платформе; множества элементов сети. Таким образом, система управления и платформа управления – это различные понятия, хотя платформа управления, как правило, может рассматриваться как частный случай СУС.

Поэтому если платформу управления можно выбирать, то СУС надо проектировать, определив решающие критерии. В большинстве случаев это: набор функциональных возможностей; стоимость; надежность [3].

На базе ЛВС Сибирского государственного университета Минздравсоцразвития РФ проводятся исследования [4], направленные на проектирование и разработку специализированной СУС.

ЛИТЕРАТУРА

1. *Гребешков А.Ю.* Управление сетями электросвязи по стандарту TMN: Учеб. пособие. М.: Радио и связь, 2004. С. 88–111.

2. ITU-T Recommendation M.3010. Principles for telecommunication management network. 2000.

3. Многоуровневое представление задач управления [Электронный ресурс] URL: http://lanhelper.ru/seti/7/3.

4. *Исхаков С.Ю.* Анализ структуры сети учреждения здравоохранения // Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2010», Томск, 4–7 мая 2010 г. Томск: В-Спектр, 2010. Ч. 3. С. 40–42.

СРЕДСТВА И МЕТОДЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ СОЕДИНЕНИЙ С ГАРАНТИРОВАННЫМ НАТЯГОМ

А.В. Кабакова, ст. преподаватель каф. ПиМКК, к.т.н.

Научный руководитель В.П. Иванников, зав. каф. СТИБ, проф., д.т.н.

г. Ижевск, ИжГТУ, sunanniv@mail.ru

Возможность применения ЭВМ и создание средств автоматизированного проектирования (САПР) изделий на основе соединений с натягом (СсН) требуют разработки такого подхода к оценке нагрузочной способности (НС), который объединял бы в себе и возможность оптимизации расчетов при проектировании СсН, и возможность экспериментального контроля результатов проектирования как при создании соединений, так и в процессе эксплуатации. Создание такой системы автоматизированного проектирования требует научно обоснованного выбора и учета всех факторов, определяющих основные параметры СсН, параметры процесса сборки, зависящие от размеров, вида соединений, технологии сборки и оборудования, которые могут влиять на НС соединения. Разработку комплексной САПР СсН целесообразно начинать с создания подсистем CAE/CAD, то есть с решения задач компьютиризованого конструкторско-технологического проектирования.

Нагрузочная способность СсН зависит, главным образом, от взаимодействия составных частей и условий сборки. Поэтому решение задачи конструкторско-технологического проектирования СсН следует начинать с разработки обобщенной геометрической модели соединения, соответствующей ему математической модели (ММ) и методики преобразования обобщенной геометрической и математической модели для получения того или иного частного решения. Результатом решения на основе разработанной обобщенной модели соединения и соответствующей ему ММ будет оптимизация технологических условий сборки-разборки на основе научно обоснованного выбора факторов и параметров, зависящих от размеров соединений и технологии сборки, а также возможность исследования новых перспективных конструктивных решений СсН.

Моделирование и учет влияния напряженно-деформированного состояния на эксплуатационную прочность СсН для всего многообразия параметров и условий сборки базируются на возможности получения точного аналитического решения многосвязной контактной упругой и упругопластических задач [1]. Математической моделью СсН является система дифференциальных уравнений, описывающая процессы, происходящие в объекте с заданием начальных и краевых условий. Как уже упоминалось, эта система уравнений известна под названием уравнений Ламе в механике сплошных сред [2].

Указанная математическая модель позволяет установить точную связь нагрузочной способности СсН с другими конструкторско-технологическими параметрами в виде:

$$HC[A,T,M_{\text{и}},M_{кр}] = f_{A,T,M_{\text{и}},M_{кр}}(\Delta, p_{\text{к}}, d'/d_2, \frac{l}{d'}, f_{mp}),$$

где $M_{\text{кр}}$ – крутящий момент сил, приведенный к единице поверхности; A – осевая сила; T – комбинированная сила (одновременное действие осевой силы и крутящего момента); $M_{\text{и}}$ – изгибающий момент; Δ – натяг в соединении; $p_{\text{к}}$ – контактное давление в сопряжении; d' – диаметр посадки; d_2 – внешний диаметр охватывающей детали; l – длина сопряжения; f_{mp} – коэффициент трения, с поправкой на шероховатость поверхности и реологические свойства смазки.

Нагрузочную способность цилиндрических и конических соединений с натягом обычно оценивают по формулам:

– при нагружении осевой силой НС:

$$A = \pi d' l p_K f \ ;$$

– при нагружении крутящим моментом:

$$M_{Kp} = \frac{1}{2}\pi d'^2 l p_K f \ ;$$

– при нагружении изгибающим моментом:

$$M_{II} = 0{,}2\, p_K d' l^2 \ ;$$

– при одновременном нагружении осевой силой и крутящим моментом:

$$T \le \sqrt{\left(\frac{2M_{Kp}}{d}\right)^2 + A^2} \ ,$$

где d' и l – диаметр и длина посадки; f – коэффициент трения; p_K – контактное давление на сопряженных поверхностях.

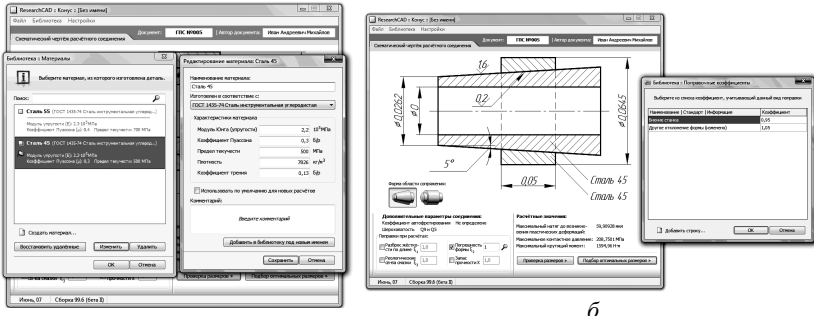
Таким образом, обобщенная формула расчета несущей способности соединения с натягом будет иметь следующий вид:

$$\text{НС} = \pi 2^{x} 10^{y} p_K d^m l^n f^p, \qquad (1)$$

где m, n или p могут принимать значения 0, 1, 2; x=1, –1 и y= –1, 0.

Разработка базовой программы расчета СсН в виде программной оболочки в среде Delphi на основе (1) обеспечивает получение точного аналитического решения и в то же время, при необходимости, предусматривает возможности применения численного моделировании на основе метода конечных элементов (МКЭ) на отдельных этапах расчета посредством подключения дополнительных программных модулей для уточнения отдельных параметров, коэффициентов и поправок, а также введения и использования данных эксперимента.

Разработанная программа состоит из ряда окон. В главном окне (рис. 1, *а*) задаются габаритные параметры соединения с натягом: внешний диаметр охватывающей детали, внешний диаметр охватываемой детали (вала), внутренний диаметр охватываемой детали (вала), длина прессового соединения. Здесь же вызывается окно библиотеки, в котором выбираются материалы для деталей, и окна библиотек поправочных коэффициентов (см. рис. 1, *б*).



а *б*

Рис. 1. Окна программы: *а* – главное окно, окно библиотеки и окно редактирования материала; *б* – главное окно и окно библиотеки поправок

На рис. 1, *б* показаны главное окно с чертежом и окно библиотеки поправочных коэффициентов.

Удобством программы в целом является возможность построения нескольких графиков зависимости для различных первоначальных параметров, что существенно облегчает анализ полученных данных.

ЛИТЕРАТУРА

1 *Абрамов И.В.* Высоконапряженные соединения с гарантированным натягом / И.В. Абрамов, Ф.Ф. Фаттиев, А.В. Щенятский и др. Ижевск: Изд-во ИжГТУ, 2002. 300 с.

2 *Гречищев И.С.* Соединения с натягом. Расчет, проектирование, изготовление / И.С. Гречищев, А.А. Ильяшенко. М.: Машиностроение, 1981. 247 с.

УЛЬТРАЗВУКОВАЯ ТОМОГРАФИЯ И УПРАВЛЕНИЕ КАЧЕСТВОМ ТЕХНИЧЕСКОЙ ДИАГНОСТИКИ СОЕДИНЕНИЙ С НАТЯГОМ

А.В. Кабакова, ст. преподаватель каф. ПиМКК, к.т.н.
Научный руководитель В.П. Иванников, зав. каф. СТИБ, проф., д.т.н.
г. Ижевск, ИжГТУ, sunanniv@mail.ru

При производстве изделий на основе соединений с натягом (СсН) необходимо учитывать и технологию изготовления деталей соединения, и особенности его сборки и последующей эксплуатации. Важнейшим фактором проектирования является анализ напряжённо-деформированного состояния (НДС) соединения, так как НДС непосредственно связано с главным и безусловным критерием работоспособности соединения, его нагрузочной способностью (НС) – прочностью. Прочность элементов конструкций СсН обеспечивается еще на стадии их проектирования. Однако изменение свойств материала в процессе эксплуатации, не говоря уже о различных нарушениях технологии производства и сборки, требует развития и применения методов и средств оценки реальной несущей способности материала в конструкции.

Вплоть до настоящего времени для прогнозирования эксплуатационного ресурса СсН использовались только методы статистического анализа накопленных данных, а в случае применения других методов говорилось только о возможностях качественной оценки состояния соединения. Поэтому очень важным, в этой части проблемы, представляется получение количественных данных о натяге, НДС в зоне сопряжения реализованных изделий, в том числе и для подтверждения расчётных характеристик и НС соединений, а также прогнозирования их долговечности. В этой связи сущностью проведенных нами исследований является развитие метода неразрушающего контроля напряжённо-деформированного состояния соединений с натягом с целью экспериментального определения максимально допустимой величины прикладываемых к объекту контроля силовых воздействий [1].

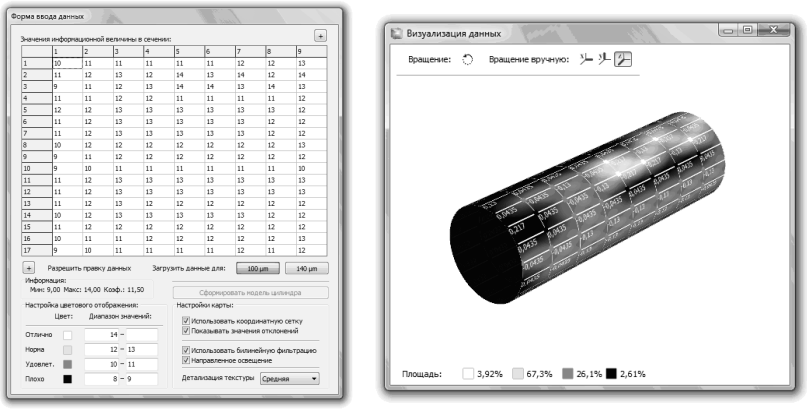
В наших исследованиях «томографический эффект» достигается с помощью ультразвукового (УЗ) эхо-импульсного метода за счёт того, что источник и приемник излучения неподвижны, а объект исследования может вращаться и поступательно двигаться относительно источника и приемника излучения, что легко достигается при выполнении условий автоматизации процесса измерений. Поскольку, по определению, двумерная томография, или 2D-томография – это многоракурсные исследования объекта в одной плоскости, то есть набор одномерных проекций плюс математическая обработка данных, то легко ви-

деть, что диаграммы ослабления акустического сигнала, полученные в разных сечениях прессового соединения, как раз и представляют собой результаты многоракурсного исследования объекта в одной плоскости, то есть 2D-томограмму напряженно-деформированного состояния зоны сопряжения, поскольку математическая обработка данных реализуется в дефектоскопе электронными средствами. Поэтому для получения УЗ томографического образа области сопряжения соединения с натягом нет необходимости в какой-то особой математической обработке, так как УЗ-преобразователь посылает ультразвуковую волну, которая частично отражается от микронеоднородностей напряженно-деформированной области натяга и возвращается к УЗ-преобразователю, где и регистрируется. А с помощью ЭВМ, по отношению амплитуд первого и второго отражений от каждой точки исследуемой области сопряжения, осуществляется вычисление показателей ослабления УЗ-волны и выполняется математическая реконструкция (строится трёхмерный образ) поверхности сопряжения в терминах коэффициента отражения сигнала (или ослабления) на экране дисплея.

По описанной методике были получены результаты многоракурсной съёмки для ряда соединений с натягом. На основе данных эксперимента выполняется математическая реконструкция поверхности сопряжения в терминах коэффициента отражения сигнала. Для этого были выполнены следующие шаги с массивами данных. В первую очередь проведено нормирование данных по максимальному значению. Это позволяет в последующем не вести контроль интерполированных данных по значению коэффициента отражения сигнала. На следующем шаге производим линейную интерполяцию массива данных и выборку опорных точек (сетки) интерполяции, что обеспечит корректные результаты преобразований. После этого по каждому из сечений производим кусочно-полиномиальную интерполяцию с заданной точностью, а затем и интерполяцию по длине объекта контроля. После завершения интерполяции строим карту интенсивностей и накладываем полученную текстуру на 3D-модель объекта контроля.

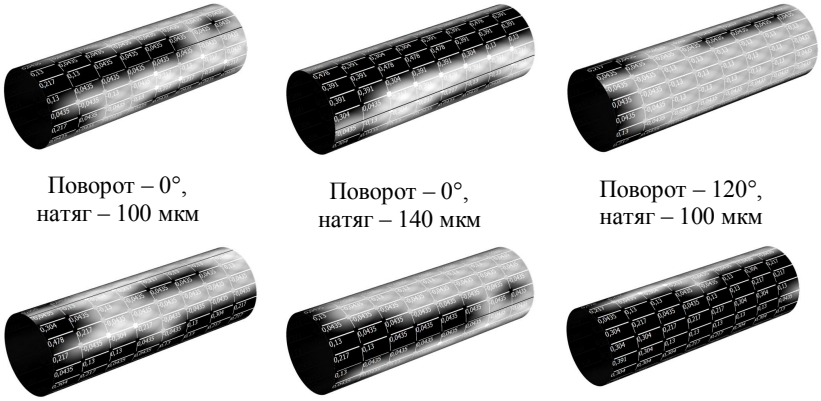
Программную реализацию описанного алгоритма осуществим в среде Delphi. Программа включает в себя два окна: первое – для ввода данных и указания сопутствующих настроек, а второе – непосредственно для вывода полученной томограммы.

Диалоговые окна программы показаны на рис. 1, а полученные с помощью программы томограммы соединений с натягом приведены на рис. 2.



а *б*

Рис. 1. Диалоговые окна программы построения томограмм:
а – окно вода данных; *б* – окно вывода томограмм



Поворот – 0°,
натяг – 100 мкм

Поворот – 0°,
натяг – 140 мкм

Поворот – 120°,
натяг – 100 мкм

Поворот – 120°,
натяг – 140 мкм

Поворот – 240°,
натяг – 100 мкм

Поворот – 240°,
натяг – 140 мкм

Рис. 2. Пример томограмм соединений с натягом на 100 мкм и 140 мкм
с поворотом на 0°, 120° и 240°.

ЛИТЕРАТУРА

1. *Буденков Г.А.* Ультразвуковой контроль качества соединений с натягом / Г.А. Буденков, В.П. Иванников, А.В. Кабакова, В.А. Стрижак // Дефектоскопия. 2009. №8. С. 73–81.

СИСТЕМА ОПТИМАЛЬНОГО ПО КРИТЕРИЮ ТОЧНОСТИ УПРАВЛЕНИЯ ИНДУКЦИОННЫМ НАГРЕВОМ КРУПНОГАБАРИТНЫХ КОЛЕЦ ПЕРЕД РАСКАТКОЙ

С.В. Князев, А.В. Кожемякин, аспиранты каф. электроснабжения промышленных предприятий

Научный руководитель А.И. Данилушкин, проф.

г. Самара, Самарский государственный технический университет, epp@samgtu.ru

Технологический процесс производства колес и бандажей включает в себя комплекс операций по нагреву заготовок в газовой печи, осадке и обжатию на прессах, транспортировке, прошивке отверстий и последующей горячей раскатке кольцевых заготовок. Температурное поле заготовки после всех рассмотренных операций становится неравномерным, на краях наблюдается недопустимое переохлаждение, что неминуемо ведет к браку в ходе завершающей операции – раскатки.

Для устранения этого положения в технологическую линию дополнительно вводится система индукционного нагрева, основная задача которой состоит в том, чтобы обеспечить требуемое распределение температуры по всему объему изделия за заданное время в условиях ограниченной вариации начального температурного распределения перед подогревом и тепловых потерь.

Рассмотрена задача оптимизации процессов индукционного нагрева в комплексе «нагреватель–деформирующее оборудование» при задании требуемого по технологии температурного распределения по объему изделия непосредственно перед раскаткой.

Расчет оптимальных алгоритмов функционирования индукционной установки выполняется при фиксированном времени транспортирования для технологической линии, состоящей из двух последовательно сменяющих друг друга во времени технологических звеньев – индукционного нагревателя и транспортирования заготовки к деформирующему оборудованию. Модель каждого звена представляется соответствующим уравнением нестационарной теплопроводности. На первой стадии это уравнение соответствует процессу нагрева ограниченного цилиндра внутренними источниками тепла в индукционной установке. Вторая стадия, представляющая собой процесс охлаждения нагретого изделия при его транспортировании к раскаточной машине в течение времени транспортирования, моделируется той же краевой задачей с увеличенными тепловыми потерями в условиях отсутствия внутренних теплоисточников.

Решение оптимальной задачи по критерию точности выполнено альтернансным методом. Показано, что в условиях исследуемой зада-

чи поставленным требованиям к конечному температурному распределению полностью удовлетворяет двухинтервальное оптимальное управление, причем второй интервал управления частично реализуется при охлаждении на воздухе в течение периода транспортирования изделия.

Основной задачей синтеза является построение структуры системы автоматической оптимизации режимов работы нагревательной установки с целью достижения заданной точности нагрева изделия до заданной температуры за фиксированное время. Поиск алгоритма управления в замкнутой системе автоматической оптимизации при переводе объекта из фиксированного начального положения в заданное основан на методе фазового пространства [1].

Для построения замкнутой системы оптимального управления индукционным нагревом необходим текущий контроль температуры в некоторых точках по объему нагреваемого изделия. Измерение температуры в точках контроля может быть реализовано, в зависимости от конкретных технических возможностей системы, либо непосредственно на управляемом объекте с помощью соответствующих датчиков обратной связи, требуемые коэффициенты передачи которых предварительно определяются расчетом, либо с использованием специализированных аналоговых или цифровых моделей процесса.

Результаты, полученные в ходе теоретических исследований, положены в основу при разработке реальной системы управления нагревом цилиндрических заготовок, встроенной в технологическую линию раскатки колец. Система управления нагревом заготовки реализована на базе рабочей станции, подключенной к шкафу управления преобразователя частоты и датчикам температуры через соответствующие устройства сопряжения. Рабочая станция AWS – 825 B/ 825PB соединяется с внешними устройствами с помощью преобразователей ADAM-4018 и ADAM-4021, выпускаемых фирмой Advantech (США). Блоки ADAM-4018 представляют собой модули аналогового ввода на 8 каналов для подключения термопар. Они содержат 16-разрядный АЦП, 6 дифференциальных и 2 однополюсных канала. Блоки ADAM-4021 предназначены для аналогового вывода и содержат 12-разрядный ЦАП, имеют программу настройки выхода на сигнал в виде напряжения (В) или тока (мА), контролируют состояние выхода, позволяют программировать скорость изменения сигнала на выходе от 0,125 до 128 А/с или от 0,0625 до 64 В/с.

СИТУАЦИОННЫЙ ЦЕНТР УПРАВЛЕНИЯ ЭНЕРГОЭФФЕКТИВНОСТЬЮ

А.Н. Корнилов, студент 2-го курса
Научный руководитель Н.В. Замятин, проф., д.т.н.
г. Томск, ТУСУР, ajlex@sibmail.com

Процесс роста эффективности и производительности труда выражается в развитии средств и методов его организации. Автоматизация – очередная ступень развития производительных сил – подразумевает сведение к минимуму непосредственного участия человека в процессах получения, преобразования, передачи и использования материалов, энергии, информации в пользу технических средств, математических методов и систем управления. Полностью исключить человека из производственного процесса возможно только для производств, весь цикл которых можно описать точно заданной последовательностью однозначно понимаемых операций.

Наиболее остро стоит проблема автоматизации сложных процессов, которые, как правило, не имеют адекватного математического описания, зашумлены и нестационарны, что делает применение традиционных подходов малоэффективным.

Важнейшей технологической основой эффективного управления сегодня является ситуационный центр. СЦ может быть представлен как организационно-технический комплекс, основу которого составляют информационное и программное обеспечение поддержки управленческих решений на основе комплексного мониторинга факторов влияния на развитие происходящих процессов.

Конечной целью создания СЦ является повышение эффективности и качества управленческих решений, предотвращение и устранение кризисных и чрезвычайных ситуаций. На его основе может быть обеспечена информационно-аналитическая поддержка процедур и процессов, позволяющих оперативно анализировать, моделировать, прогнозировать сценарии развития ситуации и динамично вырабатывать эффективные решения.

Целью данной работы является создание модели ситуационного центра для управления энергоэффективностью, в котором будет происходить сбор данных из некоторой базы, поступающих с измерительных приборов, и дальнейшее прогнозирование полученных данных на последующие периоды.

Прогнозирование будет осуществляться путем внедрения в программу нейросети Кохонена, которая принципиально отличается от всех других типов сетей. В то время как все остальные сети предназначены для задач с управляемым обучением, сеть Кохонена главным об-

разом рассчитана на неуправляемое обучение, т.е. обучающие данные содержат только значения входных переменных.

Связь базы данных с нейросетью Кохонена будет взаимодействовать посредством выполненного интерфейса.

ЛИТЕРАТУРА

1. Компания «ТБН энергосервис». http://www.tbnenergo.ru

2. *Банников Н.А.* http://www.stikriz.narod.ru/stikriz@nvrsk.ru, 2000.

3. *Дубровин В.И., Субботин С.А.* Оценка значимости признаков с фиксацией значений // Нейронные сети и модели в прикладных задачах науки и техники: Тр. междунар. конф. КЛИН–2002. Т. 3. Ульяновск: УлГТУ, 2002. С. 101–102.

4. Сеть Кохонена.
http://www.statsoft.ru/home/textbook/modules/stneunet.html

5. http://uvsr.stu.ru/foto/Ucheba/TechBD.htm

ОБЗОР ПРОГРАММНЫХ ПРОЦЕССОРОВ

П.Н.Коваленко, инженер каф. КИБЭВС, к.т.н.,
А.А.Шелупанов, проф., зав. каф. КИБЭВС, д.т.н.
г. Томск, ТУСУР, ФВС, kpn@keva.tusur.ru

Термин «soft-core процессор», или «микропроцессор с программным ядром», означает процессор, поведение которого представлено при помощи языка описания электронных схем (Verilog, VHDL) и реализуется синтезом на программируемой логической интегральной схеме (ПЛИС). Использование soft-core процессоров позволяет сократить время на разработку сложных систем, уменьшить конечную цену изделия и повысить эргономические показатели конечного устройства, что позволит ему быть конкурентоспособным на рынке.

Производители ПЛИС одними из первых начали свои разработки и исследования в области soft-core процессоров. Например, MicroBlaze и PicoBlaze были разработаны компанией Xilinx. С точки зрения архитектуры, MicroBlaze – это RISC процессор (Reduction Instruction Set Computing – архитектура процессора с сокращенным набором команд), который может выполнять по одной инструкции за такт, сохраняя такую производительность для большинства команд.

Если оптимизировать процессор по количеству занимаемых ресурсов ПЛИС, можно синтезировать ядро, работающее на тактовой частоте до 307 МГц (для семейства Virtex-6)[1]. Синтезированное ядро процессора занимает 1324 логических элемента (условная единица измерения вычислительного ресурса, которая состоит из 4-входового табличного элемента (LUT – Look Up Table) и триггера), что составляет менее 2% ресурсов ПЛИС XCE6VLX760 (таблица).

Сравнительные показатели программных процессоров

Название ядра	Разрядность, бит	Глубина конвейера, команд	Время выполнения инструкции, тактов	Количество занимаемых ресурсов, логических элементов	Лицензия
S1 (SPARCv9)	64	6	1	37000–60000	Открытый код (GPL)
Leon3 (SPARCv8)	32	7	1	3500	Открытый код (GPL)
OpenRISC1200 (RISC)	32	5	1	6000	Открытый код (LGPL)
LatticeMico32 (RISC)	32	6	1	1984	Открытый код (GPL)
Cortex-M1 (ARMv6)	32	3	1	2600	Собственность (ARM Limited)
MicroBlaze (RISC)	32	3,5	1	1324	Собственность (Xilinx)
Nios 2/f (RISC)	32	6	1	1800	Собственность (Altera)
Nios 2/s (RISC)	32	5	1	1170	Собственность (Altera)
Nios 2/e (RISC)	32	Нет	6	390	Собственность (Altera)
Xr16 (RISC)	16	3	1,4	260	Собственность (Gray Research LLC)
DSPuva16 (RISC)	16	Нет	4	510	Открытый код (GPL)
PicoBlaze ()	8	Нет	2	192	Собственность (Xilinx)

Soft-core RISC процессор PicoBlaze имеет 16-разрядную шину команд и 8-разрядную шину данных и адресов. Компактное ядро PicoBlaze специально оптимизировано для ПЛИС семейств Spartan-3, Spartan-6, Virtex-5, Virtex-6 и занимает 192 логических элемента, что составляет 0,08% всех ресурсов ПЛИС XCE6VLX760 [2]. Производитель ПЛИС, компания Altera, поддерживает и совершенствует программные ядра процессоров Nios, Nios2. Soft-core процессор Nios2 реализован по гарвардской архитектуре, имеет 32-битную шину адреса и данных. Оба ядра, Nios, Nios2, являются конвейерными RISC-процессорами, выполняют одну операцию за один такт. Nios2 может быть сконфигурирован в одном из 3 вариантов:

Nios2f (fast) – оптимизирован на максимальную производительность;

Nios2s (standard) – сконфигурирован как компромиссное решение между быстродействием и количеством занимаемых ресурсов. В этой конфигурации присутствует кэш инструкций, аппаратный умножитель и блок сдвиговых операций;

Nios2e (economy) – оптимизирован по количеству занимаемых ресурсов [3].

Ядро S1 реализовано по SPARCv9 архитектуре и поставляется в открытом коде с GNU(GPL) соглашением. UltraSPARC T1 имеет 8 ядер 64-битного процессора SPARCv9, разработанного для применения в ограниченных режимах энергопотребления. Ядро S1 – это ограниченная версия UltraSPARC T1, которое имеет только один процессор, который может поддерживать 4 независимых потока и одну шину Wishbone [4].

Leon3 является 32-битным ядром SPARCv8 с открытым исходным кодом. Это ядро использует 7-ступенчатый конвейер, выполняет одну инструкцию за такт и может применяться в системах средней и высокой сложности [5].

Ядро OpenRISC1200 разработано обществом OpenCores.org и является процессором, основанным на OpenRISC1000 архитектуре [6].

Ядро LatticeMico32 разработано компанией Lattice Semiconductor. Отличительной особенностью этого ядра является то, что оно не зависит от архитектуры логических элементов и может быть легко реализовано на ПЛИС различных производителей [7].

Cortex-M1 – это реализация закрытой 32-битной ARMv6 архитектуры. Чтобы использовать Cortex-M1 в своих разработках, необходима лицензия от компании ARM Limited. ПЛИС, выпускаемые компанией Actel, уже имеют соответствующую лицензию [8].

DSPuva16 – это ядро основано на RISC архитектуре и имеет специализированный сумматор-умножитель. Процессор имеет низкую разрядность программной памяти и не имеет памяти данных (кроме внутренних регистров). Процессор может использоваться для реализации простых алгоритмов, в которых присутствуют операции умножения [9].

Ядро xr16 представляет собой 16-битный RISC-процессор, работающий с целочисленными операциями. Ядро специально оптимизировано по количеству занимаемых ресурсов ПЛИС. Предоставляется как в коде, так и в виде схем [10].

В заключение необходимо отметить, что выбор ядра в первую очередь определяется спецификой решаемой задачи. Для решений на ПЛИС компаний Xilinx и Altera, реализация ядер MicroBlaze и Nios2

являются оптимальным с точки зрения производительности и используемых ресурсов, что подтверждается большим количеством приложений, которые выполняются на этих soft-core процессорах.

ЛИТЕРАТУРА

1. MicroBlaze Soft Processor Core. http://www.xilinx.com/tools/microblaze.htm
2. PicoBlaze 8-bitEmbedded Microcontroller. User Guide
3. Nios II Performance Benchmarks. DS-N28162004-6.0, Performance Benchmarks Overview, ALTERA
4. OpenSPARC T1. http://www.opensparc.net/opensparc-t1/index.html
5. Leon3 Processor. http://www.gaisler.com/cms/index.php
6. OR1200 OpenRISC processor. http://opencores.org/openrisc,or1200
7. LatticeMico32 Architecture. http://www.latticesemi.com
8. Cortex-M1 Processor. http://www.arm.com
9. Third-party open-source projects, DSPuva16, http://www.1-core.com/resources/
10. The xr16 CPU Core. http://www.fpgacpu.org/xsoc/xr16.html

ПРИЛОЖЕНИЕ ДЛЯ ВЗАИМОДЕЙСТВИЯ С ОБСЛУЖИВАЮЩИМ ПЕРСОНАЛОМ НА БАЗЕ WINDOWS MOBILE

А.Е. Леонов, студент 4-го курса, М.И. Мельников, аспирант
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, damned-13@sibmail.com

В настоящее время почти все сферы деятельности человека имеют сетевую структуру. Это влечет за собой тот факт, что множество объектов автоматизации оказываются распределенными по достаточно большой территории. С одной стороны, данная тенденция затрудняет обслуживание системы в целом, с другой – учитывая развитие средств коммуникации, позволяет контролировать отдельные узлы системы удаленно. На данный момент пока не удается полностью исключить участие человека в обслуживании такого рода систем, поэтому понятие «обслуживающий персонал» остается актуальным. Наиболее подходящим способом взаимодействия с обслуживающим персоналом является использование средств на базе беспроводных технологий. Одним из таких средств являются коммуникаторы, использующие в качестве операционной системы Windows Mobile. Данная платформа позволяет реализовать все необходимые функции для оперативного взаимодействия обслуживающего персонала с субъектом управления.

Основные функции приложения, обеспечивающие необходимый и достаточный обмен данными с субъектом управления:

− прием/Отправка SMS сообщений;

− прием/Отправка сообщение через Интернет посредством протокола XMPP;

− определение текущего местоположения при помощи GPS-приемника;

− отправка координат на сервер.

Данное приложение состоит из пяти основных модулей: модуля интерфейса, модуля обработки, модулей jabber и SMS и модуля GPS. Взаимосвязь модулей друг с другом и окружающей средой отражает функциональная схема, представленная на рис. 1.

Рис. 1. Функциональная схема приложения

Модуль интерфейса содержит формы главного меню, настроек, вызовов и форму для работы с GPS-данными.

Форма главного меню содержит кнопки, с помощью которых пользователь может перейти на необходимую ему форму.

При получении приложением сообщения пользователь получает уведомление о новом входящем сообщении. При подтверждении пользователем принятия сообщения открывается форма «Вызовы», содержащая текстовое окно, в котором отображается принятое сообщение. Под текстовым окном расположены кнопки для быстрого ответа. При нажатии кнопки «Принять» на сервер будет отправлено сообщение о том, что пользователь принял запрос на выполнение ремонтных работ. Соответственно, при нажатии кнопки «Отказаться» на сервер будет отправлено сообщение о том, что пользователь отказывается от данного запроса.

Форма настроек должна содержать необходимые поля и кнопки для настройки параметров сервера (IP-адрес, номер телефона GSM-модема и jabber-ID).

Форма для работы с GPS-данными должна содержать поля отображения координат и кнопку для начала и остановки отправки данных на сервер. Таким образом, удобный и простой интерфейс позволяет быстро отреагировать на поставленные перед персоналом задачи.

Модуль обработки предназначен для организации приема и отправки сообщений от сервера и обработки входящих и исходящих сообщений. Содержит методы для обработки протокола XMPP и SMS сообщений и метод обработки данных со встроенного GPS-приемника.

Модули jabber и SMS организуют представление входящих сообщений в формат, приемлемый для чтения пользователем, и организует отправку ответов на поступающие запросы.

Модуль GPS предназначен для отображения координат местоположения пользователя и отправки текущего положения на сервер. Эти данные будут использованы для определения ближайшей к месту аварии бригады.

Данное приложение позволяет обеспечивать взаимодействие обслуживающего персонала с автоматизированным центром управления распределенными объектами автоматизации в режиме реального времени, способствует упрощению координации действий обслуживающего персонала и оперативному получению запросов на выполнение каких-либо работ.

ЛИТЕРАТУРА

1. *Мельников М.И.* Разработка автоматизированной системы управления распределённым лифтовым хозяйством на базе беспроводных технологий // Доклады ТУСУРа. Ч. 2. Томск: Изд-во ТУСУРа, 2009. №1 (19). С. 81–82.

2. *Фридл Дж.* Регулярные выражения. Серия «Библиотека программиста». СПб.: 2-е изд. Питер, 2003. 464 с.

3. *Климов А.П.* Программирование КПК и смартфонов на .NET Compact Framework. СПб.: Питер, 2007. 320 с.

МОНИТОРИНГ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ СТЕКА ПРОТОКОЛОВ TCP/IP

И.М. Макаров, студент 3-го курса

г. Томск, ТУСУР, каф. КИБЭВС, videi@mail.ru

Научный руководитель С.Ю. Исхаков, аспирант каф. КИБЭВС

Каких бы масштабов ни была компьютерная сеть, она нуждается в управлении и наблюдении. Система мониторинга направлена на обеспечение постоянного наблюдения за состоянием узлов компьютерной сети: выполнять проверку доступности сетевых ресурсов, служб, следить за работой серверного и коммуникационного оборудования; в случае нарушения стандартной работы уведомлять администратора, используя различные средства оповещения.

Выбор способов и объектов мониторинга сети зависит от множества факторов – конфигурации сети, действующих в ней сервисов и служб, конфигурации серверов и установленного на них ПО, возможностей ПО, используемого для мониторинга, и т.п. На общем уровне можно говорить о таких элементах, как:

– проверка физической доступности оборудования;

– проверка состояния (работоспособности) служб и сервисов, запущенных в сети;

– проверка таких параметров функционирования сети, как производительность, загрузка канала и т.д.;

– проверка параметров, специфичных для сервисов и служб данного конкретного окружения (наличие некоторых значений в таблицах БД, содержимое лог-файлов).

В рамках разрабатываемого проекта системы управления сетью «SOWA» [1] реализовано тестирование физической доступности оборудования (которая может быть нарушена в результате отключения самого оборудования либо отказа каналов связи). Это означает проверку доступности по ICMP-протоколу (ping), необходимо проверять не только факт наличия ответа, но и время прохождения сигнала, и количество потерянных запросов – аномальные значения этих величин сигнализируют о серьезных проблемах в конфигурации сети [2]. Некоторые из этих проблем можно отследить при помощи трассировки маршрута (traceroute) – сетевую утилиту также можно автоматизировать при наличии «эталонных маршрутов». Также осуществляется получение данных о работе службы DNS с помощью сетевых утилит nslookup, dig, host, whois.

Для тестирования физической доступности сети было разработано Web-приложение [3], которое содержит в себе необходимые сетевые утилиты и параметры, задаваемые пользователем для получения информации о данном соединение или DNS-сервере.

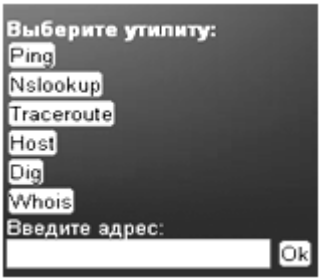


Рис. 1. Web-приложение с сетевыми утилитами

Результатом работы является приложение, позволяющее использовать сетевые утилиты без привязки к определенной ОС. Основным достоинством является возможность запуска данного web-приложения с любого вида коммуникационного устройства.

Проект реализовывался для мониторинга сети СибГМУ [1], которая использует стек протоколов TCP/IP [2].

Для мониторинга данной компьютерной сети были задействованы следующие утилиты:

– ping – утилита для проверки соединений в сетях на основе TCP/IP [2];

– nslookup – позволяет задавать различные типы запросов и запрашивать произвольно указываемые серверы. Её аналогом являются утилиты host [2] и dig [2];

– traceroute – отображает адреса всех маршрутизаторов на пути от клиента до удаленного хоста [4];

– host – утилита, предназначенная для обращения и получения информации DNS-серверов [4];

– dig – утилита, предназначенная для поиска информации в DNS [3];

– whois – основное применение – получение регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем [2].

Данные сетевые утилиты предоставляют администратору информацию для анализа компьютерной сети, использующий стек протоколов TCP/IP.

Выполнено в рамках проекта ГПО КИБЭВС-1002 – «Построение автоматизированной системы администрирования локально-вычислительных сетей».

ЛИТЕРАТУРА

1. *Исхаков С.Ю.* Анализ структуры сети учреждения здравоохранения // Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2010», Томск, 4–7 мая 2010 г. Томск: В-Спектр, 2010. Ч. 3. С. 40–42.

2. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. 3-е изд. СПб., 2005. С. 564–701.

3. *Шлосснейгл Д.К.* Профессиональное программирование на PHP. СПб., 2006. С. 1–50.

4. *Курячий Г.В., Маслинский К.А.* Операционная система Linux. М.: Интуит.Ру, 2005. С. 150–300.

РАЗРАБОТКА ГЕОИНФОРМАЦИОННОЙ СИСТЕМЫ С ПОИСКОМ ПО СЕКТОРАМ И ЗОНАМИ ОТВЕТСТВЕННОСТИ

М.О. Мельникова, студентка, М.И. Мельников, аспирант
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, amira32@rambler.ru

В современном обществе человек уже не может обойтись без привычных устройств. Они окружают нас постоянно, на улице, дома, на

работе. Многие уже не могут представить свою жизнь без мобильного телефона, компьютера. Все эти удобные в нашей жизни устройства продолжают развиваться, становясь более компактными и функциональными. Не стоят на месте и программы, обеспечивающие контроль за местоположением объектов.

Стараясь обеспечить контроль за перевозками, перелетами, передвижением объектов, нуждающихся в безопасности или представляющих ценные грузы, разрабатываются системы для слежения. Обязательным элементов каждой системы будет GPS-навигация. Изначально разрабатываемая для военных нужд, сейчас она незаменимо используется для определения положения объектов в гражданских целях [1].

GPS-навигация представляет собой 30 спутников, которые вращаются вокруг Земли. Так как спутники находятся постоянно в движении, определение координат происходит при получении сигналов нескольких спутников на GPS-приемник [2].

Получая данные со спутников, можно определить место положения объектов находящихся в движении, и отследить их перемещение. Такая функция слежения необходима для организаций, осуществляющих перевозки или транспортировку каких-либо грузов или объектов. Разрабатываемая геоинформационная система позволит не только отслеживать перемещение, но и отправлять на помощь свободных специалистов. Программа отображения местоположения объектов мобильных групп работает с базой данных, где хранятся координаты передвижения мобильных групп. Данные поступают в базу данных с мобильных устройств и датчиков. Полученные данные отображаются на карте в режиме реального времени. Главной отличительной функцией системы будет поиск свободных мобильных групп в радиусе секторов с зонами ответственности.

Независимо от места, где необходимы специалисты при подаче сигнала, программа отображает на карте сигнал о помощи, указывает специалистов в районе этой аварии и отправляет свободную бригаду специалистов на место. Наличие эффективного алгоритма разграничения секторов работы является ключевым моментом при автоматическом построении карт с участками работы для мобильного персонала [3].

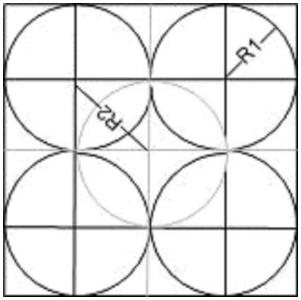


Рис. 1. Построение координатной сетки с радиусами поиска

При конструировании алгоритмов и программ для построения осей приходится учитывать разнообразные требования в различных сочетаниях и вариантах. Первоначально происходит определение ближайших секторов. При обнаружении отправляются данные в базу данных, где проходит обнаружение свободных секторов. Так как используется сетка со смещение необходимо 2 радиуса.

Используемые формулы (1) для описания радиусов:

$$R_1 - 2a, \quad R_2 = \sqrt{2a^2}\ . \qquad (1)$$

Построение координатной сетки необходимо производить на загруженной карте города, области, страны. При построении необходимо задать шаг ячейки с площадью охвата работы бригад.

Нумерация секций происходит автоматически, при желании можно самостоятельно поменять номера секторов. Поиск соседних секторов осуществляется по двум радиусам, при этом название не влияет на поиск. Чтобы определить соседние сектора, используются центры квадратов. Таким образом, поиск всегда идет по заданным радиусам окружности в квадрате и окружности, проходящей через центры квадратов, имеющие общие зоны ответственности. Такой метод универсален на любой сетке с наложением второй координатной сетки со смещением вполовину.

На рис. 2 отображены основные положения сетки. Так сектор 5 является резервным, сектора 1, 2, 3, 4 основные.

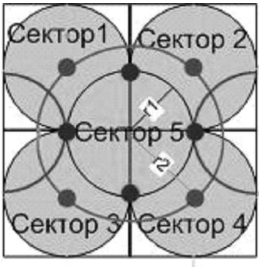


Рис. 2. Работа поиска в секторах

В случаях, когда на разбиваемой карте имеются участки не нуждающиеся в контроле (лес, парк), поиск не отображает эти участки.

Таким образом, разрабатываемая геоинформационная система поиска по секторам с зонами ответственности позволяет решать проблемы с поиском свободных групп в радиусе, максимально приближенном к месту аварии. Не требует диспетчера для отправки информации мобильному персоналу. Уменьшает время реагирования с момента подачи сигнала о помощи до ее оказания.

ЛИТЕРАТУРА

1. GPS-навигация [Электронный ресурс]. Сайт программного обеспечения GPS. URL: http://gps.ru/about/ (дата обращения: 1.03.2011).

2. GPS навигация и навигационные системы Garmin, навигаторы и GPS приёмники [Электронный ресурс]. Сайт компании Garmin. URL: http://www.garmin.ru/ (дата обращения: 2.03.2011).
3. Статистическое исследование алгоритма [Электронный ресурс]. Сайт компании Garmin. URL: http://www.math.spbu.ru/user/gran/sb3/sushkov_kusher.pdf (дата обращения: 2.03.2011).

ФИЛЬТРАЦИЯ ШУМА В ЦИФРОВОМ ИЗОБРАЖЕНИИ НА ОСНОВЕ КЛЕТОЧНОГО АВТОМАТА

С.В. Моисеенко, Е.О. Оплачко, студенты 4-го курса
Научный руководитель О.О. Евсютин, аспирант
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, ekatopla@rambler.ru

Обработка изображений как направление компьютерной графики отвечает за преобразование (фильтрацию) изображений. Примерами могут служить повышение контраста, резкости, коррекция цветов, сглаживание. Задачей обработки изображения может быть как улучшение (восстановление, реставрация) изображения по какому-то определенному критерию, так и специальное преобразование, кардинально меняющее изображение. В последнем случае обработка изображений может быть промежуточным этапом для дальнейшего анализа изображения (например, для выделения контура объекта).

Если изображение или видеопоследовательность были получены с помощью оцифровки, на них, как правило, присутствует шум. Проблема шумоподавления является одной из самых актуальных и распространенных проблем в области обработки как статичных изображений, так и видео [1].

В любой системе мультимедиа, начиная со спутников и заканчивая сотовыми телефонами, используется передача изображений. При передаче, оцифровке или сжатии качество изображения может ухудшиться, что может проявляться в возникновении шума в графическом изображении. Чаще всего шумоподавление служит для улучшения визуального восприятия, но может также использоваться для каких-то специализированных целей – например, в медицине для увеличения четкости изображения на рентгеновских снимках, в качестве предобработки для последующего распознавания и т.п.

Также шумоподавление играет важную роль при сжатии изображений. В изображениях сжатие основано на пространственной корреляции значений пикселей. При сжатии сильный шум может быть принят за детали изображения, и это может, во-первых, привести к увели-

чению сложности с точки зрения сжатия и, во-вторых, отрицательно повлиять на результирующее качество сжатого изображения [2].

Источники шума могут быть различными: неидеальное оборудование для захвата изображения (видеокамера, сканер), плохие условия съемки, помехи при передаче по аналоговым каналам и т.п. Алгоритмы шумоподавления обычно специализируются на подавлении какого-то конкретного вида шума. Не существует пока универсальных фильтров, обнаруживающих и подавляющих все виды шумов [3].

Рассмотрим вид шума, с которым проводилась работа. Шум типа «salt-and-pepper» [4, 5] похож на просыпанные на бумагу соль и перец. С некоторой вероятностью пиксели заменяются максимальными или минимальными значениями. Для классического представления пикселя 8 битами это значения 0 и 255, что выглядит как черные и белые точки на изображении. Одним из примеров появления подобного шума является передача изображения по зашумленным цифровым сетям. Устранить подобный шум можно с помощью медианного фильтра или статистических фильтров.

Существует достаточно большое количество методов подавления шума, выделим некоторые из них:

- линейное усреднение пикселей;
- медианная фильтрация;
- математическая морфология;
- гауссовское размытие;
- методы на основе вейвлет-преобразования;
- метод главных компонент;
- анизотропная диффузия;
- фильтры Винера.

Рассмотрим методы, с которыми проводилось сравнение разработанного метода на основе клеточного автомата, более подробно.

Линейное усреднение пикселей изображения производит анализ некоторой окрестности пикселя и заменяет его средним арифметическим соседей, значения которых отличаются от центрального пикселя на некоторое пороговое значение.

Медианная фильтрация для каждого пикселя в некоторой окрестности определяет медианное значение и присваивает этому пикселю. Данный фильтр размывает мелкие детали, величина которых меньше размера выбранной окрестности пикселя.

Гауссовское размытие представляет собой все то же усреднение, только пиксель смешивается с окружающими по определенному закону, заданному функцией Гаусса [6].

В ходе работы проводилась генерация шума «salt-and-pepper», для чего было создано отдельное приложение. Фильтр КА представляет

собой фильтр на основе клеточного автомата, который позволяет при известном расположении шумящих пикселей удалить шум. Для определения положения пикселей шума был разработан анализатор шума, который на вход фильтра подает данные о расположении шума в обрабатываемом изображении. Во многом качество фильтра зависит именно от точности результатов работы анализатора шума.

На вход фильтра для удаления шума отправляется полученное от отправителя изображение и массив шумящих пикселей, и фильтр, в свою очередь, проводит восстановление изображения. Задача фильтра сводится к замене значений пикселей, идентифицированных как шум, на некоторый случайный пиксель, принадлежащий окрестности.

Добавим к исходному изображению, приведенному на рис. 1, шум типа «salt-and-pepper». Для иллюстрации работы разработанного фильтра также применим некоторые другие фильтры, используемые для шумоподавления.

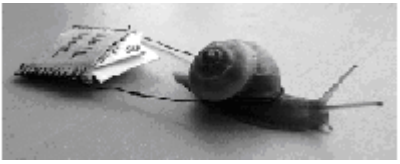


Рис. 1. Исходное изображение

На рис. 2 приведены зашумленное на 55% изображение, изображение, полученное при применении медианного фильтра, и результат выполнения фильтрации на клеточном автомате.

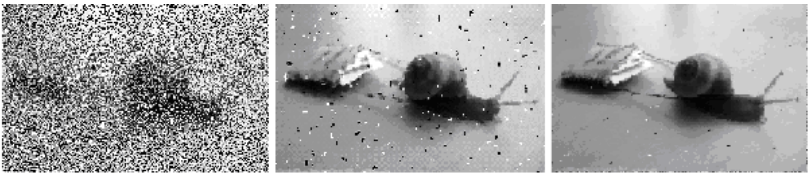


Рис. 2. Сравнение результатов фильтрации изображения, зашумленного на 55%

Аналогичные результаты для зашумленного на 90% исходного изображения приведены на рис. 3.

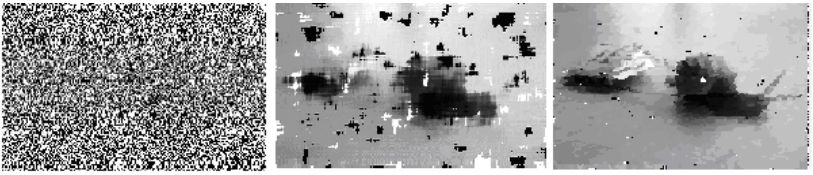


Рис. 3. Сравнение результатов фильтрации изображения, зашумленного на 90%

Как можно видеть, разработанный фильтр дает хороший результат для этого вида шума. Восстановленное изображение содержит некоторые артефакты, но уровень четкости достаточно высок по сравнению с медианным фильтром.

Выполнено в рамках проекта ГПО КИБЭВС-0904 – «Криптосистемы клеточных автоматов».

ЛИТЕРАТУРА

1. *Bovik A.C.* Handbook of Image and Video Processing. Academic Press, 2005.

2. *Калинкина Д., Ватолин Д.* Проблема подавления шума на изображениях и видео и различные подходы к ее решению // Компьютерная графика и мультимедиа. 2005. №3(2).

3. *Гонсалес Р.* Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1072 с.

4. *Burdick H.E.* Mc Graw-Hill Digital Imaging: Theory and Applications. 1997.

5. Wolfram MathWorld: The Web's Most Extensive Mathematics Resource [Электронный ресурс]. – Режим доступа: http://mathworld.wolfram.com

6. *Rosenthaler L.* Digital Image Processing / Introduction, Digital representation of images, Histogram, Arithmetical operations, Geometrical transformations, Neighborhood operations.

7. *Xavier F., Leal-Toledo R.C., Conci A.* Image Noise Reduction Based on Cellular Automata Filter, 2005.

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС ПО МОНИТОРИНГУ И УПРАВЛЕНИЮ ТЕПЛОСНАБЖЕНИЕМ ЗДАНИЙ И ПОМЕЩЕНИЙ

Н.И. Муслимова, И.А. Заречная, студентки, каф. ТОР,
Д.Н. Ушарова, техник 1-й категории, Д.Ю. Майков, студент РТС
г. Томск, ТУСУР, n.i.m.@sibmail.com

Одной из наиболее актуальных проблем в области систем жизнеобеспечения зданий является энергосбережение. Мониторинг задач этой проблемы показывает, что наиболее важным звеном в ее решении является рациональное использование тепловой энергии, особенно на участках «конечных пользователей».

Основной научно-технической задачей данного проекта является разработка аппаратно-программного комплекса (АПК) и технологии учета расхода тепловой энергии, потребляемой как зданием в целом, так и его отдельными помещениями с учетом индивидуальных особенностей помещений, отопительных приборов и реальных климатических условий. Решение этой задачи позволит значительно экономить тепловую энергию.

Одним из основных достоинств АПК по сравнению с существующими аналогами является динамический характер функционирования измерительной системы. При этом создаются условия, когда измеряемые температуры являются функциями времени и включают в себя реакцию на изменение параметров источников тепла, температуры и ветровой нагрузки внешней среды и др. Кроме того учет индивидуальных особенностей каждого помещения, простота конструкции, автоматизация процессов, низкая стоимость. Это обеспечивается применением оригинальной математической модели с использованием дифференциальных балансных уравнений [1].

Так как в реальной ситуации температура смежных помещений может не совпадать с температурой нашего помещения, а температуры теплоносителя и внешней среды зависят от времени, математическая модель была доработана (1). Было введено третье уравнение для системы отопительных приборов и во второе уравнение системы добавлен член, учитывающий излучение тепла в соседние помещения:

$$\begin{cases} dQ_1/dt = R_{\text{ист}} \cdot (T_{\text{ист}} - T_1) - R_{\text{к}} \cdot (T_1 - T_2) - R_{\text{внеш}} \cdot (T_1 - T_{\text{внеш}}); \\ dQ_2/dt = R_{\text{к}} \cdot (T_1 - T_2) - R_{\text{см}} \cdot (T_2 - T_{\text{см}}); \\ dQ_3/dt = C_{\text{вод}} \cdot v \cdot (T_0 - T_{\delta}) - R_{\text{ист}} \cdot ((T_0 + T_{\delta})/2 - T_1), \end{cases} \quad (1)$$

где $R_{\text{ист}}$ – коэффициент теплопередачи теплоносителя [кВт/К]; $R_{\text{внеш}}$ – коэффициент теплопередачи внешнего ограждения, учитывающий явления теплопроводности, конвекции и теплового излучения [кВт/К]; $R_{\text{к}}$ – коэффициент теплопередачи внутреннего ограждения [кВт/К]; $R_{\text{см}}$ – сопротивление излучения в соседнее помещение [кВт/К]; $C_{\text{вод}}$ – теплоемкость воды [кДж/(м^3·К)]; $T_{\text{ист}}$ – температура системы отопительных приборов [К]; T_1 – температура воздуха в помещении [К]; T_2 – температура ограждения [К]; $T_{\text{внеш}}$ – температура внешней среды [К]; $T_{\text{см}}$ – температура воздуха смежного помещения [К]; v – скорость теплового потока [м/с].

В процессе работы проведены эксперименты для получения температурной зависимости помещения и нахождения параметров ограждения, проведены моделирование и анализ тепловых режимов помещения в пакете MatLab и с использованием разработанного программного обеспечения.

Суть эксперимента заключалась в следующем: температурные датчики размещались на стенах и перекрытиях в нескольких местах с тем, чтобы можно было потом получить усредненный интегральный коэффициент, связанный с теплоемкостью ограждений. Одновременно датчики размещались в воздухе, на теплоносителе и во внешней среде. Температурные данные снимались через интервал в одну минуту.

Воздух и стены помещения охлаждались за счет притока холодного воздуха из внешней среды. Затем система помещения приводилась в естественное состояние, и происходило нагревание объема воздуха и стен за счет притока тепла от отопительных источников. Этот процесс нагревания фиксировался с помощью только что описанной системы температурных датчиков.

Полученные экспериментальные кривые были использованы для нахождения недостающих параметров: $R_{ист} = 25{,}37$ Вт/К; $R_{внеш} = 7{,}75$ Вт/К; $R_к = 352{,}95$ Вт/К.

В результате работы были найдены основные характеристики тепловых режимов помещения и рассчитана экономия тепловой энергии при регулировании температуры внутри помещения в течение суток, были созданы: алгоритм, структурная схема и протокол функционирования автоматизированной системы сбора, хранения, обработки информации и управления инженерными сетями зданий и сооружений; программная модель системы теплоснабжения на базе балансных дифференциальных уравнений; комплекс технических средств системы (рис. 1) [2].

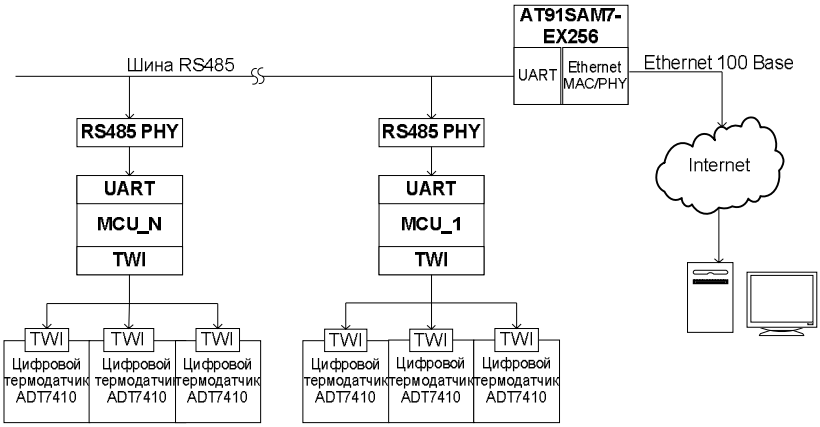


Рис. 1. Структурная схема аппаратной части комплекса

Микроконтроллеры MCU_1–MCU_N опрашивают цифровые датчики температуры ADT7410, подключенные по линии TWI (two wire interface, I2C). Значения температуры передаются по линии RS485 на шлюз, который управляется микроконтроллером AT91SAM7-EX256, как по запросу, так и по таймеру. Данные хранятся на шлюзе и по запросу передаются на ПК.

Основные принципы работы комплекса: 1) измерение температур в помещении; 2) вычисление параметров теплового ограждения; 3) вычисление тепловой энергии, отдаваемой источником.

Аппаратно-программный комплекс позволяет сократить на 15–20% потребление тепловой энергии жилыми домами, сократить на 20–30% потребление тепловой энергии помещений организаций и учреждений.

Значимость результатов работы определяется возможностью внедрения АПК в зданиях, помещениях производственных комплексов и систем ЖКХ с целью экономии тепловой энергии.

ЛИТЕРАТУРА

1. *Пуговкин А.В.* Математическая модель теплоснабжения помещений для АСУ энергосбережения / А.В. Пуговкин, С.В. Купреков, Д.В. Абушкин, И.А. Заречная, Н.И. Муслимова // Доклады Том. гос. ун-та систем управления и радиоэлектроники. 2010. №2 (22). Ч. 1.

2. *Пуговкин А.В., Купреков С.В., Ушарова Д.Н., Майков Д.Ю.* Программно-аппаратный комплекс для АСУ энергосбережения // 4-я Всерос. науч.-техн. интернет-конф. «Энергетика. Инновационные направления в энергетике. CALS-технологии в энергетике». 1–31 октября 2010 г. М., 2010.

ЗАДАЧИ УПРАВЛЕНИЯ И АВТОМАТИЗАЦИИ ПРИ РАСПРЕДЕЛЕНИИ РЕСУРСОВ НА ПРОМЫШЛЕННЫХ ОБЪЕКТАХ ПРИ ВОЗНИКНОВЕНИИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

И.С. Наумов, аспирант

Научный руководитель А.М. Пушкарёв, проф. Пермского военного института ВВ МВД России, к.т.н.

г. Пермь, Пермский государственный технический университет, igor14-88@list.ru

Возникновение чрезвычайных ситуаций (ЧС) – событие, сложно предсказуемое, требующее оперативного реагирования. Для устойчивого развития любого предприятия и страны в целом необходимо принятие мер по сокращению ущерба, причиняемого ЧС, и количества ресурсов, используемых при их предупреждении и ликвидации. Однако опасные природные и техногенные явления как источник ЧС могут прогнозироваться лишь на очень малых с точки зрения проведения превентивных мероприятий временных интервалах.

Необходимо совершенствование систем управления, ориентированных на локализацию и ликвидацию ЧС. Основными критериями формирования оптимального плана по предупреждению и ликвидации

последствий ЧС являются минимум ущерба; минимум общих затрат на реализацию превентивных мероприятий; минимум общего времени реализации оперативных мероприятий по ликвидации ЧС и ее последствий.

Вследствие этого создана модель совершенствования и функционирования системы обеспечения ресурсами, на основании которой разработана методическая схема решения задачи, предполагающей автоматизацию процесса управления ресурсами:

− обоснование рационального объема бюджетного финансирования, типов и количества ресурсов, размещаемых в системе обеспечения ресурсами;

− обоснование иерархии структуры систем обеспечения ресурсами и соответствующего расположения центрального пункта с учетом инфраструктуры района функционирования;

− обоснование порядка определения потенциальной опасности объектов для противодействия возможным ЧС, на которых создается система;

− обоснование размещения ресурсов по элементам системы;

− обоснование эффективной стратегии функционирования системы.

На первом этапе использования методической схемы необходимо провести предварительную оценку общих затрат на систему обеспечения ресурсами. Это обеспечивает исходную информационную основу для последующей оптимизации параметров системы. Для этого оценивается возможный ущерб от ЧС при отсутствии обеспечения ресурсами процесса ее ликвидации. Выражение этого ущерба сопоставляется с объективными потребностями в ресурсах на предотвращение ожидаемого ущерба. Полученное выражение потребности в ресурсах приводится к форме затрат на их приобретение. Решение этой задачи базируется на известных моделях развития ЧС, применяемых в отношении конкретных промышленных объектов, данные о которых могут определяться по паспортам этих объектов. Кроме того, используются известные сведения о затратах на приобретение и ввод в эксплуатацию всех доступных видов ресурсов, а также об их производительности. Эти сведения могут быть конкретизированы для объектов, так как производительность и стоимость размещения ресурсов на различных объектах могут различаться. Полученные результаты ложатся в основу для выработки решений о финансировании создания или совершенствования системы ликвидации ЧС и позволяют выработать предварительное заключение о степени совершенства существующей системы.

Для завершения первого этапа методической схемы необходимо определить типы ресурсов и их количество на объектах.

Для реализации второго этапа методической схемы требуется обоснование структуры системы обеспечения ресурсами с учетом предлагаемого нового подхода. В сложившейся практике доминирует развитие систем обеспечения ресурсами как двухэшелонных систем, то есть основное совершенствование системы состоит в развитии централизованного ресурса, например региональной базы МЧС. Для такой структуры необходимо определить центральный пункт размещения ресурсов с учетом сложившейся инфраструктуры района функционирования системы. Для этого с позиции реализации принципа гарантированного результата целесообразно использовать минимаксный критерий удаленности центра от потенциально опасных объектов, так как продолжительность доставки ресурсов влияет на величину возможного ущерба. Задача решается полным перебором. Если в качестве центра размещения ресурсов выбирается один из объектов, то в прикладном отношении решение задачи сводится к записи в таблицу всех длин маршрутов между объектами, определению для каждого объекта максимального маршрута до других объектов и выбору объекта, для которого максимальный маршрут минимален.

Третий этап реализации предложенной методической схемы предполагает обоснование порядка определения потенциальной опасности объектов для ликвидации ЧС, на которых создается система обеспечения ресурсами. Если на некоторых объектах возможна ЧС в течение времени ликвидации ЧС на одном из объектов, то с этих объектов нельзя направлять ресурсы на объект, где возникла ЧС. Кроме того, на центральной базе необходимо оставить ресурсы для ликвидации возможных ЧС на этих объектах. Поэтому необходимо определить максимальное количество объектов, на которых с вероятностью не меньше заданной, возможно возникновение ЧС в течение $\tau_{\max}$.

Четвертый этап предполагает обоснование распределения ресурсов между центральной базой и объектами, обеспечивающего минимум максимального ущерба от ЧС. Для минимизации возможного ущерба объектам выделяются ресурсы как с центральной базы, так и с объектов, на которых нет ЧС. В случае возникновения ЧС на *i*-м объекте, которая может привести к ущербу на этом объекте величиной $U_i^{\max}$, ресурсы, размещенные на нем, немедленно используются для ее ликвидации и предотвращают ущерб на величину U_i^0.

Задача решается последовательно для всех ситуаций. При этом алгоритм решения задачи состоит в следующем:

1. Вычисляются оптимальные величины $x_{ij}, x_{kj}, x_{\text{Ц}j}, U_i^{\Sigma}$ решением целочисленной задачи линейного программирования.

2. Эта процедура повторяется для всех возможных ситуаций.

3. Строится матрица $\left\| U_i^{\Sigma} \right\|$.

4. Распределяются ресурсы по варианту, для которого $\left\| U_i^{\Sigma} \right\|$ максимально.

Тем самым согласно общей методической схеме завершается предварительный процесс синтеза системы и осуществляется переход к решению задач, связанных с количественным анализом результатов ее функционирования.

ЛИТЕРАТУРА

1. *Кюнтрейтер Г.* Проблемы принятия решений в условиях риска. М.: Наука, 1982.

ТЕХНОЛОГИЧЕСКИЙ МОДУЛЬ ИЗГОТОВЛЕНИЯ ПЕЧАТНЫХ ПЛАТ

И.В. Неволин, студент 5-го курса

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, kain-still@yandex.ru

Целью данной работы является разработка технологического модуля изготовления печатных плат. Модуль предназначен для автоматизированного выполнения технологических работ по формированию проводных соединений на платах с одно-двухсторонней металлизацией в условиях неспециализированных помещений.

В разрабатываемом модуле реализован субтрактивный метод [1] получения проводящего рисунка печатных плат (ПП). Субтрактивный метод заключается в избирательном удалении участков фольги с пробельных мест (места, не закрытые защитной маской) фольгированного материала и включает в себя следующие этапы [1]:

1) подготовка поверхности заготовки печатной платы;
2) нанесение защитной маски;
3) химическое травление открытых участков фольги.

В разрабатываемом модуле реализован химический способ подготовки поверхности заготовки печатной платы. Нанесение защитной маски осуществляется термотрансферным способом [2], сущность которого заключается в переносе защитного рисунка с промежуточного носителя на заготовку печатной платы при помощи нагрева контактирующих между собой поверхностей промежуточного носителя и заготовки печатной платы. Химическое травление печатной платы осуществляется в растворе хлорного железа.

Перечисленные операции изготовления печатных плат, подразделяются по своему роду на химические и термические операции. Целесообразно объединить выполнение этих операций в блоки:

- блок термотрансфера защитного рисунка;
- блок химических операций;
- блок сушки.

Для автоматизированного управления транспортными и контрольными операциями по процессу изготовления печатных плат предназначен блок управления.

Блоки модуля изготовления печатных плат выполнены в виде отдельных конструктивных частей, что способствует более удобному расположению модуля на рабочем месте. Связь датчиков и исполнительных органов блоков химических операций, трансфера и блока сушки с блоком управления осуществляется при помощи соединительных кабелей и разъемных соединений.

Состав блока химических операций:

1) емкости для химических растворов (раствор хлорного железа, промывочная вода, очиститель);

2) защитная кювета для предотвращения попадания химических растворов на транспортные механизмы технологического модуля;

3) транспортный узел, обеспечивающий перемещение заготовки печатной платы (ПП) между емкостями для химических растворов;

4) узел перемешивания раствора хлорного железа подачей в ёмкости с жидкостями потока воздуха от компрессора;

5) узел поддержания температуры растворов подогревом.

В блоке химических операций контролируются концентрация и температура раствора хлорного железа, время очистки и травления платы. В транспортных операциях блока контролируется положение заготовки платы относительно емкостей химических растворов.

Состав оборудования блока термотрансфера защитного рисунка:

1) основание;
2) электронагреватель;
3) транспортный узел термоплиты с нагревателем.

В блоке термотрансфера контролируются температура нагрева поверхностей и время операции переноса изображения с промежуточного носителя на поверхность заготовки ПП.

Сушка платы осуществляется обдувом потоком воздуха комнатной температуры без подогрева. Вентилятор и фиксатор платы при сушке выполнены в виде отдельного конструктивного модуля, включение вентилятора в котором осуществляется на заданное время от общего блока управления технологического модуля.

Электронный блок управления технологическим модулем предназначен выполнять следующие задачи:

1) контролировать состояние датчиков в блоках состава;
2) управлять двигателями транспортных механизмов блоков;
3) контролировать и подтверждать состояния переключателей и кнопок пульта оператора.

Названные задачи в работе решаются построением устройства управления на однокристальном микроконтроллере, с включением в состав устройства усилителей и коммутаторов управления двигателями транспорта, вентиляции, нагревателями. Связь блока управления с блоками химических операций, термотрансфера, блоком сушки платы обеспечивается через разъёмные электрические соединения. Питание оборудования модуля осуществляется от сети переменного тока через встроенный источник блока электропитания.

Вид лицевой панели блока управления показан на рис. 1.

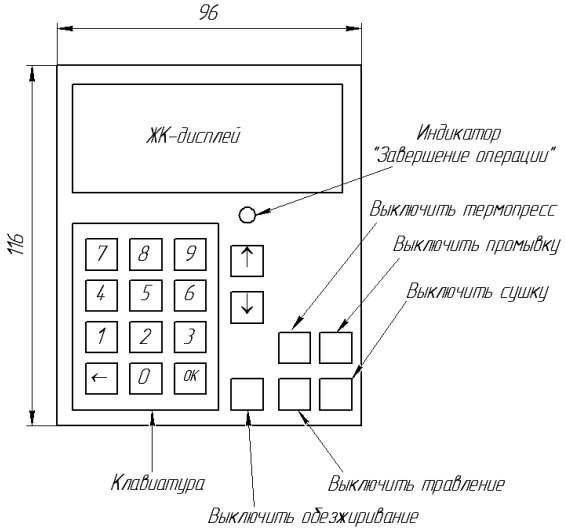


Рис. 1. Лицевая панель блока управления

В ходе работы выполнены расчётные оценки параметров технологического оборудования, для выбора комплектующих средств. Проработаны эскизы кинематических схем механики технологического модуля, подобраны материалы по датчикам и исполнительным органам, проведены эскизные проработки приёмов программного контроля температуры, управления матричной панелью визуального отображения информации, управления транспортными двигателями.

ЛИТЕРАТУРА

1. *Медведев А.М.* Печатные платы. Конструкции и материалы. М.: Техносфера, 2005.

2. Технология производства – термотрансфер [Электронный ресурс]. Режим доступа: http://renessans2000.ru/index.phppage=tech_termotransfer, свободный.

ТЕСТИРОВАНИЕ АЛГОРИТМОВ СЕГМЕНТАЦИИ РЕЧЕВОГО СИГНАЛА НА ВОКАЛИЗОВАННЫЕ И НЕВОКАЛИЗОВАННЫЕ УЧАСТКИ

В.А. Осипов, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, vitalisosipov_@mail.ru

Под термином «сегментация» всегда понимается операция целесообразного разбиения речи на фрагменты. Целесообразность того или иного типа сегментации определяется: конкретной задачей обработки речи; моделью, выбранной для решения этой задачи; требованиями к точности и времени работы системы, реализующей модель [1].

В системах автоматического распознавания речи важной задачей является сегментация речи в соответствии с фонетической транскрипцией языка. Ручная сегментация требует значительных затрат сил и времени. Кроме того, практически невозможно точно воспроизвести результаты ручной сегментации вследствие субъективности человеческого слухового и зрительного восприятия. Подобных проблем не возникает при автоматической сегментации, которая все же не безошибочна, но дает воспроизводимые результаты. Идеальным случаем было бы создание алгоритма сегментации, работающего с любыми языками и дикторами.

Существует два основных типа алгоритмов сегментации речи. К первому типу относятся алгоритмы, которые производят сегментацию речи при условии, что известна последовательность фонем данной фразы. Другой тип алгоритмов не использует априорной информации о фразе, и при этом границы сегментов определяются по степени изменения акустических характеристик сигнала. Существует и иной тип алгоритмов, которые принимают решение как на основе априорной информации, так и на основе изменения акустических характеристик [1].

При автоматической сегментации желательно использовать только общие характеристики речевого сигнала, поскольку обычно на этом этапе нет конкретной информации о содержании речевого высказывания [2].

Общепринятая классификация звуков речи базируется на ряде упрощающих допущений, из которых наиболее существенными являются следующие:

– каждый язык может обойтись весьма ограниченным набором действий органов, участвующих в речеобразовании (набор «артикуляторных жестов»);

– каждый артикуляторный жест есть некоторое характерное для него состояние речевого аппарата (особенности работы источников звуковой энергии, конфигурация речевого тракта) и ведет к возникновению определенного звука речи;

– артикуляторные жесты выполняются последовательно один за другим [3].

В результате этих допущений мы имеем дело с идеализированной речью, составляющейся из предельно четко выраженных, характерно различающихся между собой звуковых элементов. При этом обеспечивается возможность разобраться в исходной структуре звукового материала, на которой основывается естественная речь того или иного языка.

В работе представлены результаты сегментации на вокализованные и невокализованные участки речи. В качестве примера использовалась фраза «Он целует её в щёки, в лоб, в закрытые веки», произнесенная женским и мужским голосом.

Для проведения сегментации необходимо найти непрерывные отрезки сигнала, состоящие из дискретных временных отсчетов с одинаковым признаком вокализации.

В таблице приведены значения моментов времени, полученные при автоматической сегментации границы между вокализованными и невокализованными участками различных дикторов и их сравнение с эталонной ручной сегментацией. В результате определено, что основные ошибки возникают при определении границы заключительного сегмента.

Значения моментов времени

ЭТ	ЭС	ЭТ	ЭС	ЭТ	ЭС
23диктор		24диктор		25диктор	
(Отт)	0,49	(ат1)	0,05	(Отт)	0,05
(н)		(н)		(н)	
(ц)		(Итт)	\	(ц)	
(эм1)		(ц)		(эм1)	
(л)		(эм1)		(л)	
(Утм)		(л)		(Утм)	
(й')		(Утм)		(й')	
(эм3)		(й')		(эм3)	
(т)	1,157	(ум2)	\	(т)	0,59
23диктор		24диктор		25диктор	
(и)	нет	(т)	0,71	(и)	0,695
(й')		(и)	0,77	(й')	

Продолжение таблицы

ЭТ	ЭС	ЭТ	ЭС	ЭТ	ЭС
(Омт)		(й')		(Омт)	
(ф)		(Омт)		(ф)	
(щ')		(ф)		(щ')	
(Омм)		(щ')		(Омм)	
(к')	1,673	(Омм)		(к')	1,23
(им2)	1,91	(к')	1,57	(им2)	нет
(пауза)		(им2)	1,68	(пауза)	\
(в)	1,93	(пауза)		(в)	1,42
(л)		(в)	1,74	(л)	
(Отт)		(л)		(Отт)	
(п)	2,25	(Отт)		(п)	1,95
(пауза)		(п)	2,15	(пауза)	\
(в)	2,37	(пауза)	\	(в)	2,04
(з)		(в)	2,37	(з)	
(ат1)		(з)		(ат1)	
(к)	2,686	(ат1)		(к)	2,275
(р)	2,719	(к)	2,55	(р)	2,29
(Ы)		(р)	2,65	(Ы)	
(т)	2,916	(Ы)		(т)	2,49
(ы)	2,939	(т)	2,84	(ы)	2,55
(й')		(ы)	2,92	(й')	
(эм3)		(й')		(эм3)	
(в')		(эм3)		(в')	
(Эмм)		(в')		(Эмм)	
(к')	3,353	(Эмм)		(к')	2,9
(им2)	3,403	(к')	3,522	(им2)	3,1
		(им2)	3,57		

Примечание. ЭТ – эталонная транскрипция (фразы), ЭС – эталонная сегментация (фразы).

В данной работе был наработан материал, содержащий речевые сигналы 23 дикторов, из них 14 женщин и 9 мужчин. Речевой материал необходим для проведения тестирования алгоритмов сегментации речевого сигнала на вокализованные и невокализованные участки.

ЛИТЕРАТУРА

1. Наука и образование [Электронный ресурс]. URL: http://technomag.edu.ru/doc/58069.html (дата обращения: 01.03.2011).

2. Сибирское отделение Российской академии наук [Электронный ресурс] URL: http://www.nsc.ru/ws/YM2004/8614/Medvedev.html (дата обращения: 01.03.2011).

3. Медицинская нанобиблиотека [Электронный ресурс]. URL: http://www.med-n.anolibrary.ru/node/144 (дата обращения: 02.02.2011).

РАЗРАБОТКА СИСТЕМЫ ВИРТУАЛИЗАЦИИ ДЛЯ АСУ ТП. ПРОГРАММНОЕ РЕШЕНИЕ

А.А. Петрова, студентка
Научный руководитель Ю.П. Палагин, главный специалист
отдела АТиС ООО НИПИ «ЭлеСи»
г. Томск, ТУСУР, ФВС, paa-pro@yandex.ru

Современный подход к автоматизации технологических процессов подразумевает комплексные решения на всех уровнях организации предприятия.

Автоматизация верхнего уровня – одна из самых важных, поскольку позволяет исключить либо значительно уменьшить влияние человеческого фактора. Программный комплекс должен решать ряд задач:

– обеспечение обмена данными с устройствами связи с объектом (контроллерами, платами ввода-вывода);

– обработка информации;

– отображение информации в доступной для оператора форме;

– ведение базы данных с технологической информацией;

– аварийная сигнализация и управление тревожными сообщениями;

– подготовка и генерирование отчетов о ходе технологического процесса.

Выполнение приведенного списка задач должно осуществляться в режиме реального времени – это, пожалуй, самое важное требование.

Всем этим требованиям удовлетворяют современные SCADA-системы (от англ. *Supervisory Control And Data Acquisition*) – «диспетчерское управление и сбор данных» – представляют собой программный пакет для сбора, обработки, отображения и архивирования информации об объекте управления [1].

SCADA-система включает в себя следующие подсистемы:

• Человеко-машинный интерфейс (HMI, англ. Human Machine Interface) – инструмент, который представляет данные о ходе процесса человеку-оператору, что позволяет ему контролировать процесс и управлять им.

• Диспетчерская система – собирает данные о процессе и отправляет команды процессору (управление).

• Абонентский оконечный блок, либо УСО (RTU, англ. Remote Terminal Unit), подсоединяемый к датчикам процесса, преобразует сигнал с датчика в цифровой код и отправляет данные в диспетчерскую систему.

• Программируемый логический контроллер (PLC, англ. Programmable Logic Controller) – используется как полевое устройство

из-за экономичности, универсальности и гибкости, нежели RTU специального назначения.

- Коммуникационная инфраструктура для реализации промышленной сети.

Построить свою АСУ ТП, организовать сбор данных и виртуализировать технологические процессы можно с помощью современных программных пакетов, как коммерческих, так и свободных для доступа пользователя версий. Я ознакомилась с программным комплексом Rapid SCADA, в котором планирую выполнять свой дипломный проект.

Это бесплатная версия, которая обладает полной функциональностью базовой версии и позволяет спроектировать систему со следующими функциями:

– мониторинг состояния и управление инженерными системами зданий, технологическими системами предприятий;

– учёт расхода энергоресурсов, потребляемых организацией;

– учёт ресурсов оборудования;

– контроль систем пожарно-охранной сигнализации;

– контроль и управление доступом на объекты предприятия;

– учёт рабочего времени персонала предприятия (при использовании в составе системы «Часовой») [2].

В ходе ознакомления с рядом программных комплексов, предназначенных для виртуализации АСУ ТП, был выявлен ряд преимуществ пакета Rapid SCADA. В результате после реализации проекта разработанная в нем система позволит предприятию:

– уменьшить расходы на электрическую и тепловую энергию за счёт оптимизации потребления энергоресурсов;

– достичь экономического эффекта при автоматизации управления технологическими процессами;

– обеспечить высокий уровень безопасности на предприятии или географически распределённых контролируемых объектах;

– повысить качество работы подразделений, отвечающих за эксплуатацию зданий, и службы контроля безопасности;

– повысить рабочую дисциплину сотрудников организации (при использовании в составе системы «Часовой»).

ЛИТЕРАТУРА

1. Википедия – свободная энциклопедия [Электронный ресурс]. URL: http://ru.wikipedia.org/wiki/SCADA (дата обращения: 03.03.2011).

2. Rapid SCADA – бесплатная система диспетчерского контроля [Электронный ресурс]. URL: http://www.rapidscada.ru/ (дата обращения: 24.02.2011).

МЕТОДЫ ИССЛЕДОВАНИЯ СЛУХА

А.Г. Понизов, аспирант 1-го года обучения
Научный руководитель Р.В. Мещеряков, доцент, к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, ponizov@mail.ru

За всю историю исследования человеческого слуха было придумано множество методов и способов, начиная от заливания воска в уши до создания специализированных электроакустических приборов – аудиометров.

Все исследования слуха можно разделить на две большие группы по психофизиологическому фактору – субъективные и объективные методы.

Субъективное исследование слуха базируется на субъективных ощущениях обследуемого и на сознательной, зависящей от его воли ответной реакции. Объективная, или рефлекторная, аудиометрия основывается на рефлекторных безусловных и условных ответных реакциях обследуемого, возникающих в организме в ответ на звуковое воздействие и не зависящих от его воли.

Акустическая импедансометрия – метод исследования, основанный на измерении акустического сопротивления (или акустической податливости) звукопроводящих структур периферической части слухового анализатора. В клинической практике чаще всего используются две методики импедансометрии – тимпанометрия и акустическая рефлексометрия [1].

Тимпанометрия позволяет оценить подвижность барабанной перепонки и слуховых косточек. Это быстрый и неинвазивный метод диагностики таких заболеваний, как экссудативный (секреторный) средний отит, отосклероз и др. Метод используется для дифференциальной диагностики заболеваний среднего и внутреннего уха, для определения порогов дискомфорта, используемых при подборе и настройке слуховых аппаратов.

Отоакустическая эмиссия выступает в роли акустического ответа, который является отражением естественной работы рецептора, отвечающего за *слуховую активность*. Это очень слабые по частоте колебания звука, которые генерирует улитка [1].

Речевое исследование слуха – традиционно количественная оценка слуховой функции – начинается с определения расстояния между произносящим звуки, слова или цифры исследователем и ухом испытуемого, при котором он слышит речь – шепотную, разговорную, громкую или крик.

Исследование камертонами. Камертоны позволяют определить остроту восприятия звуков слуховым анализатором, распространяющихся по воздуху и по костной ткани [2].

Аудиометрия – исследование чувствительности слуха с помощью электроакустического прибора (аудиометра).

Аудиометрия – исследование, необходимое как для определения степени нарушения слуха, так и для подбора необходимого слухового аппарата [2].

Речевая аудиометрия обеспечивает постоянство речевого материала и дикции; возможность регулировки и регистрации интенсивности передаваемых слов; определение потери слуха в сравнимых единицах (децибелах) [3].

Шумовая аудиометрия. Другой психофизиологической функцией звукового анализатора является маскировка – величина, обратная помехоустойчивости. По мнению многих исследователей, маскировка – это процесс взаимодействия полезного и помехообразующих звуков, при которых последние подавляют первых и функцию выделения из общего звукового поля полезной информации [3].

Тональная аудиометрия определение слуховой чувствительности на звуки различной частоты. На частотах от 125 до 8000 Гц определяется минимальная интенсивность звука, которая вызывает слуховое ощущение.

Тональная пороговая аудиометрия. Исследование включает определение порогов при воздушном и костном звукопроведении. Для этого определяют пороговую чувствительность органа слуха к восприятию звуков различных частот, подаваемых через воздушные наушники или костный телефон.

Тональная надпороговая аудиометрия – исследование тихими пороговой интенсивности звуками – не дает полного представления о способности звукового анализатора воспринимать разнообразные, постоянно встречающиеся в повседневной жизни звуковые раздражители, интенсивность которых намного превышает пороговую, в частности звуки разговорной речи.

На рис. 1 представлено образное представление методов исследования слуха.

Все представленные выше методы – это все лишь малая часть основных методов, когда общее количество методов исследования слуха насчитывает порядка десяти тысяч. Такое большое количество методов связано с тем, что органы слуха человека – один из очень сложно диагностируемых органов. Также стоит отметить, что слух в свою очередь является одним из главных каналов приёма информации. Люди, которые страдают нарушением слуха, страдают от нехватки информации об окружающем их мире.

Рис. 1. Методы исследования слуха

Таким образ, крайне важно заниматься как разработкой новых методов исследования слуха, так и созданием абсолютно новых приборов для исследования слуха. Одним из таких устройств может стать портативный аудиометр, позволяющий оценить слух не только одноточечными исследованиями в кабинете врача-отоларинголога, а проводить многоточечные исследования своего собственного слуха, выявляя тем самым наиболее точное состояние своего органа слуха.

ЛИТЕРАТУРА

1. *Наседкин А.Н.* Врожденные аномалии уха, горла, носа и шеи у детей. М., 1975. С. 38–43.

2. *Тарасов Д.И., Наседкин А.Н., Лебедев В.П., Токарев О.П.* Тугоухость у детей. М.: Медицина, 1984. 240 с.

3. *Тавартkиладзе Г.А., Васильева Л.Д.* Раннее выявление нарушений слуха у детей первых лет жизни: метод. реком. М., 1988. С. 15.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЁТА ОРГТЕХНИКИ

М.П. Прокопчук, А.А. Ковалёв, А.С. Малоштан, студенты 3-го курса
Научный руководитель С.Ю. Исхаков, аспирант каф. КИБЭВС
г. Томск, ТУСУР, каф. КИБЭВС, proroker@sibmail.com

Число используемой оргтехники в современных организациях постоянно увеличивается, увеличиваются объёмы потребления расход-

ных материалов. Необходимо вести постоянный учёт оргтехники и расходных материалов. Для автоматизации данного процесса в Сибирском государственном медицинском университете необходимо разработать программный комплекс для решения этой задачи.

Было решено создать единую базу данных [1], содержащую перечень оргтехники СибГМУ и всю связанную с ней информацию, что позволит автоматизировать ее обработку. Также необходим графический интерфейс для пользователей. Условно решение задачи автоматизации процесса учёта можно разделить на четыре основных этапа, для каждого из которых необходимо определить методы и средства реализации.

Первым этапом является проектирование и создание базы данных. Концептуальная модель [2] базы приведена на рис. 1.

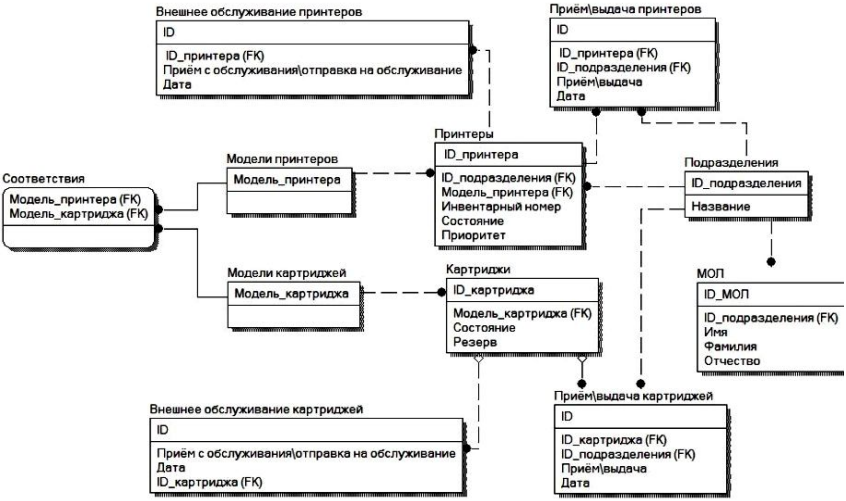


Рис. 1. Концептуальная модель базы данных учёта оргтехники СибГМУ

Для реализации первого этапа была выбрана СУБД MySQL [1], предоставляющая необходимые средства для решения данной задачи. Кроме того, использование MySQL для некоммерческих проектов не требует финансовых затрат.

Второй этап – разработка интерфейса [1]. Решено было построить его с использованием веб-технологий, так как это позволит пользователям дистанционно получать доступ к базе данных. Для достижения этой цели используется язык программирования PHP, языки HTML и CSS [1]. Разработку веб-интерфейса можно разделить на 3 подзадачи: дизайн, вёрстка и программирование. В результате создана веб-

оболочка с реализацией основных функций: добавление, удаление, изменение записей в базе данных.

Третий этап – реализация информационной безопасности (разграничение прав доступа и защита от несанкционированного доступа), репликации и резервного копирования.

Заключительный этап – завершение разработки программного средства, тестирование и, при необходимости, доработка.

На данный момент создана база данных и веб-интерфейс, реализованы функции репликации и резервного копирования. Дальнейшая работа будет заключаться в обеспечении безопасности, добавлении необходимых функций в веб-интерфейс, автоматизации заполнения базы данных списком оргтехники и расходных материалов с последующим полным тестированием готового решения.

Выполнено в рамках проекта ГПО КИБЭВС-1002 – «Построение автоматизированной системы администрирования локально-вычислительных сетей».

ЛИТЕРАТУРА

1. *Колисниченко Д.Н.* PHP5/6 и Mysql. Разработка Web-приложений. СПб.: БХВ-Петербург, 2009. 624 с.

2. *Карпова Т.С.* Базы данных: модели, разработка. СПб.: Питер, 2001. 304 с.

ОПТИМАЛЬНОЕ ПРОЕКТИРОВАНИЕ ТЕХНОЛОГИЙ ИНДУКЦИОННОГО НАГРЕВА

А.М. Щелочкова, каф. электроснабжения промышленных предприятий, магистрант

Научный руководитель Л.С. Зимин, зав. каф., проф.

г. Самара, Самарский государственный технический университет, epp@samgtu.ru

Рассматривается системный подход к проектированию и функционированию системы индукционного нагрева, включающей индукционную нагревательную установку (ИНУ), источник питания, системы электроснабжения и управления и предназначенной для нагрева металла под деформацию. Причём ИНУ рассматривается в едином комплексе с оборудованием для обработки металла давлением (ОМД) с целью достижения экстремальных технико-экономических показателей работы технологического комплекса в целом.

Применение системного подхода в данном случае вызвано тем, что он представляет собой методологию эффективного решения задач, возникающих в сложных системах, к которым может быть отнесен и комплекс «ИНУ-ОМД».

При формализации достаточно общей задачи проектирования проектное решение представляется вектором

$$X = X\left[Y(t), X(0), Z, K\right], \qquad (1)$$

где составляющие векторы $Y(t)$ – внешнее воздействие, зависящее от времени; $X(0)$ – начальное условие; Z – параметры, не зависящие от времени; K – вектор параметров структурной или конструктивной схемы.

При этом можно считать, что

$$Z = Z(K), \quad Y = Y(t, K), \quad X = X(t, K). \qquad (2)$$

На реализацию и функционирование объекта проектирования накладываются разнообразные ограничения, совокупность которых можно представить с помощью вектор-функционала

$$H\left[X(t), Y(t), X(0), Z, K\right] \leq\geq 0 . \qquad (3)$$

Условия (1)–(3) выделяют в векторном пространстве переменных замкнутые допустимые области, внутри которых находятся искомые проектные решения

$$X \in \Omega_x , \; Y \in \Omega_y , \; X(0) \in \Omega_{0\,0} , \; Z \in \Omega_z , \; K \in \Omega_k , \qquad (4)$$

где Ω – замкнутое множество векторов.

Представленная задача (1)–(4) относится к обратным задачам исследования операций, которые в общем виде некорректны. Для регуляризации задачи используется идея целенаправленности, реализуемая с помощью критерия оптимальности, определяемого через проектные данные функционалом

$$I \cdot \left[X(t), Y(t), X(0), Z, K\right] . \qquad (5)$$

Введение критерия оптимальности преобразует рассмотренную выше задачу проектирования в задачу оптимального проектирования: максимизировать (минимизировать) функционал I по всем независимым аргументам при соблюдении (4).

Если рассматривается случай, когда объект оптимизации по принципу действия предопределен – система индукционного нагрева, то рассмотрению подлежат последние два уровня задачи оптимизации, которая в общем случае представляется в виде

$$I\left(X^* = extrI(X)\right), \quad \forall X \in \Omega_x . \qquad (6)$$

Здесь X^* – оптимальное проектное решение, отражающее в соответствии с (1) структуру системы и ее конструктивные и режимные параметры.

Вначале, на этапе структурной оптимизации, обычно на эвристическом уровне определяются: тип индукционного нагревателя по принципу действия и конструктивному исполнению; схема соединения секций индуктора; компоновка нагревательного отделения. Затем производится определение наилучших значений параметров – параметрическая оптимизация, когда находится экстремум (5) по аргументу Z при фиксированном K с учетом (4). К этому же уровню можно отнести задачу оптимального управления, когда аргументом является $Y(t)$.

Перед параметрическим синтезом необходимо четко выделить параметры системы, которые в общем случае можно разделить на входные (варьируемые) и выходные (рабочие показатели). Вектор варьируемых параметров значениями своих составляющих однозначно определяет вектор рабочих показателей, определяющий качество системы и характеризующий вариант проекта.

Заключение. Системный подход к оптимальному проектированию при индукционном нагреве позволяет по-новому увидеть объект проектирования: основной фактор, органически связывающий обе стадии обработки металла в единый технологический комплекс – температурные кондиции металла, заранее не фиксируются, а находятся, исходя из достижения экстремума совокупного экономического показателя.

ОПТИМАЛЬНАЯ МОДЕЛЬ РОБОТА

И.И. Шиляев, студент 4-го курса
Научный руководитель Д.Д. Зыков, доцент, к.т.н.
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, virtualist@sibmail.com

Целью работы является изучение предмета автоматизации и робототехники, рассмотрение различных модификаций существующих в мире роботов, количественная и качественная оценка, технико-экономическое обоснование создания учебно-исследовательской модели роботов.

В мире уже достаточно продолжительное время существует огромное разнообразие робототехнических решений. Существует множество различных модификаций и даже классификаций роботов [1]. Несмотря на это, все модели можно охарактеризовать не только по техническим, но и по производственным параметрам, что обусловлено стандартизацией и унификацией технологии производства. Так, вне зависимости от типа модели созданного робота он, как и любая товарная (экономическая) единица, подпадает под экономические законы и законы надежности.

Вполне естественно, что произведенные по заводским технологиям и в больших объемах, да еще и стандартизованные или унифицированные, при необходимости конкурентоспособности, роботы становятся надежнее, экономичнее, более эргономичными и намного экологичными. Надежность обусловливается автоматизацией, которая в значительной степени точнее человека и не подвержена большинству внешних воздействий (отсутствует человеческий фактор). Экономичность во многом обусловлена эффектом масштаба, который делает массовую продукцию менее затратной. Эргономичность и экологичность также гораздо легче достигаются в производственной среде.

Создание любой модели робота в рамках учебно-образовательной деятельности во многом зависит от технического уровня учебного заведения, его экономической обеспеченности и квалификации сотрудников (преподаватель, студентов, аспирантов и др.), занятых в проекте. Естественно, что создание высокотехнологичных, надежных роботов в российских вузах в связи с экономической неразвитостью просто не по карману. Эта причина не только лишает вуз необходимых деталей, но и необходимого технического оборудования. Из-за этой же причины многие сотрудники стремятся принять участие в менее затратных и более прибыльных проектах. Как следствие, чуть ли не каждый прибор имеет возраст 10–20 (а то и более) лет, если вообще имеется, зато почти все компьютерные и программные средства приобретаются и используются с завидной частотой. Так, создание любого мало-мальски прибыльного компьютерного приложения занимает и меньше времени, и меньше ресурсов, и больше прибыли принесет (а следовательно, этот проект более привлекателен), зато более наукоемкие (вместе с тем и более затратные) материальные технические единицы используются в научно-исследовательской деятельности дольше и гораздо более эффективней (что в конечном итоге принесет гораздо больше материальных и нематериальных благ).

Поэтому роботом, созданным в рамках вуза, целесообразно придать небольшую движущую платформу с расположенными на ней датчиками, модулем управления, общими размерами не более 0,7 м (высота) 0,4–0,5 м (длина и/или толщина) и общей массой не более 20–30 кг [2].

ЛИТЕРАТУРА

1. *Шиляев И.И.* Создание исследовательского робота // Научная сессия ТУСУР–2010: Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых, Томск, 4–7 мая 2010 г. Томск: В-Спектр, 2010. С. 72–73.

2. *Зыков Д.Д., Шиляев И.И.* Учебный робот // Современное образование: перспективы развития многопрофильного технического университета: Матер. междунар. науч.-метод. конф., 28–29 января 2010 г., Томск. Томск: Том. гос. ун-т упр. и радиоэлектроники, 2010. С. 160–161.

К ВОПРОСАМ О СВЕТОТЕХНИКЕ

И.И. Шиляев, студент, каф. КИБЭВС
г. Томск, ТУСУР, ФВС, virtualist@sibmail.com

Светотехника – это наука о свойствах света и принципах его использования, а также о новых альтернативных источниках получения света. Светотехника связана с энергетикой, электроникой, оптикой. Наиболее востребованные и популярные направления светотехники – разработка новых световых источников и приёмников, управление светом и цветом. В этой связи возрастает роль оперативного и достоверного измерения световых и энергетических параметров и характеристик источников излучения и приёмников в видимой области спектра. К числу таких параметров относятся яркость, освещенность, сила света, пульсации освещённости и ряд других параметров, формирующих комфортные условия и «климат труда» в жизни людей.

Применяются два метода световых измерений: субъективный (зрительный), при котором приемником служит человеческий орган зрения (глаз), и объективный (физический), где для световых измерений используются физические приемники – фотоэлементы, фотографические материалы и др. В настоящее время субъективные измерения проводятся значительно реже, чем объективные. Субъективным методом пользуются при градуировке физических приемников, измерениях на линейном фотометре (светотехнической скамье), измерениях цветовой температуры. Измерение яркости проводят тем и другим методом. Для измерения освещенности, светового потока, снятия продольных кривых сил света, измерения энергетических величин используются физические приемники потока излучения. В основе субъективного метода световых измерений лежит способность глаза устанавливать равенство яркостей двух соприкосающихся поверхностей. При использовании для световых измерений физических приемников излучения приходится исправлять (корригировать) их спектральные чувствительности под спектральную чувствительность светлоадаптированного глаза [1].

При оценке освещения используют несколько параметров (яркость, освещенность, сила света и пр.). Основным показателем является освещенность. Измерение освещенности осуществляется прибором, названным «люксметр». Принцип работы люксметра основан на преобразовании светового потока, создаваемого естественным и искусственным светом, в непрерывный электрический сигнал, пропорциональный световой освещенности. Непрерывный электрический сигнал преобразуется в цифровой код и числовое значение индицируется на цифровом табло индикаторного блока. Показания индицируются в

единицах люкс или килолюкс (1000 люкс). Освещённость признана одним из определяющих параметров жизнедеятельности живой природы и человека в частности. Требования по освещённости в быту и на рабочих местах регулируются национальными и международными нормативными актами.

Эти правила устанавливают определённый набор требований к количественным и качественным показателям освещения. В этих нормах регламентируются такие параметры, как освещенность зоны выполнения зрительной задачи (Task Area), освещённость зоны непосредственного окружения, обобщённый показатель дискомфорта, общий индекс цветопередачи, пульсации освещённости. Для рабочих мест с компьютерами, кроме этого, регламентируются предельные значения яркости светильников, отражающихся на экранах дисплеев. Первые два параметра характеризуют количественную сторону освещения, три других – качественную. В нашей стране основными документами, устанавливающими требования к освещению, являются «Строительные нормы и правила» (СниП), «Санитарные правила и нормы» (СанПиН) [2, 3] и иные отраслевые акты. Проводятся работы по приведению отечественных норм в соответствие с общеевропейскими.

ЛИТЕРАТУРА

1. *Гуторов М. М.* Основы светотехники и источники света: учеб. пособие для вузов. 2-е изд., доп. и перераб. М.: Энергоатомиздат, 1983. 384 с.

2. СНиП 23-05–95. Строительные нормы и правила РФ естественное и искусственное освещение. Введен 1996-01–01. Минстрой России. М.: ГП ЦПП, 1995.

3. Санитарные правила и нормы СанПиН 2.2.1/2.1.1.1278–03. Гигиенические требования к естественному, искусственному и совмещенному освещению жилых и общественных зданий. Введен 2003-15–06. Главный государственный санитарный врач Российской Федерации. М., 2003.

СИСТЕМА ДИАГНОСТИКИ ОБЪЕКТОВ ЖКХ И УПРАВЛЕНИЯ ОБСЛУЖИВАЮЩИМ ПЕРСОНАЛОМ НА БАЗЕ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ

И.Н. Шишкин, студент 4-го курса, М.И. Мельников, аспирант
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, sin@keva.tusur.ru

Ещё десять лет назад автоматизация и управление в системе ЖКХ в России были крайне не развиты, в то время как зарубежные компании уже повсеместно внедряли комплексные системы автоматизации зданий (так называемые системы умного дома).

Современные технологии могут значительно облегчить труд человека, и в частности системы контроля процессов с применением ЭВМ – SCADA-системы. Они получили широкое распространение для управления технологическими, инфраструктурными и обслуживающими процессами.

Зачастую от действий оператора или обслуживающего персонала может зависеть очень многое, и цена их ошибки будет колоссальна. Поэтому желательно минимизировать влияние человеческого фактора, именно с этой целью создаётся данная система.

На рис. 1 представлена упрощенная структурная схема системы.

За основу взята SCADA-система, которая через технологическую сеть связана с объектами ЖКХ и отслеживает все изменения параметров объектов. В случае возникновения неполадок на объекте информация передаётся SCADA-системе, которая в свою очередь передает ее с помощью технологии OPC [2] программному модулю, с помощью которого производиться анализ и обработка полученной информации, с дальнейшей передачей данных на мобильные устройства обсуживающего персонала. Также в системе есть база данных, используемая для обработки и хранения данных.

Технологическая сеть может быть создана на базе беспроводных технологий, что значительно упростит обслуживание сети и увеличит скорость развёртывания системы, так как отсутствует необходимость прокладывать каналы связи.

Благодаря использованию технологии OPC система не привязана к конкретной SCADA-системе, что облегчает внедрение системы и позволяет использовать встроенные средства программирования SCADA-системы для решения широкого спектра задач.

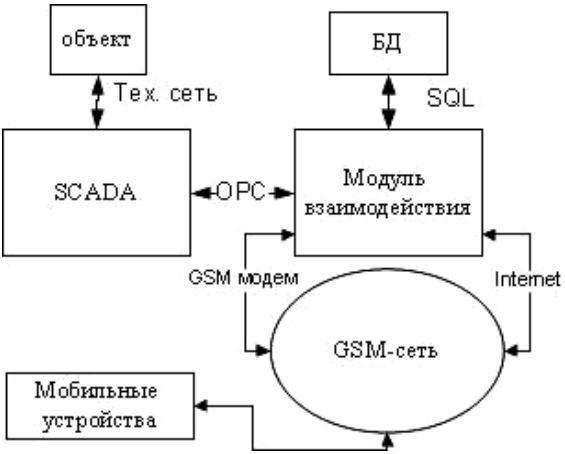


Рис. 1. Упрощенная структурная схема

Для передачи данных на мобильные устройства используются GSM-сети, и со стороны управляющего компьютера было выделено 2 независимых канала связи: непосредственно GSM-сеть и сеть Internet. Это обеспечивает более надёжную работу системы. Для защиты передаваемые данные шифруются, также для подключения к системе мобильное устройство должно быть авторизовано.

Наличие обратной связи позволяет не только контролировать действия персонала, но и облегчить его работу. С помощью мобильного устройства можно диагностировать систему после восстановления (ремонта).

Создание приложений на платформах java и windows mobile также ускорит внедрение системы, так как отсутствует необходимость в создании специализированных мобильных устройств – достаточно обычных сотовых телефонов или коммуникаторов, которые получают всё большее распространение. Мобильные устройства позволяют отслеживать положения персонала, что служит для снижения времени реагирования, а также позволит контролировать добросовестность выполнения работы.

База данных служит для хранения информации о персонале (контактная информация, состояние, положение, рейтинг), информации о самих объектах (расположение, модель и т.п.), ведутся журналы работы системы, возможен подсчет различной статистики.

В таблице представлена сравнительная таблица существующих решений с функционалом разрабатываемой системы.

Сравнительная таблица функциональных возможностей

Функционал	Диспетчерский комплекс “ОБЬ”	Комплекс диспетчеризации лифтов КДЛ-2	Проект автоматизации здания компании КРОК	Sauter Corp.Building Management System	Siemens Corp. DESIGO
Беспроводные каналы связи	Да	Да	Нет	Нет	Нет
Ведение журналов	Да	Нет	Да	Да	Да
Наличии базы данных	Нет	Нет	Да	Да	Да
Сандартизованные технологии обмена данными (OPC, SQL и тд.)	Нет	Нет	Да	Да	Да
GPS-трекинг	Нет	Нет	Нет	Нет	Нет
Удалённое взаимодействие системы управления с обслуживающим персоналом	Нет	Нет	Нет	Нет	Да
Масштабируемость	Да	Да	Нет	Да	Да
Управление персоналом	Нет	Нет	Нет	Нет	Нет
Голосовое оповещение	Да	Да	Да	Да	Да
Географическая распределённость	Да	Да	Нет	Нет	Нет
Взаимидействие с инженерными системами объекта	Да	Нет	Да	Да	Да

ЛИТЕРАТУРА

1. *Мельников М.И.* Разработка автоматизированной системы управления распределённым лифтовым хозяйством на базе беспроводных технологий // Доклады ТУСУРа. Томск: Изд-во ТУСУРа, 2009. №1 (19), ч. 2. С. 81–82.

2. OPC Foundation. http://www.opcfoundation.org

СРАВНЕНИЕ КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРЕДНАЗНАЧЕННОГО ДЛЯ ОБРАБОТКИ РЕЧЕВОГО СИГНАЛА

И.Ю. Шорохов, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, krain2007@yandex.ru

Важнейшим параметром, характеризующим спектр речевого сигнала, являются форманты. Источник звука вызывает в системе резонаторов (т. е. в надгортанных полостях) собственные колебания, следовательно, то, что мы обычно слышим, – это сложный звук, являющийся результатом преобразования звука, возникающего в источнике, резонирующей системой надгортанных полостей. Собственные частоты резонаторов являются наиболее усиленными в акустической картине звука. Эти усиленные частоты называют «формантами» звука.

Форманты определяют концентрацию энергии речевого сигнала по частоте и характеризуют вокализованные звуки. Форманты, начиная с F3, несут информацию о дикторе и широко используются в системах распознавания диктора [1].

На участках вокализованного звука речевой тракт человека возбуждается периодическим колебанием связок. Период этого колебания называют периодом основного тона. Эта величина является индивидуальной характеристикой диктора. Она может меняться в зависимости от эмоциональной окраски речи, но в достаточно узких пределах. При параметрическом кодировании речи предполагают, что частота основного тона человека лежит в пределах 80–400 Гц.

Одним из наиболее удобных и, как следствие, популярных программных инструментов для обработки речевых сигналов является приложение PRAAT, позволяющее, в частности, осуществлять «формантный анализ» [2].

Для работы с приложением PRAAT выставлялись настройки по умолчанию. Графики представляют собой зависимость частоты от времени, максимальное значение частоты 3000 Гц, время в миллисекундах и зависит от продолжительности звукового отрезка. При определении частоты основного тона частота выставлена на 500 Гц.

Помимо приложения PRAAT, для получения параметров речевого сигнала, необходимых для описания ударных гласных звуков, использовался программный комплекс, реализующий модель периферической части слуховой системы человека.

Для обработки использовались вручную отсегментированные речевые сигналы дикторов обоего пола.

Для параметрического описания вокализованных участков использовались следующие параметры:

1) признак вокализованности сегмента;

2) частота максимальной по интенсивности гармоники, лежащей в области частот до 800 Гц;

3) частота второй по интенсивности гармоники, лежащей в области частот до 800 Гц;

4) частота максимальной по интенсивности гармоники, лежащей в области частот от 800 до 2300 Гц;

5) частота второй по интенсивности гармоники, лежащей в области частот от 800 до 2400 Гц [3].

На рис. 1 показан обработанный речевой сигнал (верхний – программный комплекс по обработке речевых сигналов, нижний – приложение PRAAT). При этом черным цветом указаны максимальные по интенсивности гармоники в каждой из рассматриваемых областей, а серым – вторые по интенсивности гармоники. На нижнем рисунке белым цветом обозначены первая, вторая форманты.

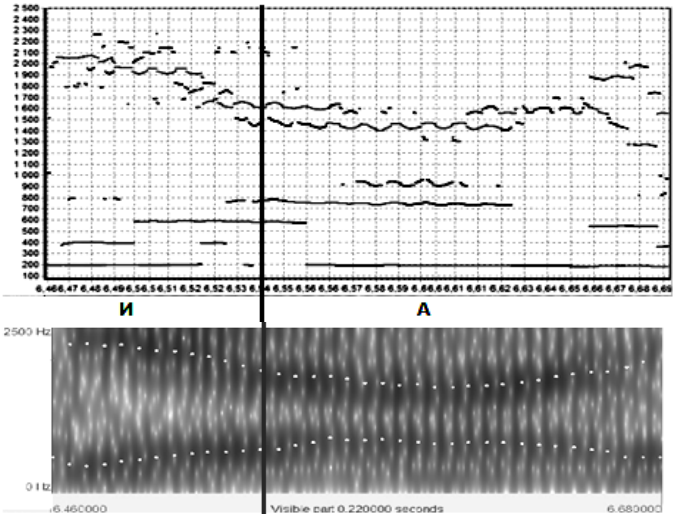


Рис. 1. Звук «иа» из слова «океана» (диктор – женщина)

Из верхнего графика рис. 1 следует, что на участке гласной «И» первая (200–600 Гц) и вторая (1700–2050 Гц) форманты соответствуют известным данным по частоте формант. На участке гласной «А» первая форманта (200–750 Гц) соответствует среднестатистическим частотам, а вторая (1400–1700 Гц) их превышает.

Из нижнего графика первая (400–690 Гц) и вторая (1700–2250 Гц) форманты участка гласной «И» соответствуют известным данным по частоте формант. На участке гласной «А» первая (560–840 Гц) форманта также сходится с известными частотами, вторая (1570–2000 Гц) форманта их превышает.

На рис. 2 изображена динамика изменения частоты основного тона на анализируемом участке.

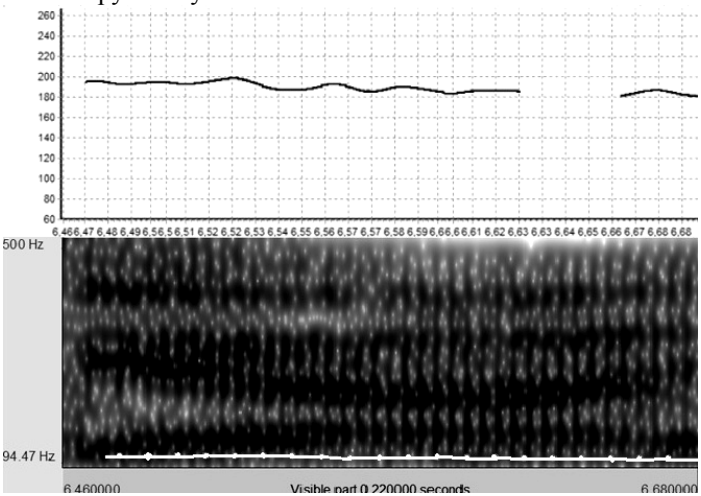


Рис. 2. Частота основного тона

Оба приложения показали примерно одинаковые результаты.

$F_{\text{осн.т}}$ женских голосов от 200 до 400 Гц. Она определяется числом колебаний голосовых связок. *F*I определяется степенью подъема языка к нёбу, т.е. подъемом гласного, *F*II определяется степенью продвинутости языка, т.е. его рядом.

Из рис. 1 следует, что $F_{\text{осн.т}}$, показанная приложением PRAAT, не соответствует действительности, т.е. алгоритм определения $F_{\text{осн.т}}$ работает некорректно.

ЛИТЕРАТУРА

1. *Бондарко Л.В.* Звуковой строй современного русского языка. М.: Просвещение, 1977. 175 с.

2. Paul Boersma's writings on the Praat program [Электронный ресурс]. URL: http://www.fon.hum.uva.nl/paul/praat.html (дата обращения: 28.02.2011).

3. *Конев А.А., Мещеряков Р.В., Тиунов С.Д. и др.* Параметрическое описание ударных гласных звуков // Сб. тр. XXII сессии Российского акустического общества. Т. III. М.: ГЕОС, 2010. С. 41–45.

СИСТЕМА ОЦЕНКИ КАЧЕСТВА ЖИЗНИ

А.Г. Сизов, аспирант

г. Томск, ТУСУР

Голосообразование является очень сложным механизмом, в котором взаимодействует большое количество органов и систем. Проблемы диагностики и лечения нарушений голоса – это актуальная и сложная тема, которая еще не полностью раскрыта. Клиническая картина различных функциональных нарушений голоса сильно отличается. Часто дисфонии перерастают в серьезные заболевания, в результате чего у человека проявляется длительная нетрудоспособность, иногда он становится профессионально непригодным (певец, диктор) – оценка качества жизни у таких людей становится довольно низкой.

Весь акт звукообразования управляется центральной нервной системой (ЦНС), способной регулировать частоту и амплитуду колебаний голосовых складок. Темпы, с которыми развивается наше общество, предъявляют такие высокие требования к нервно-психической сфере, что риск функциональных голосовых нарушений значительно увеличивается. Довольно часто психический фактор недооценивается в диагностике соматических заболеваний, поэтому болезнь может перейти в более тяжелую форму, выздоровление затянуться, а в более крупном масштабе – увеличиваются расходы государства на таких больных. А ведь нейропсихические отклонения являются основой нарушений голосообразования. Увеличение числа стрессовых ситуаций, ухудшение качества жизни за последние несколько лет увеличили распространенность нарушений голоса (рис. 1).

Во время исследования наблюдалось 120 больных с нарушениями голосообразования. Чтобы повысить эффективность диагностики и лечения больных с нарушениями голосообразования, определить влияние лечения на конкретные категории с проблемами дисфонии, применялись различные исследования по оценке качества жизни. Это и анкетирование, и тестирование, и клиническое интервью, экспериментально-психологическое исследование. Проводилось лечение функциональных дисфоний с помощью дифференцированного использования голосового тренинга, осуществлялись психологическая кор-

рекция с ортофонической коррекцией голоса, физиотерапия (как стационар, так и амбулаторные условия).

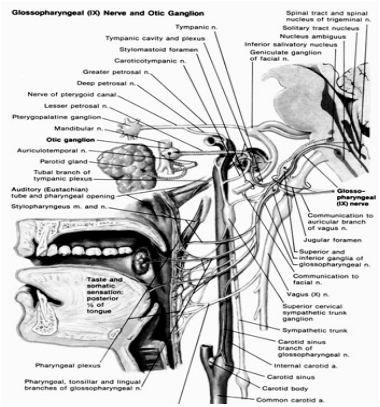


Рис. 1

В результате оценки голосового аппарата была прослежена четкая закономерность между невротическими расстройствами и нарушениями голосообразования. Также было замечено, что изменения в голосе напрямую зависят от тяжести и формы неврологического расстройства. Изучение качества жизни больных с функциональными дисфониями позволило составить полную картину о влиянии заболевания на самые разные моменты качества жизни – физическую, социальную, эмоциональную сферу. Такой метод оценки качества жизни существенно помогает в правильности диагностирования, в индивидуализации проводимого лечения и в улучшении его эффективности. Сроки лечения сократились на 9–14 дней, а повторность заболевания снизилась на тридцать процентов.

Было выявлено, что нарушения в тонусе гортани вызывают функциональные нарушения в голосе. Около 60% больных имели гипотонусную форму дисфонии, 21% – гипертонусную, а 19% больных имели смешанную форму дисфонии. Низкие показатели качества жизни, а именно психологический стресс и хронические эмоциональные перегрузки, стали основными причинами расстройств у больных с нарушениями голосообразования. Так как основой проведенной терапии являлись показатели качества жизни, а не только акустические параметры голоса, то это следует учитывать при реабилитационных мероприятиях больных (проведена адекватная терапия). Привлечение профильных специалистов и принятие во внимание индивидуальных аспектов заболевания каждого больного, включая оценку качества жизни, позволяют увеличить эффективность лечения.

МОДЕЛИРОВАНИЕ ТЕПЛОВЫХ ПРОЦЕССОВ ДЛЯ ЗАДАЧ СИНТЕЗА УПРАВЛЕНИЯ

С.В. Степанов, И.О. Щепин, аспиранты каф. электроснабжения промышленных предприятий

Научный руководитель А.А. Базаров, доцент

г. Самара, Самарский государственный технический университет, epp@samgtu.ru

Рассматривается задача построения модели тепловых процессов для синтеза и исследования системы управления индукционным нагревом тел сложной формы. Исследуемый объект относится к объектам с распределенными параметрами. Задача синтеза систем управления объектами с распределенными параметрами может быть решена путем построения аппроксимирующей многосвязной системы с сосредоточенными параметрами на основе метода интегральных элементов.

Для использования аппарата теории систем с сосредоточенными параметрами необходим переход от математической модели объекта с распределенными параметрами, записанной в виде уравнения в частных производных, к классической формулировке в виде системы обыкновенных дифференциальных уравнений.

Построение качественной модели возможно несколькими путями. Например, с помощью обратного перехода от конечно-элементной формулировки к классической постановке задачи управления. Более предпочтительным вариантом решения указанной задачи представляется исходная дискретизация расчетной области с помощью метода интегральных элементов.

Тепловые потоки между соседними элементами определяются через усредненные температуры блоков, площади контакта между ними и коэффициент теплопроводности. Таким образом, можно сформировать как чисто электрическую модель на конденсаторах и резисторах, так и ее цифровой аналог.

Аналогичный подход, основанный на расчетах электрических моделей различных процессов неэлектрической природы, таких, как тепловые, диффузионные, пневматические, используется при определении теплового состояния различных объектов.

Комбинация электрических моделей и современной вычислительной техники с соответствующими вычислительными методами позволила авторам решить ряд сложных задач.

Для использования стандартных программных средств при моделировании процессов необходим переход из области действительных чисел в область изображений. Это дает возможность представить объект в виде набора интегрирующих звеньев, блоков суммирования и

усилителей. Такое представление является довольно громоздким, но, помимо возможности исследования процессов на модели, может быть использовано в качестве встроенной модели в контур управления реального процесса.

Важной особенностью системы индукционного нагрева является несимметричность управляющего воздействия. Обычно уровень мощности внутренних источников превышает мощность потерь на несколько порядков. Кроме того, области приложения этих мощностей тоже не совпадают. Переходный процесс в такой системе, полученный с помощью модели теплового процесса, имеет ярко выраженные особенности, проявляющиеся в том, что кривые разогрева и охлаждения представлены различными экспонентами.

Удобным средством для моделирования замкнутых систем управления объектами с распределенными параметрами, дискретизированными в пространстве, является пакет *SIMULINK MATLAB*. Наличие большого количества линейных и нелинейных блоков в его составе позволяет учитывать все особенности как самого объекта, так и системы управления.

Для замкнутой системы управления, имеющей небольшую величину коэффициента усиления, период колебаний имеет явную зависимость от состояния во внутренних областях. Этот факт позволяет подойти к решению некоторых задач при синтезе управления с более практических позиций. Например, вместо решения уравнения Риккати для поиска коэффициентов оптимального регулятора вполне возможно найти приемлемые по точности зависимости коэффициентов от времени через зависимости от теплосодержания нагреваемого тела. Еще одной важной особенностью является то, что для некоторых задач нагрева в принципе не обязательно становится отыскивать весь вектор переменных состояния объекта, а использовать только измеряемые значения. Этот подход очень ценен в ситуации с ограниченной наблюдаемостью, особенно после технологических остановок.

Проведен анализ качественных показателей работы комплекса «система регулирования – модель объекта» при отработке возмущающих воздействий по различным каналам воздействий. Результаты анализа свидетельствуют об эффективности алгоритма настроек регуляторов.

ИССЛЕДОВАНИЕ ПОДХОДА К СЕГМЕНТАЦИИ ВОКАЛИЗОВАННЫХ УЧАСТКОВ РЕЧЕВОГО СИГНАЛА

Н.А. Тесленко, студент 5-го курса, каф. КИБЭВС
г. Томск, ТУСУР, ФВС, venik6000@gmail.com

При построении систем распознавания слитной речи с неограниченным словарем важное значение принимает качественная предварительная обработка сигнала. Звуки могут быть образованы как при помощи только голосового (гласные, сонанты) или шумового (глухие согласные) источника, так и с использованием обоих типов источников (звонкие согласные). Очевидно, что точность выделения таких параметров, как частота основного тона, интенсивность гармоник, динамика их изменения и т.д., непосредственно зависит от данного этапа обработки речевого сигнала. Использование модели обработки речевого сигнала на периферической части слуховой системы человека является одним из наиболее перспективных методов предварительной обработки. Звуки могут быть образованы как при помощи только голосового (гласные, сонанты) или шумового (глухие согласные) источника, так и с использованием обоих типов источников (звонкие согласные) [1].

Основываясь на формантной структуре ударных гласных, можно предположить, что в области формантных частот должны находиться максимальные по интенсивности гармоники сигнала. Тогда в параметрическое описание должны быть включены максимальные по интенсивности гармоники. При этом их поиск должен проводиться в областях первой и второй формант. Граница разбиения всей анализируемой частотной области на области первой и второй формант расположена около 800 Гц. В каждой из полученных частотных областей были выбраны по две гармоники с максимальной интенсивностью [2].

Рассмотрим динамику изменения гармоник на примере вручную отсегментированного речевого сигнала диктора. Сигнал содержит слитную речь диктора мужского пола. Фраза: «В это время перед объявлением остановился рослый, широкоплечий человек, без шапки, по одежде солдат, в рубахе без пояса, в обмотках» и «Скайлс, тоже теперь прищурясь, оглянул солдата, вспыхнул гневно, и пошёл по направлению к Неве, – шагал уверенно, и широко».

Для простоты частоту максимальной по интенсивности гармоники, лежащей в области частот до 800 Гц, назовём «1.1», на рис. 1 она светло-серого цвета. Частоту второй по интенсивности гармоники, лежащей в области частот до 800 Гц, назовём «1.2», на рисунке она чёрного цвета. Частоту максимальной по интенсивности гармоники, лежащей в области частот от 800 до 2300 Гц, назовём «2.1», на рисунке она светло-серого цвета. Частоту второй по интенсивности гармоники,

лежащей в области частот от 800 до 2400 Гц, назовём «2.2», на рисунке она чёрного цвета.

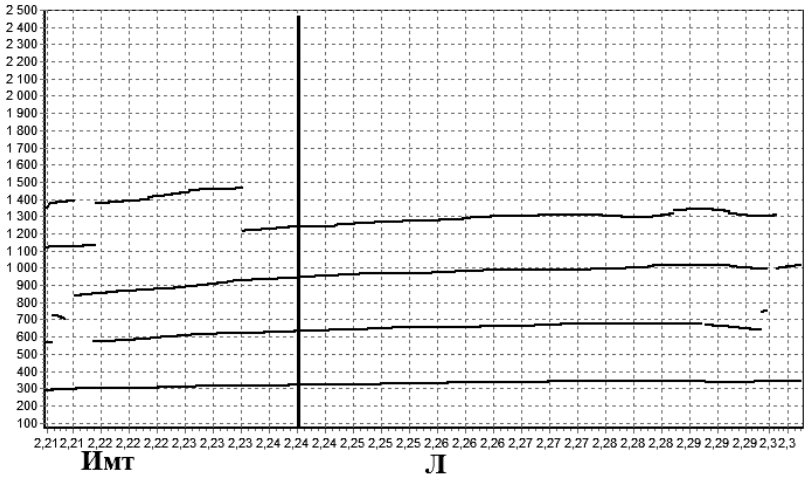


Рис. 1. Сегмент «ил» из слова «остановился» диктор – женщина

Из рис. 1 видно, как при переходе от звука «и» к звуку «л» 2.1 резко изменяет своё положение с 900 до 1200 Гц.

На рис. 2 при переходе от звука «и» к звуку «у» 2.2 изменяет своё положение с 1300 до 1100 Гц, а при переходе от звука «у» к звуку «л» 2.2 из ровной линии превращается в неравномерно распределённое множество точек и отрезков.

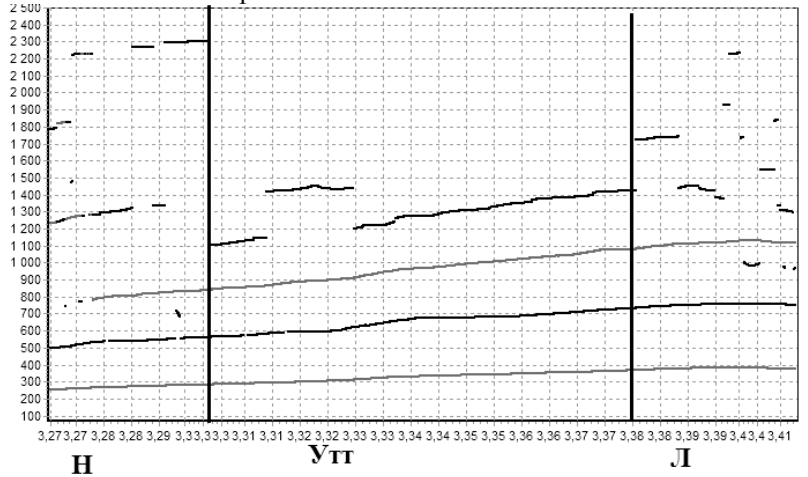


Рис. 2. Сегмент «нул» из слова «оглянул» диктор – женщина

ЛИТЕРАТУРА

1. *Конев А.А., Мещеряков Р.В., Тиунов С.Д. и др.* Параметрическое описание ударных гласных звуков // Сб. тр. XXII сессии Российского акустического общества. Т. III. М.: ГЕОС, 2010. С. 41–45.

2. *Конев А.А., Мещеряков Р.В.* Оценка вокализованных участков речевого сигнала // Тр. Второго междисциплинарного семинара «Анализ разговорной русской речи» (АРЗ–2008). СПб.: ГУАП, 2008. С. 59–65.

КОМПЬЮТЕРНЫЙ ОСЦИЛЛОГРАФ

Д.А. Вольф, Д.В. Березин, студенты каф. КИБЭВС

Научный руководитель Е.Д. Головин, зам. директора филиала ТУСУРа в г. Сургуте, доцент, к.т.н.

г. Сургут, Филиал ТУСУР, runsolar@mail.ru

В рамках учебной программы по дисциплине «Общая электротехника и электроника» для студентов филиала ТУСУРа в городе Сургуте проводится лабораторный практикум с использованием учебного оборудования (далее – лабораторная установка), разработанного в СКБ «Импульс».

Каждая учебная установка снабжена встроенным генератором низких частот от 1 Гц до 1,7 кГц, максимальная амплитуда по напряжению 2 В, две формы сигнала: синус и меандр.

Для эффективного проведения данного лабораторного практикума на лабораторных установках на одно рабочее место требуется обязательное наличие измерительного прибора типа осциллографа.

Стоимость самого недорогого осциллографа составляет порядка десяти тысяч рублей, при этом технические характеристики во много раз превосходят минимальные требования лабораторных установок.

Проведенные исследования и анализ современной элементной базы позволяет собрать цифровой осциллограф при минимальных затратах, который удовлетворит необходимым требованиям лабораторных установок.

В соответствии с поставленными задачами предлагается бюджетный вариант компьютерного осциллографа в виде микроконтроллерного устройства, структурная схема которого изображена на рис. 1.

Осциллограф состоит из аппаратной и программной части. Аппаратная часть устройства состоит из АЦП, который производит выборки с частотой дискретизации 60 кГц, глубиной 8 бит и отправляет их в компьютер через интерфейс USB. Программная часть, реализованная на компьютере, обрабатывает данные и восстанавливает форму входного сигнала, а также содержит различные индикаторы и органы управления.

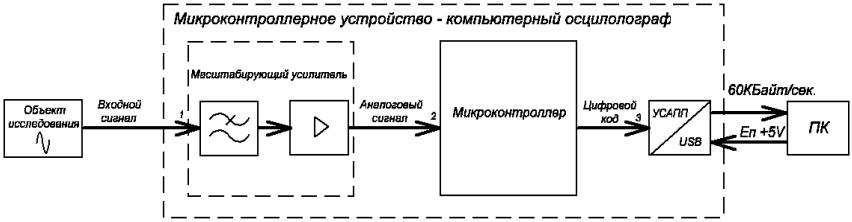


Рис. 1. Компьютерный осциллограф. Схема структурная

Питание устройства (рис. 1) и передача данных от устройства осуществляется с использованием интерфейса Universal Serial Bus (USB), реализуемый с помощью микросхемы DD2 (рис. 2) производства Future Technology Devices [1], которая представляет собой преобразователь из интерфейса USB в интерфейс последовательного порта.

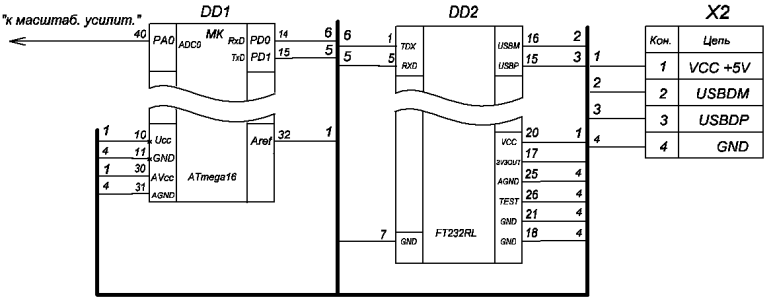


Рис. 2. Принципиальная схема блока преобразования и передачи информации

Аналогово-цифровое преобразование (АЦП) организовано микроконтроллером (МК) DD1, производства Atmel [2], со встроенным аналого-цифровым преобразователем последовательного приближения. Питание АЦП осуществляется от внешнего источника опорного напряжения шины USB.

Биполярный сигнал, подаваемый на вход АЦП МК, преобразуется в униполярный от нуля до пяти вольт с помощью масштабирующего усилителя (рис. 3), выполняющего функцию смещения биполярного сигнала в область положительного напряжения.

Емкость С1 дает шунтирующий эффект, образуя фильтр НЧ для защиты входного сигнала от ВЧ помех [3].

Масштабированный сигнал, поступающий на вход АЦП МК (вывод 40 МК) (см. рис. 2), оцифровывается и записывается в специальный регистр. Далее средствами УСАПП МК через USB преобразователь DD2 цифровой код передается по шине USB на ПК.

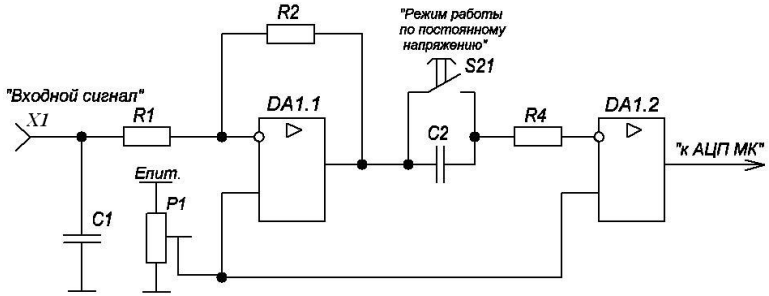


Рис. 3. Принципиальная схема масштабирующего усилителя

В результате создан эскизный вариант структурной и принципиальной электрической схемы, а также подготовлен предварительный перечень элементов для изготовления компьютерного осциллографа и как следствие предоставлен опытный образец (рис. 4).

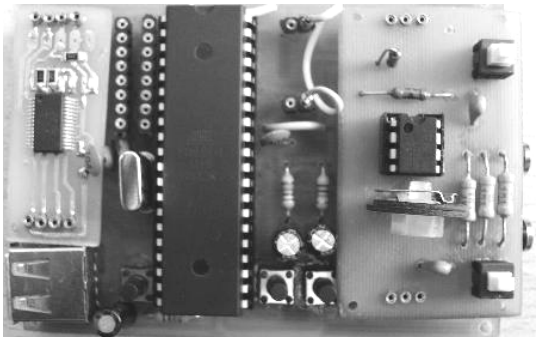


Рис. 4. Опытный образец компьютерного осциллографа

Настоящее измерительное устройство изготовлено с учетом доступности элементной базы и недорогой себестоимости (порядка 1500 рублей). Простота конструкции дает возможность репликации данного устройства студентами в качестве курсового проектирования с целью тиражирования устройства, а также освоения архитектуры и методов разработки микропроцессорных систем различного назначения. Устройство может стать основой дипломного проектирования студентов с целью модернизации и улучшения его тактико-технических характеристик.

Предложенное измерительное устройство можно применить в качестве недорогого измерительного прибора, способного удовлетворить всем технико-экономическим, эксплуатационным и учебно-методическим требованиям при проведении лабораторного практикума в филиале ТУСУРа в городе Сургуте.

ЛИТЕРАТУРА

1. FT232RL USB UART [сайт]. URL: http://www.ftdichip.com/
2. Atmega16 [сайт] URL: http://atmel.com/
3. *Синдеев Ю.Г., Грановский В.Г.* Радиоэлектроника: учеб. для студентов педагогических и технических вузов. Ростов н/Д: Феникс, 2000. 352 с.

ИССЛЕДОВАНИЕ СИСТЕМЫ ЧПУ ОБОРУДОВАНИЕМ С ПРИВОДОМ ПОСТОЯННОГО ТОКА И ДАТЧИКОМ ПОЛОЖЕНИЯ

А.А. Захаров, студент 5-го курса, П.Н. Коваленко, инженер, к.т.н., В.А. Бейнарович, проф., д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, sanyazahar1@sibmail.com

Автоматизация производства во всех отраслях промышленности выдвинула ряд проблем, связанных с улучшением качества управления агрегатами и технологическими объектами, основным видом регулируемого электропривода которых служит тиристорный электропривод (ТЭП) постоянного тока. Электрический привод является в современном производстве основным средством превращения электрической энергии в механическую и определяет технические возможности повышения эффективности труда и качества его результатов во всех сферах, связанных с реализацией механической энергии и точным воспроизведением требуемых движений [1]. Изучение электрических приводов производится на лабораторных работах по дисциплине «Системы автоматического управления».

На лабораторном стенде изучаются аппаратные и программные средства микропроцессорного устройства числового программного управления (УЧПУ), рассматриваются принципы действия электропривода постоянного тока, датчика положения, построения программного обеспечения реального времени, которое позволяет управлять следящим и регулируемым электроприводом.

В состав лабораторной установки входят:

– персональный компьютер IBM PC 486 с операционной системой MS-DOS;

– преобразователь привода постоянного тока;

– источник питания персонального компьютера;

– контроллер следящего привода (СП);

– электродвигатель постоянного тока с индуктивным датчиком положения.

Персональный компьютер осуществляет управление электроприводом через контроллер СП и преобразователь привода постоянного тока с

помощью специального программного обеспечения (СПО). Основными задачами СПО компьютера являются:

– приём с контроллера информации о действительном положении выходного вала электродвигателя;

– передача в контроллер информации по управлению приводами;

– обеспечение управления электроприводом в режиме реального времени жёсткого типа;

– реализация основных режимов работы, характерных для УЧПУ.

Преобразователь привода постоянного тока преобразует управляющее воздействие, поступающее с контроллера СП, в сигналы управления электродвигателем постоянного тока. Скорость вращения электродвигателя должна быть пропорциональной управляющему напряжению (±10 В). Контроль скорости вращения осуществляется за счёт обратной связи по скорости. Преобразователь имеет блочную конструкцию и предназначен для вертикального монтажа в металлическом шкафу.

Источником питания контроллера является блок питания персонального компьютера, который вырабатывает напряжения: +5 В, +12 В, –12 В.

Контроллер СП, который изображен на рис. 1, содержит микроконтроллер (МК), схему согласования интерфейса RS-232, цифроаналоговый преобразователь (ЦАП) и преобразователь сигналов индуктивного датчика.

Электродвигатель постоянного тока создает вращение, скорость которого прямо пропорциональна управляющему напряжению, поступающему с преобразователя привода. Направление вращения зависит от полярности управляющего напряжения. На одной оси с ротором электродвигателя установлен тахогенератор, напряжение с которого используется в преобразователе привода в качестве обратной связи по скорости.

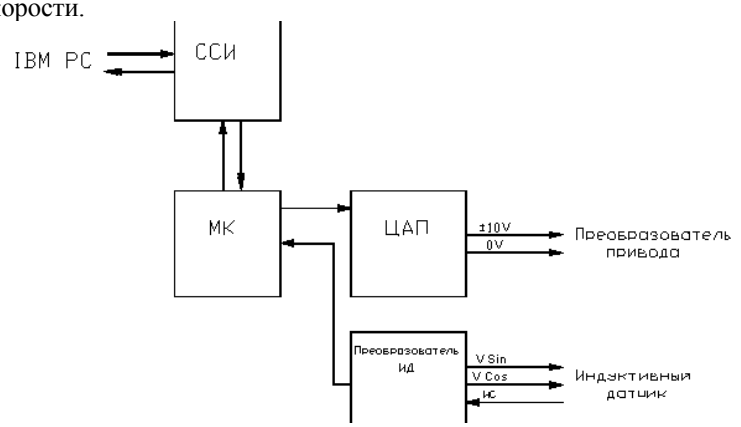


Рис. 1. Структурная схема контроллера СП

Таким образом, лабораторный стенд позволяет производить управление положением электродвигателя постоянного тока в режиме реального времени. Программное управление, реализованное на персональном компьютере, позволяет реализовать различные алгоритмы управления в виде последовательности команд, которые студент изучает в процесссе выполнения работы.

ЛИТЕРАТУРА

1. *Чернов Е.А., Кузьмин В.П.* Комплектные электроприводы станков с ЧПУ: справ. пособие. Горький: Волго-Вятское кн. изд-во, 1989. 320 с.

2. Руководство к лабораторным работам «Исследование системы ЧПУ оборудованием с приводом постоянного тока и датчиками положения». Томск, 2003. 40 с.

РАЗРАБОТКА БАЗЫ ДАННЫХ ДЛЯ МОДУЛЯ ВЗАИМОДЕЙСТВИЯ С МОБИЛЬНЫМ ПЕРСОНАЛОМ

К.М. Жернаков, студент 4-го курса, М.И. Мельников, аспирант

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, kzhernakov@sibmail.com

Одной из основных частей модуля взаимодействия является база данных, предоставляющая всю необходимую информацию для организации оперативной работы модуля. Такая БД должна содержать в себе информацию о координатах места положения обслуживающего персонала и обслуживаемых объектов; о состоянии бригады персонала на данный момент, где под состоянием понимается наличие или отсутствие возможности выехать на вызов, т.е. «свободен/занят»; о способах связи с бригадами; о составе бригад; об обслуживаемых объектах; о типе возникшей неполадки; а также прочую информацию, необходимую в большей степени для создания отчетности, такую как список возникших неполадок, список вызовов, личные данные рабочих и т.д. Обмен данными между базой данных и модулем взаимодействия осуществляется в режиме реального времени. Схема БД приведена на рис. 1.

Кроме того, для организации взаимодействия между обслуживающим персоналом и объектами обслуживания необходим алгоритм, в соответствии с которым производился бы выбор бригады для отправки к объекту, давшему сбой. Такой алгоритм заключается в вычислении расстояний от сбойного объекта до каждой свободной бригады и выборе наименьшего. Причем возможны два варианта привязки к географическим координатам. В первом случае используется глобальная система навигации и позиционирования GPS.

Рис. 1. Схема базы данных

Во втором – условное разбиение обслуживаемой зоны на сектора координатной сеткой. В обоих вариантах координаты объектов обслуживания заранее известны и остаются неизменными, а координаты бригад вычисляются или назначаются с некоторой периодичностью.

Обращение к БД осуществляется посредством SQL-запросов, которые могут формироваться автоматически или оператором. Например, при получении кода вышедшего из строя объекта и кода неисправности программа выполнит поиск бригады, находящейся на наименьшем удалении от неисправного объекта, сформирует сообщение, содержащее адрес, описания объекта и неисправности, и отправит его выбранной бригаде по одному из каналов связи. Все эти действия сопровождаются созданием соответствующих записей в списках возникших неполадок и вызовов.

Данная база данных создавалась на сервере Microsoft SQL Server 2000 Desktop Engine (MSDE 2000), выбор которого обусловлен его простотой, доступностью, а также высокой скоростью ответа на короткие SQL-запросы. Сама БД создавалась с помощью SQL Server Management Studio Express.

Алгоритм выбора бригады реализован в приложении, созданном посредством среды разработки Microsoft Visual Studio 2008. Алгоритм позволяет определить ближайшую к месту аварии обслуживающую бригаду. Для этого сначала необходимо выявить свободные бригады.

С данной целью создаются два массива: один содержит коды свободных бригад, а второй – их координаты. Далее вычисляются расстояния от сбойного объекта до каждой свободной бригады путем извлечения корня из суммы квадратов расстояний по оси X и по оси Y, т.е. определяется гипотенуза прямоугольного треугольника. Все результаты образуют третий массив – массив расстояний. Члены этого массива сравниваются между собой и определяется наименьшее расстояние. По соответствующему индексу определяется код бригады, находящейся на наименьшем расстоянии от неисправного объекта, и ей высылается сообщение определенного содержания. После ответа бригады на вызов в базе данных ее состояние меняется на «занят» до тех пор, пока она не сообщит о завершении работ. Эти действия фиксируются в базе данных путем занесения в список вызовов времени отправки сообщения, времени получения ответа и времени окончания работы.

Кроме того, данное приложение позволяет осуществлять необходимые для корректной работы модуля операции с базой данных, такие как добавление, редактирование, удаление данных и т.д.

ЛИТЕРАТУРА

1. *Мельников М.И.* Разработка автоматизированной системы управления распределённым лифтовым хозяйством на базе беспроводных технологий // Доклады ТУСУРа.Томск: ТУСУР, 2009. № 1(19), ч. 2. С. 81.

2. *Кирнос В.Н.* Основы программирования на языке С++: учеб. пособие. 2-е изд., перераб. и доп. Томск: В-Спектр, 2007. 130 с.

3. *Давыдова Е.М. Новгородова Н.А.* Базы данных: учеб. пособие. 2-е изд. перер. и доп. Томск: В-Спектр, 2007. 127 с.

ИДЕНТИФИКАЦИЯ ВОДИТЕЛЯ АВТОМОБИЛЯ ПО СТАТИСТИЧЕСКИМ ДАННЫМ ПЕРЕДВИЖЕНИЯ

В.С. Жилкин, студент, каф. ПрЭ

Научный руководитель Д.Д. Зыков, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, serbies@mail.ru

Данную работу можно отнести к программно – аппаратным системам поддержки принятия решений (СППР) слабоструктурированных ситуаций. К ним относятся системы интеллектуального анализа данных (Data Mining), которые позволяют выявить закономерности изменения; экспертные системы, которые основываются на использовании знаний экспертов; системы компьютерного имитационного моделирования; системы выбора решений. Принципы и методы построения СППР для слабоструктурированных ситуаций в административной и социально-политической сферах рассмотрены в литературе [1].

Существует множество алгоритмов идентификации людей по походке [2], однако такая область, как противоугонные сигнализации автомобилей, до сих пор развито слабо. И способы защиты, наращиваемые их (противоугонных сигнализаций) производителями, – лишь применение новых устройств без усовершенствования технологий обнаружения.

В рамках проекта производится работа по двум направлениям: создание противоугонного устройства и алгоритма идентификации водителя автомобиля по способу вождения. По мнению автора, именно алгоритм является наиболее значимым и актуальным аспектом данного проекта. Поэтому в рамках данной статьи будет рассмотрен только он (алгоритм) и по мере необходимости будет употребляться устройство.

Предлагаемый способ обнаружения угона основан на том предположении, что способ вождения автомобиля являются уникальным, как и походка человека, только идентификация происходит по другим данным, таким как скорость, направление, расположение (координаты x, y, z).

Рассмотрим в общем виде способ работы алгоритма. Входные данные поступают с GPS (координаты, время, скорость передвижения). На основании полученных данных происходит формирование первичных знаний о передвижении конкретного водителя автомобиля и при их (данных) увеличении становится возможным производить статистический анализ с целью выявления общих закономерностей передвижения наблюдаемого объекта.

Если рассматривать данный способ с точки зрения Data Mining, то от устройства постоянно поступает информация, на ее основе происходит выработка знаний, а на основании знаний можно провести кластеризацию. Но кластеризация, скорее всего не будет соответствовать всем критериям этого определения, так как процесс вождения применительно определения угона не является процессом дискретным, а наоборот, является непрерывным (интегральным) и постоянным. Поэтому кластеры часто будут обладать значительным сходством.

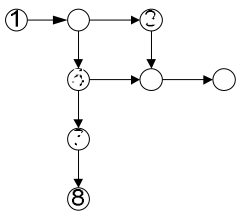


Рис. 1. Граф передвижения автомобиля

Кластеры в последующем следует представить, как вершины графа и использовать уже расстояния между вершинами как дополнительный параметр определения угона.

На рис. 1 изображен, простой пример такого графа, где расстояние между вершинами пропорционально реальному расстоянию. Допустим, водитель всегда производил поездку от вершины номер 1 к вершине номер 6 по маршруту 1–2–3–5–6. Если будет

произведена поездка от вершины 2 в направлении вершины 4, то система не будет рассматривать данный случай как угон. Однако если будет произведено движение дальше в направлении вершин 7 и 8, то данный маршрут следования системой будет рассматриваться как попытка угона.

Приведем необходимые примеры для конкретизации работы алгоритма.

Рассматривать передвижение автомобиля без учета времени было бы непредусмотрительным. Если водитель никогда не ездил в ночное время и вдруг начинает передвижение, то это может рассматриваться как попытка угона.

Следует учитывать такой параметр, как частота передвижения наблюдаемого объекта по маршрутам, а в частности частота переходов между отдельными вершинами графа. Это позволит системе производить дополнительную проверку как в приведенном примере, рассмотренном выше, так как движение в «нестандартное» время может быть и не угоном, а частным случаем в передвижении водителя.

В настоящее время производится доработка алгоритма идентификации и создание самого противоугонного устройства для проведения экспериментальных исследований, в ходе которых будет проведена оценка алгоритма идентификации алгоритма и произведены необходимые доработки как программной, так и аппаратной части системы.

ЛИТЕРАТУРА

1. *Кулинич А.А.* Система моделирования плохо определенных нестационарных ситуаций // Тр. 2-й Междунар. конф. «Когнитивный анализ и управление развитием ситуации». 4–6 ноября. М.: РШУ РАН, 2002. С. 44–50.

2. Информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных – www.machinelearning.ru/ (дата обращения: 6.03.2011).

3. *Воронцов К.В.* Алгоритмы кластеризации и многомерного шкалирования: курс лекций. М.: МГУ, 2007.

4. Статьи «Защита от угона автомобиля» http://www.ladyauto.ru/index.php?mod=246 (дата обращения: 6.03.2011).

РАЗРАБОТКА И РЕАЛИЗАЦИЯ ПРОТОКОЛА ПЕРЕДАЧИ ПАРАМЕТРОВ МЕЖДУ УЗЛАМИ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ АУДИОВИДЕОНАБЛЮДЕНИЯ

А.И. Балашов, студент

г. Томск ТУСУР, каф. КИБЭВС, mailto:balashov.artem@gmail.com

Последние события в мире еще раз напомнили всему человечеству, что вопросам безопасности нужно уделять гораздо больше внимания, чем уделяется в настоящее время. Спектр охранного оборудования, обеспечивающего безопасность людей, достаточно широк и включает в себя пожарную сигнализацию, системы контроля доступа и т.д. Но наиболее активным, а соответственно, и важным звеном в комплексной системе безопасности являются непосредственно системы видеонаблюдения. Они – это «око» комплекса системы безопасности, и, как следствие, качество изображения, полученное через это «око», имеет основополагающее значение.

Главное преимущество электронных систем охраны – круглосуточный мониторинг и запись событий. В случае возникновения ЧП оператор охранных систем может прокрутить запись событий назад и получить полную информацию по конкретному ЧП. В этих случаях руководителям предприятий рекомендуется отнестись к системе охранного видеонаблюдения более серьезно, так как недостаточное вложение денежных средств и экономия их приведет к тому, что система будет не закончена и иметь «дыры».

Возможности систем видеонаблюдения, которые еще вчера казались фантастическими, сегодня совершенно объективная реальность, а порой даже необходимость. Уже давно грамотно построенная масштабируемая система оказывает руководителям существенную помощь в организации производственного процесса. Интегрированные системы видеонаблюдения способны объединить в едином аппаратном программном комплексе целый ряд подсистем: качественная, профессиональная видеоподсистема, аудиоподсистема, подсистема охранно-пожарной сигнализации и контроля доступом (в том числе с модулями фотоидентификации, «учета рабочего времени», «службы пропускного режима»).

Наиболее актуальные системы видеонаблюдения можно условно разделить на три группы:

- Системы видеонаблюдения с возможностью дальнейшего наращивания, обладающие различными функциями оповещения. Возможность расширения системы без «переплаты». Речь идет о модернизации аппаратного комплекса. Как правило, крупные игроки готовы инвестировать средства в систему безопасности. И чем крупнее объект,

естественно, тем крупнее «система», следовательно, это определенные капиталовложения.

• Территориально удаленные, но в единой системе безопасности.

• Масштабные интегрированные системы видеонаблюдения. Наиболее востребованные сегодня подсистемы видеонаблюдения, системы контроля управления доступом, охранно-пожар-ной сигнализации.

Цель работы – написание протокола передачи параметров между узлами распределенной системы аудиовидеонаблюдения.

При работе над протоколом необходимо решить следующие задачи:

• разработать протокол обмена параметрами между узлами распределенной системы аудиовидеонаблюдения;

• реализовать протокол обмена параметрами, написав сервер и клиент;

• максимально минимизировать объемы полезной информации передаваемой в процессе работы системы.

В дальнейшем будет разработаны модули, реализующие протокол обмена параметрами.

ОСОБЕННОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ ГОЛОСОВОЙ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ СЕТЕЙ ETHERNET СТАНДАРТА IEEE 802.3

С.П. Берляков, студент 5-го курса ФВС

г. Томск, ТУСУР, Ishamael@Sibmail.com

С развитием сетей Ethernet и ростом их протяженности в коммуникационной среде возникла идея их использования для обеспечения голосовой связи (телефонии). В настоящее время появились устройства, позволяющие передавать телефонный канал в цифровом виде по Ethernet. Эти устройства используются для построения систем голосовой связи разной сложности, которые, в том числе, могут составить конкуренцию существующим распространенным стандартам: телефонной сети POTS (Plain Old Telephone Service) и GSM (сотовая связь).

Данная исследовательская работа стала результатом разработки системы передачи канала ТЧ по сети Ethernet на основе протокола UDP. Предлагаемые рынком устройства являются законченными устройствами с широким функционалом и вследствие этого имеют существенную стоимость. Потребность в интеграции средств голосовой связи в разные многофункциональные системы определила необходимость уйти от готовых изделий в сторону частных решений. Разраба-

тываемая система строится на встраиваемых модулях. Появление в настоящее время на рынке недорогих 32-битных микроконтроллеров с поддержкой основных Ethernet протоколов позволило проектировать недорогие модули для передачи телефонного канала в среде Ethernet.

В зависимости от требуемой функциональности и надежности линии связи возможности ее включения в сеть Internet или использования в локальной Ethernet сети IP телефония может быть реализована с применением сложного и недешевого VoIP (Voice over IP) протокола или с помощью собственного протокола, отвечающего конкретным требованиям. В работе рассмотрены минимальные функции, требуемые от управляющего контроллера для реализации телефонной связи в Ethernet сети, и основные проблемы, которые возникают при проектировании такой системы.

Самым распространенным решеним для данных систем является VoIP-телефония, которую можно считать эталоном в этой области. VoIP подразумевает поддержку протокола установления сеанса SIP. VoIP содержит в себе специальные функции телефонии, такие как конференция, переадресация звонка, определение номера, дополнительные телефонные опции. Сейчас на рынке телефонных аппаратов представлены различные модели VoIP телефонов.

Несмотря на то, что VoIP является стандартом передачи голосового трафика по Ethernet и имеет много перспектив для развития в связи с ростом Internet-сети, для организации телефонной связи посредством канала Ethernet могут быть применены другие Ethernet протоколы, которые широко поддерживаются огромным количеством менее дорогой аппаратуры (например, TCP IP и UDP). Данная работа рассматривает главным образом особенности реализации менее сложных и узкоспециализированных встроенных систем, с которыми могут иметь дело разработчики цифровой аппаратуры широкого профиля, не являющиеся специалистами по VoIP.

Минимальный набор функций, необходимый для связи АТС – окончание – Ethernet – Абонент, – это обработка снятия трубки, набор номера, вызов, сеанс дуплексной связи в реальном времени, окончание связи, выдача сигнала о недоступности абонента. Разработчик должен закладывать такие функции еще на начальных этапах проектирования, чтобы правильно выбрать аппаратные ресурсы, так как многие из таких функций могут оказаться очень требовательными к памяти и вычислительному ресурсу процессора. На этом этапе очень важным является выбор вокодера и способа кодирования голосового потока: способы его реализации, разрядность АЦП и конечная скорость цифрового аудиопотока. Особое внимание должно быть уделено тому, чтобы система работала в реальном времени. От выбора ресурсов в конечном

счете будут зависеть стоимость конечного изделия и целесообразность использования собственного решения для организации голосовой связи.

Основными проблемами для реализации телефонной связи являются задержки в канале Ethernet, вызванные несовершенством сетевого оборудования и линий передачи. В работе рассмотрены основные программные методы борьбы с задержками для сохранения целостности передаваемых данных и непрерывности сеанса связи. К перебоям связи может привести также такое распространенное явление, как смена очередности следования пакетов в Ethernet-канале. В задачу разработчика входит способ программной обработки таких ситуаций.

В зависимости от используемой сети (локальная, разветвленная локальная, глобальная) следует решать задачи маршрутизации, оптимизации путей доставки сообщений. В некоторых случаях маршрутизация звонка может достичь ощутимого времени, если абоненты находятся в очень удаленных друг от друга сетях. Если область применения ограничивается локальной сетью первого ранга, то достаточно организовать прямое соединение. Наращивание алгоритмов маршрутизации для работы в разветвленных сетях требует дополнительных ресурсов контроллера, их применение определяется требованиями, поставленными к системе и используемыми аппаратными средствами.

ЛИТЕРАТУРА

1. *Агуров П.В.* Последовательные интерфейсы ПК. Практика программирования. СПб.: БХВ-Петербург, 2004. 496 с.

2. *Гук М.* Аппаратные интерфейсы ПК. Энциклопедия. СПб.: Питер, 2002. 528 с.

3. *Семенов Ю.А.* Telecommunication technologies = Телекоммуникационные технологии [Электронный ресурс]. (ГНЦ ИТЭФ). Электрон. дан. Режим доступа: http://book.itep.ru/, свободный. Загл. с экрана.

УСТРОЙСТВО ОЗВУЧИВАНИЯ СИМВОЛОВ АЛФАВИТА

И.Н. Глибчук, студент 5-го курса

Научный руководитель Л.А.Торгонский, доцент, к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, inglibchuk@gmail.com

Устройство предназначено для обучения шрифту Брайля слепых и слабовидящих людей в форме озвучивания символов. Обучение проходит в форме познания: пользователь нажимает на клавишу, на поверхности которой произведено тиснение шрифтом Брайля, а устрой-

ство озвучивает символ, изображенный на кнопке. Закрепление материала планируется в обратной форме: программа воспроизводит символ, а проверяемому человеку требуется нажать соответствующую клавишу. При правильном или неправильном ответе устройство должно сообщить об этом.

Устройство является простым по современным меркам уровня техники, однако практическое применение устройства ускорит процесс социализации [1] и улучшит качество обучения целевой аудитории.

Устройство, структурная схема которого приведена на рис. 1, содержит модуль упорядоченно расположенных на лицевой панели клавиш с символами рельефного шрифта Брайля и специальными символами управления, модуль излучателя звукового сигнала и микроконтроллер, для которого, в отсутствие достаточной встроенной памяти, может потребоваться модуль внешней памяти для хранения звуковых образов символов алфавита. Нажатие на клавишу с опознаваемым в обучении символом сопровождается активизацией состояния бинарного датчика, связанного с клавишей. Микроконтроллер в составе приведенной структуры устройства предназначен для управления опросом, опознания активизированных датчиков модуля клавиш и управления операциями отработки со звуковым сопровождением.

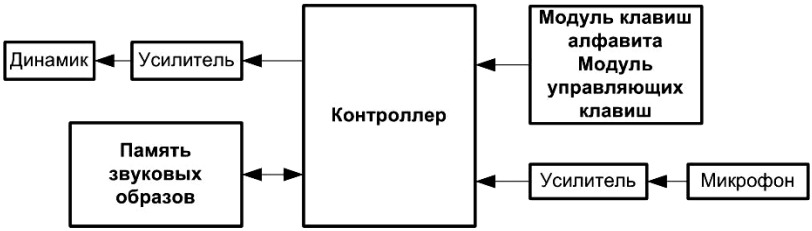


Рис. 1. Структурная схема устройства

Сигнал звукового образа генерируется цифроаналоговым преобразователем контроллера и подается на буферный усилитель. Сигнал поступает на воспроизводящее устройство – динамики наушников (гарнитуры). Использование гарнитуры наушников удобно для пользователя и снижает потребляемую мощность от батарей.

Для пользователя предпочтительно мобильное исполнение устройства, т.к. дает возможность использовать прибор в любое время и любом месте. Это исполнение обязывает применить встроенное электропитание от батарей, что налагает на конструкцию требование возможности их замены. На рис. 2 изображена компоновочная схема прибора.

Для прослушивания звуковых образов в устройстве предусмотрен разъем для подключения гарнитуры. Гнездо расположено на боковой поверхности (дальняя сторона рис. 2), а в корпусе предусмотрено специальное отверстие.

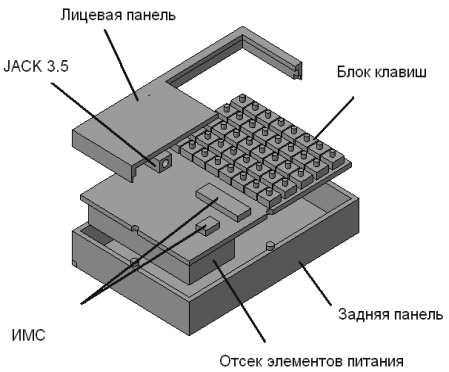


Рис. 2. Компоновочная схема устройства

На лицевой панели корпуса предусмотрено окно, предназначенное для расположения рабочей поверхности блока клавиш с алфавитом Брайля. Блок клавиш имеет сменные рабочие панели для смены алфавита языка. Работы по конструктивному исполнению панелей еще не закончены, и они на рис. 2 не представлены, однако место для них предусматривается в конструкции корпуса.

Для обеспечения процессов записи и воспроизведения звуковых образов используются аналого-цифровой преобразователь (АЦП), цифроаналоговый преобразователь (ЦАП), микрофон, гарнитура (два динамика), усилитель. Преобразователи АЦП и ЦАП интегрированы на кристалл контроллера. Остальные технические стедства выполнены в виде конструктивных модулей и располагаются на плате. Для записи звуковых образов используются микрофон, усилитель и АЦП контроллера. Для воспроизведения используются ЦАП, буферный усилитель и гарнитура.

Хранение звуковых образов сопровождается затратами постоянной памяти данных и определяется частотой дискретизации звукового сигнала. Принято компромиссное решение, что звуковые образы формируются на основе равноинтервальной дискретизации реального звукового сигнала с числом отсчётов не более 4000 в секунду при числе уровней квантования не более 128 (с временем преобразования 8–10 мкс). Длительность записи для каждого звукового образа отсчитывается в 2 с.

Занимаемый объём памяти для каждого звукового образа определяется по формуле

$$Mem = M \times N \times L, \quad (1)$$

где M – количество занимаемой памяти для одного отсчета; N – количество отсчетов; L – длительность образа.

Таким образом, при $M = 1$ байт, $N = 4000$ отсчетов, $L = 2$ с образ занимает 8000 байт, которые можно округлить до 8 кбайт. Весь алфавит русского языка будет занимать 264 кбайт (33 буквы по 8 кбайт), английский – 208 кбайт (26 букв по 8 кбайт), весь набор цифр займет в памяти 80 кбайт (10 цифр по 8 кбайт). Суммарный объем требуемой памяти для звуковых образов – 552 кбайт, что составляет 54% от общего размера хранилища (общий объем хранилища 1 Мбайт).

Остальной объем памяти планируется заполнить предложениями «Прибор включен», «Приступим к проверке», «Ваша оценка «отлично» («хорошо», «удовлетворительно», «плохо»)», а также для других игровых возможностей данного прибора.

Прибор был заявлен на НС ТУСУР–2010. Он полезен для лиц с ограниченными возможностями зрения, а также для широкого круга, при доработке системы вывода звука и программного обеспечения, в виде различных обучающих звуковых игрушек.

ЛИТЕРАТУРА

1. *Швецов В.И., Рощина М.А.* Компьютерные тифлотехнологии в социальной интеграции лиц с глубокими нарушениями зрения: учеб. пособие. Нижний Новгород: Нижегородский государственный университет им. Н.И. Лобачевского, 2007. 154 с.

УСТРОЙСТВО ПОЗИЦИОНИРОВАНИЯ ИНСТРУМЕНТА ОБРАБОТКИ ПЛАТ

Т.Р. Муксунов, студент 5-го курса ФВС
T0Snake0MR@yandex.ru

Операции размерной обработки являются важной составляющей процесса производства печатных плат и других плоских изделий. Для осуществления этих операций необходимо устройство позиционирования рабочего инструмента, перемещающее его по координатам. Наиболее ответственными объектами таких устройств являются механические узлы транспортировки несущих поверхностей относительно друг друга. Комплекс взаимосвязанных механических транспортных узлов образует так называемый мехатронный комплекс. Разновидностью мехатронного комплекса является трехкоординатное транспортное устройство [1, 2]. Выбранное в качестве базового для позиционирования рабочего инструмента устройство приведено на рис. 1.

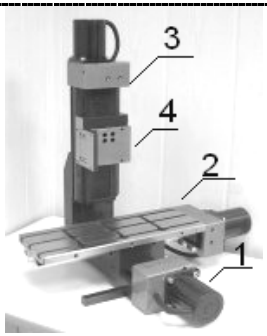


Рис. 1. Внешний вид транспортного устройства (ТУ)

На несущей колонке (*3*) устройства установлены платформы линейного перемещения по по ортогональным направлениям (например, монтажная каретка перемещения по координате *Y* вдоль колонки *3* и платформа *2* перемещения по координате *X* перпендикулярно колонке) и платформа *4* линейного перемещения по координате *Z* , перпендикулярно направлениям *X* и *Y*. Платформы приводятся в движение раздельно тремя двигателями, один из которых для перемещения по координате *Y* отмечен позицией *1*. На каретке расположен стол (платформа *2*) для закрепления обрабатываемой детали. На платформе *4* конструкцией устройства предусмотрена установка консоли с выбраным пользователем инструментом для обработки деталей (в том числе печатных плат). Таким образом, рабочий инструмент, закреплённый неподвижно на консоли, может перемещаться по трём координатам в шести направлениях относительно детали (платы), закреплённой неподвижно на платформе *2*. Устанавливая на консоли дополнительно управляемый рабочий инструмент (РИ), инструменту можно придавать дополнительные степени свободы. Рассматриваемое ТУ применено с двумя РИ, сменяемыми на консоли. Одним инструментом является сверловочная насадка со сменными свёрлами диаметром не более 3,5 мм. Другим обрабатывающим инструментом выбраны нагреваемые до температуры не более 250 °С стальные стержни диаметром не более 3 мм и разных профилей поперечного сечения.

Для управления двигателями, как правило, используют микроконтроллеры [3]. Контроллеры управляют питанием обмоток двигателей транспортного устройства, отвечающих за свои координаты транспорта, и, по необходимости, работой установленного на инструмента. Для этого контроллер принимает внешние данные, содержащие информацию о требуемом положении РИ, скорости и направлении движения по координатам, и вырабатывает сигналы управления питанием двигателей и рабочего инструмента. Выработку необходимых сигналов можно реализовать программно и с применением специальных функциональных блоков (аппаратных драйверов) управления двигателями. Аппаратные драйверы при управлении получают от контроллеров данные требуемого положения, взаимодействуют с датчиками положения и скорости вращения вала якоря, размещёнными на двигателях, определяют рассогласование координат положения. Реализуя принцип ПИД

регуляции (пропорционально-интегрально-дифференциальный алгоритм управления), аппаратные драйверы определяют направление и скорость вращения вала двигателя для компенсации рассогласования по положению. В состав аппаратных драйверов входят силовые ключи коммутации обмоток двигателей, усилители сигналов датчиков и ПИД-преобразователи. Для управления шаговыми двигателями (ШД), установленными на ТУ, удобно исполнить драйверы с программным управлением. Для этого микроконтроллеры дополнены силовыми ключами и цифровыми элементами согласования нагрузочных характеристик контроллера со входами ключей. Гибкое скоростное микропроцессорное управление силовыми ключами достигается применением отдельных контроллеров на каждом из трёх двигателей. Для планируемых задач обработки плат вполне приемлема поочерёдная отработка операций транспотра и управления инструментом. Поэтому принято решение об управлении тремя ШД одним контроллером. На платформах 2, 4 и монтажной каретке транспорта по коррдинате *Y* в крайних позициях размещены по два концевых датчика начального позиционирования РИ по координатам *X, Y, Z*. Один датчик исполнен на оптопаре и определяет базовую начальную точку позиционирования. Второй датчик контактного типа смещён на расстояние 5 мм и активизируется для аварийного отключения транспорта при «выбеге» за пределы допустимой зоны [4]. Питание двигателя для вращения сверла и нагревателя для термическго стержня предусмотрено от источника питания постянного тока на 24 В. Для управления ими предусмотрены раздельные силовые ключи с согласующими цифровыми элементами подобно ключам коммутации обмоток двигателей. Для термостержня предусмотрен контроль температуры с точностью не хуже ±5°С.

Транспортное устройство дооснащено электронным блоком управления, в котором размещены ключи коммутации обмоток трёх двигателей транспорта, двигателя вражения сверла, нагревателя термостержня с согласующими элементами и источник питания 24±5%. На отдельной плате смонтирована маломощная электроника микроконтроллера, со средствами подключения датчиков положения, контроля температур, кнопок ручного управления, светодиодных индикаторов обратной связи. Соединения блока управления узлами ТУ и РИ выполнены раъёмными. Органами ручного управления с электронного блока предусмотрены позиционирование инструмента в начальную точку, запуск диагностического теста с перемещением РИ, запуск управления с ЭВМ верхнего уровня, инициативный останов процесса управления. Для загрузки программы управления и ввода кадров координат предусмотрено кабельное разъёмное соединение с ПЭВМ верхнего уровня по протоколу USART. Управление осуществляется по-

средством связи с персональным компьютером через USART. Подготовлены и отлажены варианты программных драйверов для управления ШД, управления индикаторами, контроля температуры, контроля дискретных датчиков ТУ и датчиков ручного управления, поддержки ввода файла данных к обработке.

ЛИТЕРАТУРА

1. Координатный_стол http://ru.wikipedia.org/wiki/
2. http://reabin.ru/data/20-g1.html
3. *Емельянов А.В., Шилин А.Н.* Шаговые двигатели. М., 2005.
4. Микропроцессорное управление технологическим оборудованием микроэлектроники. М.: Радио и связь, 1988.

СИСТЕМА ИДЕНТИФИКАЦИИ ПОЛУПРОВОДНИКОВЫХ ПЛАСТИН

М.В. Червяков, студент 5-го курса, Д.Д. Зыков, доцент
г. Томск, ТУСУР, ФВС, каф. КИБЭВС,che-mv@mail.ru

При производстве полупроводниковой продукции от начала разработки до постановки в конечное устройство проводится огромное количество технологических операций. Управление всеми этапами производства в ручном режиме представляет собой очень сложную задачу. Для упрощения системы управления применяется автоматизация ведения документации и статистического учета, планирования, оперативного контроля и пр.

Введение автоматизированной системы позволяет:

− вести оперативный контроль технологического процесса производства;

− проводить анализ причин возникновения брака;

− уменьшить количество бумажных носителей;

− увеличить информативность о проведенных процессах;

− упростить учет расходных материалов;

− ввести автоматизированное планирование процессов производства.

Практически на всех предприятиях полупроводниковой продукции управление этапами производства происходит с помощью автоматизированных систем. Данные системы принято называть Product Lifecycle Management (PLM) – технология управления жизненным циклом изделий. Внедрение на предприятие готовой системы PLM – очень дорогостоящий и длительный процесс. Одной из трудностей для введения автоматизированной системы является чтение уникального кода пластин.

Для решения этой задачи необходимо в процесс производства ввести универсальные считывающие устройства для определения уникального цифробуквенного кода пластины. Было изучено предложение фирм, производящих такое оборудование, и проведен расчет стоимости для комплектации пятнадцати рабочих мест. Самый дешевый вариант составил порядка 45 тыс. евро, поэтому было принято решение рассмотреть возможность создания более доступной системы.

Считывающее устройство представляет собой оптическую камеру и вычислительное оборудование с программным обеспечением для распознавания символов [1]. Сложность выбора подходящей камеры обусловлена тем, что код представляет собой последовательность цифр и букв небольшого размера (размеры всего поля 5 на 20 мм), нанесенных лазерной маркировкой на зеркальную поверхность пластины. В связи с этим необходимо использовать камеру с короткофокусным объективом, избегая попадания в кадр бликов от освещения и других отраженных объектов. После тестирования нескольких камер удалось получить изображение кода с качеством, достаточным для последующего распознавания символов (рис. 1).

Рис. 1. Полученное изображение кода пластины

Тестирование распознающих текст программ показало, что применение обучаемых алгоритмов позволяет переводить изображение в последовательность кодов. В дальнейшем планируется продолжить разработку конструкции изделия для получения более дешевого варианта считывателя.

ЛИТЕРАТУРА

1. Официальный сайт компании Cognex. Режим доступа: http://www.cognex.com/ProductsServices/IndustrySpecificProducts/Wafer.aspx?id=116.

МЕТОДИКИ РАСЧЕТА РЕЙТИНГА

А.А. Шантаев, студент 5-го курса

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, saa-42@sibmail.com

Среди многих аспектов проблем качества высшего образования одной из ключевых является проблема мониторинга качества подго-

товки обучаемых. Одним из способов мониторинга является расчет рейтинговой оценки студентов. Ранжирование обучаемых по величине рейтинговой оценки позволяет отобрать студентов для дальнейшего обучения в аспирантуре, дать рекомендации при трудоустройстве студентов и выпускников.

Методики расчета рейтинга подразумевают использование в качестве входных данных сведений об успеваемости студентов, представленных в виде баллов по четырехбалльной шкале (для экзаменов, курсовых работ и дифференцированных зачетов), а также баллов по двухбалльной шкале (в случае простых зачетов).

Среди всего разнообразия применяемых методик можно выделить 2 группы методов, в зависимости от подхода, применяемого в обработке исходных данных:

1. Методы, основанные на арифметической обработке отметок по дисциплинам. Например, такие как сложение баллов и вычисление их среднего арифметического. Некорректность результатов такой обработки обусловлена природой оценочных баллов, представляющих собой отметки на порядковой шкале, поскольку баллы выражают качественную, но не количественную оценку знаний. Неприменимость арифметических операций при первичной обработке баллов подробно доказана в [1].

2. Методы, основанные на использовании уравнения регрессии. Суть их заключается в присвоении каждому из показателей (т.е. отметкам по каждой из дисциплин) определенного коэффициента значимости. Рейтинг по совокупности дисциплин определяется суммированием произведений оценочных баллов на соответствующие коэффициенты значимости. Методика расчета по уравнению регрессии является обоснованной с педагогической и квалиметрической точки зрения. Данная методика подробно описана и обоснована в публикациях В.С. Аванесова по теме «Теория и практика педагогических измерений» http://testolog.narod.ru/Theory45.html

Таким образом, возникает проблема корректного определения коэффициентов значимости дисциплин учебного плана. При ее решении следует учитывать следующие составляющие весомости дисциплины в учебном плане специальности:

1. Трудоемкость дисциплины (рассчитывается на основе количества часов, отведенных учебным планом для изучения дисциплины). Коэффициент значимости при этом рассчитывается путем деления количества учебных часов дисциплины на количество часов, отведенных для изучения самой трудоемкой дисциплины, с тем, чтобы все коэффициенты значимости принимали значение от 0 до 1.

2. Сложность дисциплины для освоения (определяется методом экспертных оценок, на основании результатов опроса студентов, при

этом оценки, данные студентами, обучающимися по одному учебному плану, справедливы для расчета рейтинга учащихся только этого контингента). Сложность дисциплины оценивается по шкале от 0 до 10 баллов. Для расчета коэффициента значимости используется метод согласования оценок, применение которого обосновано в публикации С.В. Терентьева http://emm.ostu.ru/lect/lect7.html. В рамках метода вычисляется медиана всех имеющихся оценок, коэффициент значимости при этом рассчитывается как отношение медианы оценок к максимальному баллу, доступному для оценки сложности (то есть 10), с тем, чтобы все коэффициенты значимости приняли значение от 0 до 1.

3. Важность дисциплины для формирования профессионально важных качеств будущего специалиста (определяется методом экспертных оценок на основании мнения преподавателей). Шкала оценивания при этом располагается от 0 до 10. Для расчета коэффициента значимости также применяется метод согласования оценок. Числовое значение коэффициента значимости получается путем деления медианы всех оценок данных экспертами на максимальное значение оценки важности дисциплины (то есть 10), для того чтобы численное значение каждого из коэффициентов укладывалось в интервале от 0 до 1.

В связи с разделением дисциплин учебного плана на группы рейтинг студентов рассчитывается в отдельности по каждой из следующих групп дисциплин:

– Общие гуманитарные и социально-экономические дисциплины.
– Общие математические и естественно-научные дисциплины.
– Общепрофессиональные дисциплины.
– Специальные дисциплины.

С учетом приведенных аргументов наиболее целесообразная методика ранжирования студентов по величине рейтинговой оценки предстает в следующем виде:

1. С помощью уравнений регрессии вычисляется рейтинг студентов по каждой из четырех групп дисциплин учебного плана.

2. На основе полученных значений рейтинга выстраиваются 4 ранжированных ряда студентов.

3. По минимальной сумме мест, занятых по группам дисциплин, строится итоговый упорядоченный ряд.

ЛИТЕРАТУРА

1. *Перегудов Ф.И., Тарасенко Ф.П.* Основы системного анализа: учеб. 3-е изд. Томск: Изд-во НТЛ, 2001. 396 с.

СЕКЦИЯ 14

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель секции – **Шелупанов А.А.**, проректор по НР ТУСУРа, зав. каф. КИБЭВС, д.т.н., проф.; зам. председателя – **Мещеряков Р.В.**, зам. начальника НУ ТУСУРа, доцент, зам. зав. каф. КИБЭВС по НР, к.т.н.*

АТТЕСТАЦИОННЫЙ И ЭКСПЛУАТАЦИОННЫЙ КОНТРОЛЬ

Р.Ф. Акчурин, Е.Н. Анищенко, В.А. Трошин, студенты 5-го курса
Научный руководитель А.П. Зайцев, проф., к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, nurka12@rambler.ru

Информация категорируется на общедоступную информацию и с ограниченным доступом (служебная тайна, государственная тайна и т.д.). Если на объекте информатизации обрабатывается информация с ограниченным доступом, то необходимо официальное подтверждение эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

Официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов по защите информации, называется аттестацией объекта информатизации [1].

Аттестация объектов проводится на соответствие требованиям СТР-К и РД ФСТЭК России. Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки конфиденциальной информации на период времени, установленный в этом «Аттестате соответствия» [2].

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров, а также для государственных учреждений, обрабатывающих конфиденциальную информацию, и организаций предоставляющих услуги по защите информации.

Комплекс специальных аттестационных мероприятий называется аттестационной проверкой и включает в себя контроль эффективности

защиты – проверку соответствия качественных и количественных показателей эффективности мер технической защиты установленным требованиям или нормам эффективности защиты информации.

Различают два вида контроля защищенности объектов:

– аттестационный контроль;

– эксплуатационный контроль.

Аттестационный контроль проводится при вводе объекта в эксплуатацию и после его реконструкции или модернизации, а эксплуатационный – в процессе эксплуатации объекта. Проведение эксплуатационного контроля является обязательным и проводится аттестующей организацией не реже одного раза в год после проведения аттестационного контроля и получения аттестата соответствия. Для проведения аттестационного и эксплуатационного контроля применяются одни и те же средства [3].

Виды контроля эффективности защиты делятся на:

– организационный контроль – проверка соответствия мероприятий по технической защите информации требованиям руководящих документов;

– технический контроль – контроль эффективности технической защиты информации, проводимый с использованием технических средств контроля.

По методике проведения и содержанию технический контроль эффективности технической защиты информации является наиболее сложным контролем и может быть:

– комплексным, когда проверяется возможная утечка информации по всем опасным каналам контролируемого объекта;

– целевым, когда проводится проверка по одному из интересующих каналов возможной утечки информации;

– выборочным, когда из всего состава технических средств на объекте проверяются только наиболее уязвимые с точки зрения утечки защищаемой информации.

Аттестационный контроль всегда является комплексным. При проведении эксплуатационного контроля на объекте допускается проведение работ выборочно относительно отдельных технических средств.

По результатам проведения аттестационного контроля формируются исходные данные для проведения эксплуатационного контроля защищенности от разведки, побочные электромагнитные излучения и наводки (ПЭМИН) технических средств автоматизированных систем управления (АСУ) и электронно-вычислительной техники (ЭВТ).

По результатам аттестационного контроля для данного объекта оформляется «Аттестат соответствия», наличие которого обязательно для проведения эксплуатационного контроля.

Таким образом, эксплуатационный контроль проводится ежегодно на протяжении срока действия «Аттестата соответствия», выданного при аттестационном контроле. «Аттестат соответствия» оформляется и выдается не более чем на 3 года после утверждения заключения по результатам аттестационных испытаний.

ЛИТЕРАТУРА

1. Российская Федерация. Положение по аттестации объектов информатизации по требованиям безопасности информации [утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.].

2. Аттестация в области защиты информации [Электронный ресурс]. Режим доступа: http://dehack.ru/lic_sert_att/att/

3. *Зайцев А.П., Шелупанов А.А.* Технические средства и методы защиты информации: учеб. пособие. Томск: В-Спектр, 2008. 228 с.

МУЛЬТИФРАКТАЛЬНЫЕ ПАРАМЕТРЫ РЕНТГЕНОВСКОГО ИЗОБРАЖЕНИЯ И РЕШЕНИЕ НЕКОТОРЫХ ЗАДАЧ ДИАГНОСТИКИ ЛЕГОЧНЫХ ЗАБОЛЕВАНИЙ СРЕДСТВАМИ И МЕТОДАМИ РЕНТГЕНОГРАФИИ. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ДИАГНОСТИЧЕСКИХ СИСТЕМ

А.В. Александров, студент магистратуры каф. СТИБ,
А.В. Кабакова, ст. преподаватель каф. ПиМКК, к.т.н.
Научный руководитель В.П. Иванников, зав. каф. СТИБ, проф., д.т.н.
г. Ижевск, ИжГТУ, sunanniv@mail.ru

Рентгеновское изображение характеризуется тем, что имеющиеся на нем возмущения (локальные значения интенсивности, связанные с заболеванием) невелики, но «усредненное» описание рассматриваемой физической системы (флюорограммы) достаточно хорошо отражает ее реальное поведение, и использование при анализе изображений детерминистических законов (причинно-следственных связей) вполне оправдано и поэтому широко используется в диагностике заболеваний. Вместе с тем на некоторых рентгеновских снимках локальные значения интенсивности, связанные с заболеванием, могут оказаться значительными, и, несмотря на детерминистский характер изменения состояния системы данные отклонения, которые применительно к аналоговому изображению интерпретировать как случайные (стохастические) невозможно, при преобразовании изображения в цифровую форму представления, с позиций статистического анализа, уже представляется возможным. Сложное непредсказуемое поведение физической

системы (называемое в дальнейшем стохастическим) в этом конкретном случае обусловлено «случайными» изменениями ее параметров (локальной интенсивностью под влиянием заболевания, характером протекания заболевания, развитием в организме человека разнообразных «неустойчивостей» под влиянием внешних воздействий – отсутствие или наличие лекарств, питания и т.п.). Все эти факторы, говоря физическим языком, приводят к развитию «в системе» так называемого детерминированного хаоса, т.е. к стохастизации сигналов и структур, характеризующих поведение и состояние системы. Для изучения же процессов стохастизации чаще всего привлекаются разнообразные вероятностные подходы.

В основе таких подходов лежат методы статистического анализа случайных величин и функций. Часто они сводятся к определению таких характеристик, как плотность распределения вероятностей, математическое ожидание, дисперсия, моменты высоких порядков, автокорреляционные функции, спектральные плотности. При проведении статистического анализа широко используются элементы математической статистики, включающие теорию выборок, оценки доверительных интервалов, проверку статистических гипотез, способы аппроксимации экспериментальных данных. Наряду с ними в последние годы получили распространение и некоторые менее известные способы обработки сигналов и структур, основанные, в частности, на фрактальном, мультифрактальном анализах и вейвлет-преобразованиях. Отличительная особенность этих способов состоит в том, что они наряду с глобальными характеристиками стохастических процессов (получающихся в результате использования процедуры усреднения по большим временным интервалам) позволяют вскрыть особенности их локальной структуры.

При преобразовании рентгеновского изображения в цифровую форму представления формируется модель марковского случайного процесса, так как вероятность того, что значение оптической плотности изображения в любой заданной точке $X(t_i)$ достигнет определенного значения при заданном $X(t_{i-1})$ ($t_{i-1} < t_i$), зависит только от t_{i-1} и t_i, а не от поведения $X(t)$ при $t < t_{i-1}$. Любой же сигнал $X(t)$ со стандартным отклонением σ, если его приращение $\Delta X = X(t_2) - X(t_1)$, $t_2 > t_1$, имеет гауссовское распределение [1], характеризуемое выражением

$$P(\Delta X < x) = \frac{1}{\sqrt{2\pi\sigma(t_2 - t_1)^H}} \cdot \int_{-\infty}^{x} \exp\left(-\frac{1}{2}\left(\frac{u}{\sigma(t_2 - t_1)^H} \right)^2 \right) du , \qquad (1)$$

а его дельта-дисперсия равна

$$E\left[(X(t_2)-X(t_1))^2\right]=\sigma^2\left|t_2-t_1\right|^{2H}. \qquad (2)$$

Входящий в (1) и (2) параметр H ($0<H<1$) называется параметром Херста. Если входящий в (1) параметр Херста $0 < H < 1$, то поверхность, характеризующая изменение величины X, представляет собой случайный фрактал. При этом фрактальная размерность $D_ф$ рассматриваемой поверхности, определенная методом ее покрытия сферами или кубами [2], связана с параметром Херста H соотношением

$$D_ф = 3 - H, \qquad (3)$$

Линии уровня фрактальных изображений (линии сканирования) также будут иметь фрактальную форму. Их размерность определяется выражением $D_ф = 2 - H$.

В основе большинства используемых на практике методов оценки фрактальной размерности изображений лежит соотношение (3). Входящий в (3) параметр Херста H может быть определен по аналогии с процедурой его определения при обработке сигналов, исходя из поведения дельта-дисперсии или структурной функции приращения исследуемой двумерной величины. С точки зрения исследования характера распределения оптической плотности на рентгеновском изображении будем использовать для исследуемой величины обозначение X. В трехмерном пространстве (x, y, X) распределение величины X будет формировать некую поверхность весьма сложной формы с многочисленными случайно расположенными, с точки зрения преобразования изображения в цифровую форму представления, впадинами и возвышенностями.

В работе [3] показано, что рентгеновское изображение может проявлять фрактальные свойства лишь в ограниченной области изменения оптической плотности. Ширина этой области (области скейлинга) является характеристикой степени фрактальности изображения. Если область скейлинга невелика (например, лишь в несколько раз превосходит элементарный шаг дискретизации), следует при анализе изображения указывать на слабость проявления фрактальных признаков. Пусть I – шаг квантования оптической плотности изображения. Тогда очевидно, что в бинарном представлении (m = 2) фрактальные признаки не проявляются; в полутоновом, например, с m = 8; проявляются слабо; с m = 24 – лучше, а с m = 255 – хорошо. Таким образом, чем выше качество преобразования рентгеновского изображения в цифровую форму представления, тем сильнее проявляются его фрактальные признаки.

При проведении медицинских диагностических исследований данные наблюдений, как правило, получают в виде временных рядов некоторых параметров или в виде фото- и видеоизображений и временных рядов фото- и видеоизображений, к которым применимы методы энтропийно-

фрактальной параметризации и идентификации. А временные ряды таких параметров позволяют решать задачи прогнозирования будущих состояний и влекут за собой необходимость проведения исследований и разработки безопасных средств, систем и комплексов по обеспечению информационной безопасности диагностирования заболеваний.

ЛИТЕРАТУРА

1. *Короленко П.В. и др.* Новационные методы анализа стохастических процессов и структур в оптике. Фрактальные и мультифрактальные методы, вейвлет-преобразования: учеб. пособие / П.В. Короленко, М.С. Маганова, А.В. Меснянкин. Моск. гос. у-т им. М.В. Ломоносова; Науч.-исслед. ин-т ядерной физики им. Д.В. Скобельцына. М., 2004. 82 с.

2. *Федер Е.* Фракталы. М.: Мир, 1991. 374 с.

3. *Иванников В.П.* Фрактальный анализ рентгенограмм / В.П. Иванников, В.В. Белых, Р.Т. Суфиянов, В.А. Степанов // Вестник ИжГТУ. 2009. №3. С. 150–154.

ПОТОКИ ПЕРСОНАЛЬНЫХ ДАННЫХ АБИТУРИЕНТОВ СУРГУТСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

И.В. Аютова, ассистент каф. радиоэлектроники

Научный руководитель В.А. Майстренко, проф. ОмГТУ, д.т.н.

г. Сургут, Сургутский государственный университет,

vishenka786@mail.ru

С 1 января 2007 г. вступил в силу Федеральный закон «О персональных данных». Цель этого закона – защита прав и свобод человека при обработке его персональных данных (ПДн), в том числе прав на неприкосновенность частной жизни, личную и семейную тайну [1].

ПДн – это важная и ценная информация о человеке, поэтому, заботясь о соблюдении прав своих граждан, государство требует от организаций и физических лиц обеспечить надежную защиту ПДн [2].

Проанализировав закон, становится понятно, что вузы являются операторами ПДн и на них распространяется действие закона. Основная проблема по обеспечению защиты ПДн в вузе – это значительное отличие процессов, ресурсов и характера информационных потоков, характерных для типовой компании.

Для того чтобы выполнить требования закона, оператору необходимо определить, какие ПДн обрабатываются в вузе и в каких структурных подразделениях ведется обработка. Рассмотрим потоки ПДн, циркулирующие в Сургутском государственном университете (СурГУ) при поступлении абитуриентов в вуз.

В соответствии с уставом в СурГУ реализуются различные по срокам и уровню подготовки специалистов образовательные программы высшего и среднего профессионального образования, послевузовского профессионального образования, программы дополнительного профессионального образования, программы профессиональной подготовки и переподготовки специалистов по очной, очно-заочной (вечерней), заочной формам, в форме экстерната [3].

Такое количество форм обучения приводит к созданию различных структурных подразделений университета, где для обеспечения образовательного процесса обрабатываются ПДн поступающих: учебно-методическое управление (УМУ), экстернат, отдел магистратуры, центр заочного образования, региональный методический центр дополнительного профессионального образования и т. д.

Рассмотрев перечень сведений, которые необходимы при поступлении в СурГУ [4], можно сделать вывод, что более 90 % этих документов относится к категории ПДн. Кроме того, медицинская справка относится к специальной категории ПД. В зависимости от выбранной формы обучения эти ПДн направляются в различные структуры СурГУ.

Также ПДн обрабатываются при оформлении договорных отношений. Так, в СурГУ в отделе доходов используются следующие бланки договоров: договор об обучении на факультете довузовской подготовки; договор об обучении студентов по заочной форме обучения; договор об обучении студентов по очной форме обучения; договор о предоставлении платных образовательных услуг.

При зачислении студента на бюджетную форму обучения ему назначается стипендия, для получения которой необходимо предоставить заявление по форме банка и предоставить копию паспорта. Кроме обычной стипендии, при особых достижениях в учебе или науке студенту полагается именная стипендия, для получения которой необходимо предоставить ПДн.

Студенты при определенных обстоятельствах имеют право на получение социальной стипендии и материальной помощи при предоставлении пакета документов. В этот пакет в зависимости от категории могут быть включены [5]:справка о признании граждан малоимущими; справка о доходах родителей; копии свидетельства о рождении (справка из ЗАГСа); копии свидетельства о расторжении брака. Все эти документы обрабатываются в отделе под руководством проректора по внеучебной и социальной работе.

Исходя из номенклатуры дел [6], в деканатах хранятся такие данные, как документы студентов (больничные листы, медсправки, заявления декану), информация по трудоустройству выпускников факультета, что по определению является ПДн.

Персональные данные постоянно циркулируют в университете. Согласно перечню документов, которые готовит деканат на студентов очной формы обучения (бакалавриат, специалитет, магистратура), сотрудники деканата передают в студенческий отдел кадров заполненные зачётные книжки, студенческие билеты, обходные листы, учебные и личные карточки, заверенные копии дипломов и приложений, акты передачи документов каждый год с сентября по ноябрь [7].

Вопрос обеспечения защиты ПДн в вузе не столь однозначен, как это кажется на первый взгляд. Нетиповая структура, открытость для посетителей, большой круг пользователей внутри вуза не позволяют однозначно формализовать процессы, протекающие в нем. Но требования закона необходимо выполнять, и первоочередная задача оператора – понять, какие ПДн обрабатываются в системе и с какими бизнес-процессами вуза связана обработка ПДн. В статье подробно проанализирован процесс обработки ПДн абитуриентов, поступающих в СурГУ. Выделены структурные единицы, где ведется обработка ПДн поступающих и обучающихся в СурГУ: УМУ, студенческий отдел кадров, экстернат, отдел магистратуры, центр заочного образования, региональный методический центр дополнительного профессионального образования, отдел доходов, отдел по внеучебной работе со студентами, материальная группа, деканаты, кафедры, библиотека.

Сбор разрешений на обработку ПДн и направления уведомления об обработке ПД – требования обязательные. Но наиболее важное требование закона – это защита ПДн, которое возможно при детальном предпроектном обследовании всех бизнес-процессов вуза, связанных с обработкой ПДн.

ЛИТЕРАТУРА

1. О персональных данных: Федеральный закон № 152-ФЗ, утвержден Президентом Российской Федерации 27 июля 2006 г. [Электронный ресурс]. Режим доступа: http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html, свободный.

2. *Шелупанов А.А.* Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // Доклады ТУСУР. 2010. № 1 (21). С. 14–22.

3. Устав СурГУ–III. Образовательная деятельность университета [Электронный ресурс]. Режим доступа: http://www.surgu.ru/index.php?view=menu&mid=109, свободный.

4. Перечень документов [Электронный ресурс]. Режим доступа: http://www.surgu.ru/index.php?view=s&sid=289, свободный.

5. Приказ на материальную помощь [Электронный ресурс]. Режим доступа: http://www.surgu.ru/index.php?view=menu&mid=173, свободный.

6. Номенклатура дел [Электронный ресурс]. Режим доступа: http://www.surgu.ru/index.php?view=menu&mid=294, свободный.
7. Перечень документов, которые готовит деканат на студентов очной формы обучения [Электронный ресурс]. Режим доступа: http://www.surgu.ru/index.php?view=menu&mid=174, свободный.

ПРОБЛЕМЫ ОПТИМИЗАЦИИ ЗАПРОСОВ В РЕЛЯЦИОННЫХ СУБД

А.С. Бирюков, В.Е. Долгушин, студенты
Научный руководитель М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, каф. КИБЭВС, birarser@gmail.com

Формулировка проблемы оптимизации SQL-запросов достаточно проста. Язык SQL декларативен. В формулировках SQL-запросов указывается, какими свойствами должны обладать данные, которые хочет получить пользователь, но ничего не говорится о том, как система должна реально выполнить запрос. Проблема в том, чтобы по декларативной формулировке запроса найти или построить программу (в мире SQL такую программу принято называть планом выполнения запроса), которая выполнялась бы максимально эффективно и выдавала бы результаты, соответствующие указанным в запросе свойствам. Так, основная трудность состоит в том, что необходимо точно построить всевозможные программы, результаты которых соответствовали бы желаемым свойствам, и найти в пространстве планов выполнения запроса такую программу, выполнение которой было бы наиболее оптимальным [3].

Подсистема выполнения запросов реализует набор физических операций. На вход каждой операции поступают один или несколько потоков данных, и на выходе формируется поток данных. Примерами физических операций являются сортировка (внешняя), последовательное сканирование, индексное сканирование, соединение методом вложенных циклов и соединение сортировкой и слиянием. Проще всего представлять физические операции как куски кода, которые используются в качестве строительных блоков для обеспечения возможности выполнения SQL-запросов. Абстрактным представлением такого выполнения является дерево физических операций, пример которого показан на рис. 1. Дуги в дереве операций представляют потоки данных между операциями. Так, используемые термины «дерево физических операций» и «план выполнения» (или просто план) имеют один и тот же смысл. Подсистема выполнения отвечает за выполнение плана, что приводит к формированию ответов на запросы. Следовательно, воз-

можности подсистемы выполнения запросов определяют структуру допустимых деревьев операций.

Предположим, что первая часть проблемы решена и имеется дерево физических операций, теперь нужно найти среди этого дерева только один вид запроса, который был бы самым эффективным при прочих равных условиях. Для этого необходим оптимизатор запросов. Оптимизатор запросов отвечает за генерацию ввода для подсистемы выполнения. Он принимает на входе представление SQL-запроса после грамматического разбора и отвечает за генерацию эффективного плана выполнения данного SQL-запроса, исходя из тех планов, которые составляют пространство возможных планов выполнения [1].

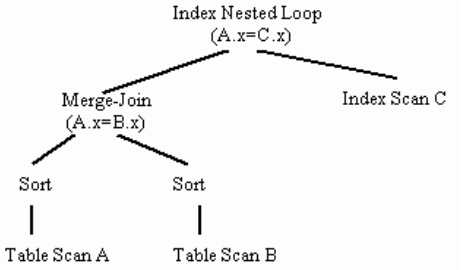


Рис. 1. Дерево операций

Задача оптимизатора нетривиальна, так как для заданного запроса может существовать большое число возможных деревьев операций (к примеру, алгебраическое представление данного запроса может быть преобразовано во многие другие логически эквивалентные алгебраические формы: Join(Join(A,B),C)=Join(Join(B,C),A)).

Кроме того, пропускная способность, или время ответа системы при выполнении этих планов, может весьма различаться. Поэтому здравый выбор плана выполнения, производимый оптимизатором, имеет критическое значение. Для выполнения этих задач требуется обеспечить:

1. Пространство планов (пространство поиска).
2. Метод оценки ресурсов, требуемых для выполнения плана.
3. Алгоритм перебора, который может осуществлять поиск в пространстве планов выполнения.

Так, желаемым оптимизатором является такой, в котором были бы реализованы следующие свойства:

1) пространство поиска включает планы с низкой стоимостью;

2) метод оценок является точным;

3) алгоритм перебора эффективен.

Реализация каждого из этих пунктов требует громадной работы. В области реализации оптимизатора наиболее примечателен подход System R, поскольку он питал многие последующие работы в области оптимизации. Пространство поиска оптимизатора System R в контек-

сте Select-Project-Join (SPJ)-запросов состоит из деревьев операций, которые соответствуют линейной последовательности операций соединения [2]. Стоимостная модель присваивает оценочную стоимость любому частичному или полному плану в пространстве поиска. Она также определяет оценочный размер потока данных для вывода каждой операции плана. Алгоритм перебора в оптимизаторе System R демонстрирует два важных метода: использование динамического программирования и использование интересных упорядочений.

Выполнено в рамках ГПО КИБЭВС-0902 – «Инженерия баз данных».

ЛИТЕРАТУРА

1. *Surajit Chaudhuri*. An Overview of Query Optimization in Relational Systems. http://research.microsoft.com/pubs/76059/pods98-tutorial.pdf

2. *Selinger P.G., Astrahan M.M., Chamberlin D.D., Lorie R.A., Price T.G.* Access Path Selection in a Relational Database System. In Reading in Database Systems. Morgan Kaufman.

3. *Кузнецов С.* Оптимизация запросов: вечнозеленая область; Открытые системы. #04/2003. http://citforum.ru/database/articles/sql_optimization.shtml

АВТОМАТИЗИРОВАННАЯ ОБУЧАЮЩАЯ СИСТЕМА ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ»

А.О. Битюцкая, студентка 5-го курса,
М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, bao_89@sibmail.ru

В настоящее время все больше разрабатываемых приложений используют базы данных в качестве основного хранилища, реализуя работу с данными через штатные или вспомогательные средства и функции СУБД. Разрабатываемая обучающая система (ОС) содержит методические материалы и указания по изучению СУБД Firebird 2.1 и MS Access 2007.

Основной задачей данного проекта является предоставление обучающемуся достаточной информации для освоения основных навыков при работе с указанными СУБД.

Структура системы представлена на рис. 1.

ОС по каждой СУБД состоит из двух основных разделов: теоретического и практического.

В теоретическом разделе обучающийся знакомится с основными функциями выбранной СУБД. Этот раздел позволяет быстро и доступно получить основную информацию по созданию баз данных и ее защите штатными средствами СУБД.

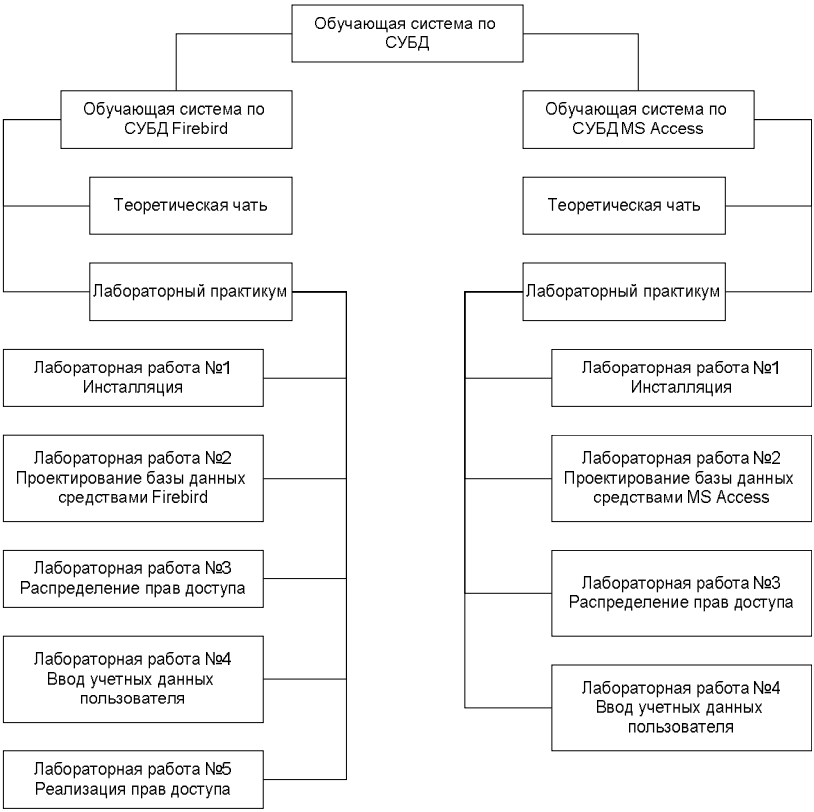


Рис. 1. Структура системы

Предполагается, что обучающийся знаком с основами проектирования баз данных и умеет анализировать предметную область и создавать реляционные модели данных, выполненные с условиями нормализации.

В разделе «Лабораторный практикум» обучающийся получает основные практические навыки реализации спроектированной базы данных в выбранной СУБД, выполняя лабораторные работы, в которых подробно и поэтапно расписаны все действия. Изучив этот раздел и выполнив все задания, пользователь сможет самостоятельно реализовать спроектированную базу данных и защитить ее средствами СУБД.

Для реализации оболочки обучающей системы был выбран язык разметки HTML.

Для работы с данной программой достаточно навыков работы с Web-документами. К достоинствам программы можно отнести челове-

ко-ориентированный интерфейс, полноту методического материала и доступное описание хода выполнения лабораторных работ.

ЛИТЕРАТУРА

1. *Хелен Борри Firebird.* Руководство разработчика баз данных. СПб.: БХВ-Петербург, 2006. 1104 с.

2. *Черемных С.В., Семенов И.О., Ручкин В.С.* Моделирование и анализ систем. IDEF-технологии: Практикум. М.: Финансы и кредит, 2005. 192 с.

3. *Давыдова Е.М., Новгородова Н.А.* Базы данных: учеб. пособие. Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2005. 127 с.

4. *Петюшкин А.В.* HTML. Экспресс-курс. СПб.: БХВ-Петербург, 2003. 256 с.

5. *Тимошок Т.В.* Microsoft Access 2003. Самоучитель. М.: Изд. дом «Вильямс», 2004. 464 с.

АНАЛИЗ УСТОЙЧИВОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ К НЕГАТИВНЫМ ВОЗДЕЙСТВИЯМ

И.В. Бондарь, аспирант, В.В. Золотарев, зам. директора ИИТК, к.т.н., А.М. Попов, директор ИИТК, д.ф.-м.н.

г. Красноярск, СибГАУ, ИИТК, firebug@yandex.ru, amida@land.ru

Возрастающая роль информационной сферы задает темпы развития информационной безопасности как научного направления, которому требуется охватывать все большие объемы информационного пространства, детальней исследовать его глубину, используя более структурированные и универсальные подходы.

Коммерческий спрос направляет ИБ на разработку технологий, более простых в использовании, применение которых не затруднит существующий ход информационных процессов, а затраты на сопровождение останутся в разумных пределах.

Единство заключается в разработке и исследовании противоположных моделей (системы защиты информации и противоборствующей системы угроз), взаимосвязанных в рамках общей модели информационной системы таким образом, что исследование любой угрозы, основанное на усилении ее области охвата/глубины/строгости, совпадает с вектором исследования соответствующего механизма защиты. Это позволяет сосредоточить усилия при решении различного рода частных задач в рамках единой руководящей идеи.

Структура ПСУ: угрозы, категории угроз, базис угроз, комбинации угроз.

Структура ИС: анклавы, активы, информация.

Структура СЗИ: цели защиты, категории требований защиты для анклава, требования поддержки среды, функциональные требования, требования доверия, временные требования.

Материалы для каждого компонента уже есть в существующих стандартах и проведенных на текущий момент исследованиях.

Этапами исследования ПСУ являются выбор базиса рисков, поиск функциональных зависимостей между угрозами и минимизация вероятностей реализации. При этом необходимо сочетать теоретические исследования, имитационное моделирование и обработку результатов наблюдений за работой реально действующей системы. Необходимые элементы математического аппарата: корреляционный анализ, регрессионный анализ, методика проверки статистических гипотез [2].

Базовая модель угроз строится на основе результатов анализа особенностей деятельности предприятия, технических характеристик сети и анализа мотивов и возможностей потенциальных нарушителей. В базовой модели угроз представлены все возможные наиболее актуальные угрозы.

Модель СЗИ представляет собой систему требований нормативных документов.

Модель устанавливает связь процессного (горизонтального) подхода с иерархической (вертикальной) моделью управления, что позволяет проводить оценку как по рекомендациям безопасности серии стандартов ISO 27000, поверхностно освещающих организационно-правовые меры в качестве элементов управления на верхних уровнях менеджмента, так и по строгим техническим требованиям профилей защиты стандарта ГОСТ ИСО/МЭК 15408 (рис. 1).

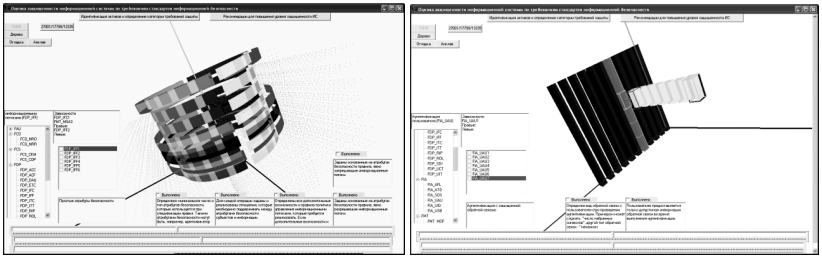


Рис. 1. Интерфейс программного средства «ОАЗИС»

На рисунке представлена качественная оценка соответствия требованиям нормативных документов.

Профили защиты на основе стандарта ГОСТ ИСО/МЭК 15408 содержат обоснование соответствий «угрозы → цели защиты → функциональные требования». Дано объяснение, как совокупность требо-

ваний полностью покрывает цели, и что каждая цель безопасности адресована одному или нескольким компонентам требований. Аргументы представлены для охвата каждой цели [1]. На основе невыполненных требований делается вывод о том, что определенные цели защиты не достигнуты, и, следовательно, высока вероятность реализации соответствующих угроз.

Возникновение угрозы способно перевести анклав в незащищенное состояние. Ценность анклава определяется пользователем на основании возможных последствий его незащищенного состояния. Произведением вероятности возникновения и оценки воздействия угрозы рассчитывается мера риска, позволяющая сравнить угрозы и выстроить по приоритетности.

В соответствии с данным приоритетом формируется перечень рекомендаций, а модель представления СЗИ отражает их влияние на картину в целом. Но таким образом оценивается полнота системы информационной безопасности только с технической точки зрения.

В профилях защиты на основе стандарта ГОСТ ИСО/МЭК 15408 представлены таблицы предположений, касающихся применения организационно-правовых и физических мер защиты, ожидаемых и необходимых для корректной оценки объекта. Требования стандартов ГОСТ ИСО/МЭК 17799, 27001, 13335 в отличие от 15408 обладают иными атрибутами области охвата, глубины и строгости, преимущественно освещают материал на верхних уровнях менеджмента. Выполнение/невыполнение этих требований влияет на значения показателей осуществляемости, которые определяют уровень соответствующей организационной поддержки техническим мерам защиты. Таким образом, стандарты взаимосвязаны.

Относительно цели, предположения, угрозы, актива требования защиты могут быть условно выполнены, и модель представления СЗИ продемонстрирует их влияние, что представляет собой гибкий механизм анализа эффективности возможных вариантов контрмер для аналитика с высокой квалификацией. Сравнивая такой подход с существующими методами анализа защищенности, можно отметить его близость факторному анализу, предполагающему декомпозицию угроз и уязвимостей и изучение влияния состояний системы защиты на эффективность ее работы.

Разработанная методика программно реализована в рамках решения частной задачи – оценки защищенности ресурсов ИС коммерческих предприятий, хранящихся в базах данных любого типа. Программа использует американский профиль защиты Commercial Database Management System Protection Profile и предназначена для специали-

стов в области ИБ и системных администраторов коммерческих предприятий.

Программа обладает свойством масштабируемости, что делает разработанный продукт гибким инструментом в области анализа рисков предприятий.

ЛИТЕРАТУРА

1. ГОСТ Р ИСО/МЭК 15408–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

2. *Жданов О.Н.* Методика анализа и минимизации рисков информационной инфраструктуры космических телекоммуникационных систем / О.Н. Жданов, В.В. Золотарев, К.В. Мушовец // Матер. X науч.-практ. конф. «Исследование, разработка и применение высоких технологий в промышленности» / СПб. НЦ РАН. СПб., 2010.

АВТОМАТИЗИРОВАННАЯ ОБУЧАЮЩАЯ СИСТЕМА ПО ДИСЦИПЛИНЕ «ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

М.П. Чеплакова, студентка 5-го курса

Научный руководитель М.А. Сопов, ассистент

г. Томск, ТУСУР, каф. КИБЭВС, milstar@inbox.ru

На конференции «Научная сессия ТУСУР–2010» была представлена статья [1, с. 271], описывающая структуру статической обучающей системы по дисциплине «Правовое обеспечение информационной безопасности». В продолжение темы в данной статье будут рассмотрены новые возможности, которые уже реализованы в описанной системе. Структура системы представлена на рис. 1.

Дисциплина «Правовое обеспечение информационной безопасности» основывается на законодательной базе, которая постоянно меняется. Поэтому задача заключалась в том, чтобы сделать обучающую систему динамической. То есть в системе должен быть предусмотрен модуль редактирования имеющейся теоретической базы.

Источником получения правовой информации для изучения дисциплины является правовая справочно-информационная система. Сегодня существует немало таких систем, лидерами которых являются КонсультантПлюс и Гарант. Система по дисциплине «Правовое обеспечение информационной безопасности» является справочно-обучающей, поэтому отличительная особенность данной системы от правовых справочно-информационных систем состоит в том, что она не только хранит определенный набор документов по узкому направ-

лению, но и имеет возможность создавать лекционный материал и проводить электронное тестирование. Также для удобства «Руководства пользователя по справочно-правовым системам КонсультантПлюс и Гарант» включены в обучающую систему.

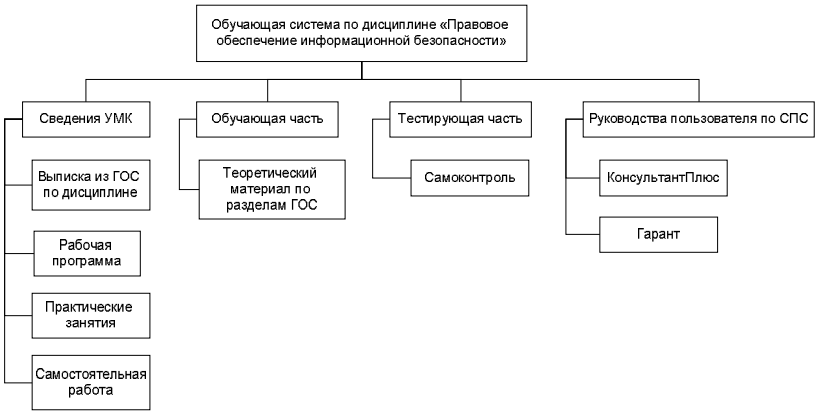


Рис. 1. Структура системы

Данная система представляет собой программный комплекс в виде веб-приложения, состоящий из базы данных, которая позволяет хранить большое количество информации, и программных инструментов, позволяющих работать с этой информацией.

В системе предусмотрены два режима работы: преподавателя и студента. Преподаватель наделен правами обновления теоретических разделов и формирования вопросов теста. Студент наделен правами чтения имеющейся информации.

Для обеспечения безопасности от несанкционированных изменений имеющейся в системе информации реализована система регистрации и аутентификации преподавателя.

Система имеет дружественный интерфейс и проста в использовании.

Данный программный комплекс является эффективным инструментом, который обеспечивает пользователям удобный доступ к информации, необходимой для изучения дисциплины «Правовое обеспечение информационной безопасности».

Выполнено в рамках проекта ГПО-0942 – «Инженерия баз данных».

ЛИТЕРАТУРА

1. Научная сессия ТУСУР–2010: Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых, 4–7 мая 2010 г.: В 5 ч. Ч. 3. Тематический выпуск «Методы и системы защиты информации. Информационная безопасность». Томск: В-Спектр, 2010. 280 с.

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ИССЛЕДОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ

Д.В. Черных, студент 5-го курса
Научный руководитель А.А. Конев, доцент, к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, dmit-cher@mail.ru

Обработка речевого сигнала в автоматическом режиме является перспективным направлением и может найти применение в различных отраслях, таких как информационные технологии, биомедицинские технологии, а также в области безопасности. Для осуществления такой обработки необходимо выделить в речевом сигнале ряд параметров, которые могли бы охарактеризовать отдельные звуковые единицы. К настоящему моменту вопросы, касающиеся выделения таких параметров применительно к русскому языку, слабо освещены, поэтому исследования в данном направлении являются актуальными. Чтобы проводить такие исследования, необходимо обладать набором инструментов, позволяющих осуществлять различные эксперименты, внедрять и испытывать разработанные алгоритмы, а также производить оценку результатов. В связи с этим существует необходимость в разработке программного комплекса, способного предоставить функционал, необходимый в исследованиях.

Разработанный программный комплекс позволяет производить свертку сигнала с фильтром, вычислять номер канала частоты основного тона, проводить одновременную маскировку, генерировать фильтры с заданными параметрами, отображать на экране и сохранять в файл полученные результаты.

Кратко схему работы программного комплекса можно описать следующим образом: входными данными являются исследуемый речевой сигнал, а также фильтр, с которым будет происходить свертка. Результатом этой свертки являются набор интенсивностей гармоник для каждого канала фильтрации на каждом временном отсчете и результаты одновременной маскировки. В дальнейшем полученные параметры сигнала вместе с различными настройками фильтра используются для вычисления остальных значений.

Все полученные характеристики сохраняются в центральную базу данных и могут быть в дальнейшем использованы без повторного их вычисления. Также существует возможность добавлять в эту базу фильтры и сигналы.

Для визуализации результатов используется графический модуль, позволяющий производить масштабирование, а также имеющий возможность отображать результаты в указанных интервалах.

Интерфейс программного комплекса разделен на функциональные блоки, в которых выполняются схожие по смыслу операции. Функциональные блоки, в свою очередь, также разбиты на группы однотипных действий в рамках текущего блока.

Для каждого модуля существует свой набор входных и выходных данных.

Модуль добавления сигнала:

– входные данные: звуковой файл формата WAV с параметрами 8000 Гц, 16 бит, моно;

– выходные параметры: запись в центральной базе данных, в которой хранится вся информация о звуковом сигнале и сам сигнал.

Модуль создания фильтра:

– входные данные: набор параметров, необходимых для создания и описания фильтра;

– выходные данные: запись в базе данных, включающая в себя все характеристики фильтра.

Модуль свертки сигнала с фильтром:

– входные данные: звуковой сигнал и фильтр из базы данных;

– выходные данные: запись в базе данных, содержащая продукты свертки, а также номера сигнала и фильтра.

Графический модуль:

– входные данные: продукты свертки из базы данных, а также информация о необходимых графиках;

– выходные данные: отображение на экране запрошенной информации, файл в формате JPEG.

В результате был реализован программный комплекс, позволяющий проводить начальные исследования со звуковыми сигналами. Была установлена на сервер и настроена центральная база данных для хранения входных сигналов и обработанных данных, решив при этом проблему доступности необходимой информации.

Развитие проекта будет продолжено. Возможны следующие дополнения:

– добавление новых алгоритмов обработки сигнала;

– модуль оценки качества работы алгоритмов;

– модуль записи и воспроизведения сигнала;

– дополнения в графическом модуле, связанные с отображением и редактированием разметки сигнала на различные классы звуков;

– интерфейс для работы с речевым корпусом и интеграция речевого корпуса с базой обработанных сигналов.

ЛИТЕРАТУРА

1. *Борри Х.* Firebird: руководство разработчика баз данных: Пер. с англ. СПб.: БХВ-Петербург, 2006. 1104 с.

2. *Райт Ричард С.-мл., Личпак Бенджамин.* OpenGL. Суперкнига. 3-е изд.: Пер. с англ. М.: Изд. дом «Вильямс», 2006. 1040 с.

3. *Агуров П.В.* C#. Разработка компонентов в MS Visual Studio 2005/2008. СПб.: БХВ-Петербург, 2008. 480 с. + CD-ROM (Профессиональное программирование).

4. The Open Toolkit Manual [Электронный ресурс]. Режим доступа: http://www.opentk.com/doc

5. Библиотека MSDN (по-русски) [Электронный ресурс]. Режим доступа: http://msdn.microsoft.com/library/ms123401.

МОНИТОРИНГ И КОНТРОЛЬ РАБОЧИХ СТАНЦИЙ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

М.А. Девяткин, аспирант

Научный руководитель А.А. Шелупанов, проректор по научной работе ТУСУР, проф., д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, max5252@vtomske.ru

В настоящее время органы внутренних дел (ОВД) являются самой большой по численности и самой разветвленной структурой из числа всех правоохранительных структур государства. Они накапливают и обрабатывают огромное количество информации, что приводит к активной компьютеризации их деятельности. Так, например, только во внутренней сети УВД по Томской области насчитывается около 3000 рабочих станций. При этом администраторы должны обеспечивать работоспособность всех рабочих станций и оперативно реагировать на любые изменения, поскольку от этого напрямую зависит качество и оперативность работы ОВД.

Рабочие станции являются наиболее доступными и уязвимыми компонентами сети и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. К тому же с рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы.

Проблема информационной безопасности для ОВД представляет наибольший интерес. При этом, как отмечают многие исследовательские центры, более 80% всех инцидентов, связанных с нарушением

информационной безопасности, вызваны внутренними угрозами, источниками которых являются легальные пользователи системы. Зачастую в силу своей халатности и небрежности они могут ввести заведомо неверные данные, пропустить ошибки в программном обеспечении, создав тем самым брешь в системе защиты. Все это заставляет задуматься о том, что внутренняя угроза, исходящая непосредственно от пользователей, значительнее и опаснее внешних воздействий.

В этом случае можно выделить следующие возможные каналы утечки информации:

- несанкционированное копирование информации на внешние носители и вынос её за пределы контролируемой территории;
- вывод на печать информации и вынос распечатанных документов за пределы контролируемой территории;
- несанкционированная передача информации по сети на внешние серверы, расположенные вне контролируемой территории;
- хищение носителей, содержащих информацию, – жёстких дисков, компакт-дисков CD-ROM и др.

Мониторинг и контроль рабочих станций является сложной задачей и позволяет обеспечивать бесперебойную работу всей сети и в любой момент времени иметь информацию о состоянии и работоспособности всех объектов, конфигурации программного и аппаратного обеспечения. Полный контроль над каждым элементом инфраструктуры гарантирует максимальную отдачу от существующей инфраструктуры.

Как правило, системы мониторинга представляют собой специализированные программные комплексы и состоят из следующих компонентов (рис. 1):

- модули-датчики, устанавливаемые на рабочие станции пользователей и обеспечивающие сбор информации о событиях, регистрируемых на этих станциях;
- модуль анализа данных, собранных датчиками, с целью выявления ошибок и несанкционированных действий пользователей;
- модуль реагирования на ошибки и действия пользователей;
- модуль хранения результатов работы системы.
- модуль централизованного управления компонентами системы.

Однако применение систем мониторинга зачастую влечёт за собой установку дополнительного ПО на каждую рабочую станцию, что потенциально может привести к увеличению сложности администрирования, а также к возможным конфликтам в работе программ системы.

Преимуществом использования таких систем мониторинга является возможность создания виртуальной изолированной среды обработки информации без физического выделения отдельных рабочих

станций для работы с данными ограниченного доступа. Кроме того, системы этого типа позволяют программно ограничить вывод информации на внешние носители, что избавляет от необходимости физического удаления из компьютеров устройств записи информации, а также опечатывания портов и системных блоков.

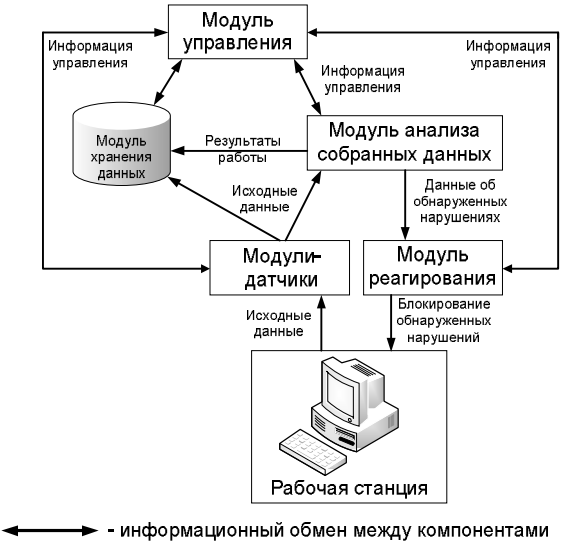


Рис. 1. Типовая архитектура системы мониторинга рабочих станций пользователей

Таким образом, поскольку в настоящее время не существует адаптированной для ОВД комплексной системы мониторинга и контроля рабочих станций, то разработка такой системы является актуальной. При этом основной задачей такой системы является повышение уровня информационной безопасности, благодаря осведомленности о состоянии рабочих станций и возможности осуществлять контроль. Её применение также поможет повысить эффективность использования аппаратного и программного обеспечения, снизить вероятность возникновения сбоев в системе (что особенно важно для госструктур) и снизить временные затраты администратора на обслуживание системы.

ЛИТЕРАТУРА

1. *Уилсон Э.* Мониторинг и анализ сетей. Методы выявления неисправностей. М.: Лори, 2002. 364 с.

2. *Доля А.* Защита от утечек через рабочие станции [Электронный ресурс]. Режим доступа: http://www.compress.ru/

СИСТЕМА РАСПОЗНАВАНИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ КЛАВИАТУРНОГО ПОЧЕРКА

С.А. Елистратов, А.А. Чичерин, М.А. Косенко, студенты
Научные руководители: Е.М. Давыдова, доцент,
Е.Ю. Костюченко, доцент
г. Томск, ТУСУР, ФВС, каф. КИБЭВС

Предложена методика защиты ЭВМ и сетей на их основе с использованием аутентификации по клавиатурному почерку. Проведено сравнение двух типов ИНС: перцептрон, сеть Кохонена.

Целью работы является создание системы для распознавания пользователя по клавиатурному почерку, основываясь на которой, в дальнейшем возможна реализация разграничения прав доступа. Модель системы в виде «черного ящика» представлена на рис. 1 [1].

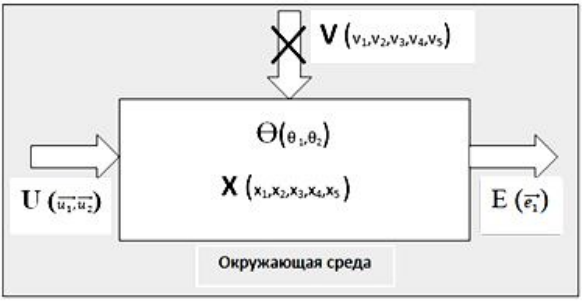


Рис. 1. Модель распознавания по клавиатурному почерку

Предполагается, что выделенная система связана со средой через совокупность входов и выходов.

$U = \{\overrightarrow{u_1}, \overrightarrow{u_2}\}$ – входные данные, где $\overrightarrow{u_1}$ – время нажатия клавиши (миллисекунды, (0; ∞)) и $\overrightarrow{u_2}$ – время задержки между нажатиями клавиш (миллисекунды, (0; ∞));

$E = \{\overrightarrow{e_1}\}$ – выходные данные, где $\overrightarrow{e_1}$ – вектор из 0 и 1, где 1 – соответствие входных данных пользователю, определяемому по UID (уникальный идентификатор пользователя);

$\Theta = \{\theta_1, \theta_2\}$ – параметры модели, где θ_1 – определенная клавиатура и θ_2 – набираемый текст;

$X = \{x_1, x_2, x_3, x_4, x_5\}$ – состояния весов для пользователей;

$V = \{v_1, v_2, v_3, v_4, v_5\}$ – внешние факторы (не учитываются);

v_1 – эмоциональный фактор;

v_2 – размер, форма руки и пальцев;

v_3 – время суток, ч; [0; 23];

v_4 – психофизическое состояние; целое, баллы [0; 5];

v_5 – внешнее воздействие на пользователя, целое, баллы [0; 5].

Сбор данных для исследований проводился приложением, написанным на Visual C++ [2]. Собираемые данные: время нажатия клавиши и время задержек между нажатиями клавиш.

Для классификации использовались ИНС, вида двухслойный перцептрон [3] и сети Кохонена, реализованные в среде MatLab [4].

В исследовании, проводимом на первом этапе, использовался двухслойный перцептрон. Обучение производилось с учителем методом обратного распространения ошибки.

Параметры ИНС на перцептроне [3]:

– метод обучения – метод связанных градиентов Флетчера–Пауэлла;

– функция активации на промежуточном слое – сигмоидная функция;

– функция активации на выходном слое – линейная функция.

Параметры ИНС на перцептроне были выбраны в ходе экспериментов как параметры, при которых процент ошибок был минимален.

В данный момент проводятся исследования с использованием сети Кохонена, которая также, как и перцептрон, применяется для распознавания образов и классификации. В отличие от обучения сети на перцептроне (обучение с учителем), обучение сети Кохонена проводилось без учителя, что существенно повлияло на процент ошибки. Сети Кохонена способны выявлять новизну во входных данных – если после обучения сеть встретится с набором данных, не похожим ни на один из известных образцов, то она не сможет классифицировать такой набор и тем самым выявит его новизну [5].

Параметры сети Кохонена:

– нормализация входных данных – нормализация в вектор с единичной длиной;

– метод обучения – метод последовательных приращений, после чего метод случайных приращений.

Классификация данных проводилась по трем и пяти пользователям. При использовании сети Кохонена для классификации на пяти пользователях происходило слияние классов, поэтому для проведения сравнительной характеристики сетей Кохонена и перцептрона было выбрано три пользователя. Результаты исследований по трем пользователям приведены в табл. 1, по пяти пользователям – в табл. 2.

Одним из возможных применений является разграничение доступа к ЭВМ и сетям на их основах. Использование сети Кохонена – про-

цент ошибок увеличился, в связи с обучением без учителя, слияние классов при количестве пользователей больше трех. Требуется дальнейшее исследование для определения причин слияния.

Таблица 1

Процент ошибок классификации для трех пользователей

Наборы для обучения	Общее кол-во наборов	Ошибок классификации, %		Итоговый процент ошибок, %	
		Перцептрон	Сеть Кохонена	Перцептрон	Сеть Кохонена
0–20	300	1,87	4,47	1,845	5,13
40–60		1,82	5,8		

Таблица 2

Процент ошибок классификации для пяти пользователей (перцептрон)

Наборы для обучения	Общее кол-во наборов	Ошибок классификации, %	Итоговый процент ошибок, %
0–20	500	1,72	1,635
40–60		1,55	

ЛИТЕРАТУРА

1. *Перегудов Ф.И., Тарасенко Ф.П.* Основы системного анализа: учеб. 3-е изд. Томск: Изд-во НТЛ, 2001. 396 с.

2. *Шилдт Г.* Самоучитель C++: Пер. с англ. 3-е изд. СПб.: БХВ-Петербург, 2003. 688 с.

3. *Хайкин С.* Нейронные сети: полный курс. 2-е изд.: Пер. с англ. М.: Изд. дом «Вильямс», 2006. 1106 с.

4. *Ануфриев И.Е., Смирнов А.Б., Смирнова Е.Н.* MATLAB 7. СПб.: БХВ-Петербург, 2005. 1104 с.

5. Классификация известных нейросетей [Электронный ресурс]. Режим доступа: http://victoria.lviv.ua/html/oio/html/theme7_rus.htm, свободный. Загл. с экрана. Яз. рус.

ПРОГРАММНЫЙ ЭМУЛЯТОР HASP

П.В. Ермолаев, студент

Научный руководитель Ю.М. Филимонов, доцент, к.ф.-м.н.

г. Томск, ТУСУР, ФВС, pikss86@gmail.com

Электронные ключи HASP – надежный способ защиты программ от копирования, но существуют способы обхода такой защиты.

Для копирования программ, защищенных с помощью HASP, нужно смоделировать физический ключ. Модель ключа HASP 4 изучена еще примерно в 2005 г. Это позволило реализовать модель в виде программы.

Реализация модели ключа в виде программы называется программным эмулятором HASP. Эмуляторы в основном применяются для нелегального копирования ПО. Чем точнее модель, тем больше возможностей для нелегального копирования ПО будет у эмулятора. Бывают программы, для копирования которых не нужна точная реализация модели. Для них достаточно табличных эмуляторов. Табличные эмуляторы созданы по принципу запрос–ответ. В таких эмуляторах есть таблица, в которой на каждый определенный запрос есть определенный ответ. Табличные эмуляторы не реализуют логику работы ключа, они просто формируют нужные ответы на запросы. При длительной работе, защищенной с помощью HASP-программы, от нее в эмулятор может поступить такой запрос, на который в таблице эмулятора не окажется ответа, и работа защищенной программы будет прервана.

Гораздо больше возможностей предоставляют эмуляторы, которые реализуют логику работы ключа. За счет реализованной логики работы физического ключа такие эмуляторы способны формировать гораздо большее количество правильных ответов на запросы. Чтобы разобраться, как работает эмулятор, реализующий логику физического ключа, рассмотрим рис. 1. На нем изображены путь запроса от приложения к ключу и путь ответа от ключа к приложению.

Как видно из рисунка, прежде чем попасть в ключ, запрос проходит через цепь посредников, в каждом посреднике запрос меняет свой вид. Протоколы обмена данными между посредниками также различны и сложны. В этой цепи есть звено, которое не создавалось разработчиками HASP – это драйвер шины USB (Universal Serial Bus – универсальная последовательная шина). Это значит, что формат обмена запросами между драйвером HASP и драйвером шины USB известен. Это URB (USB Request Block – блок запроса USB) пакеты, так как драйвер шины USB работает по стандарту, а в стандарте USB данные передаются в URB пакетах. Таким образом, чтобы данные попали в физический ключ, драйвер HASP должен упаковать запрос в URB пакет, который через драйвер шины USB попадет в физический ключ. Ответ от физического ключа также передается в URB пакете. Так как формат обмена между драйвером HASP и драйвером шины USB строго задан, проанализировав данные, передаваемые в URB пакетах, можно создать модель ключа и подменить драйвер шины USB эмулятором HASP.

Для построения модели конкретного ключа HASP сложность заключается в том, что чтобы модель была точной, нужен ключ шифрования, на котором конкретный HASP шифрует данный. Этот ключ шифрования «спрятан» в чип HASP и не доступен извне. Он доступен

только криптопроцессору внутри HASP. Весь принцип защиты HASP основан на том, что трудно узнать «спрятанный» ключ шифрования.

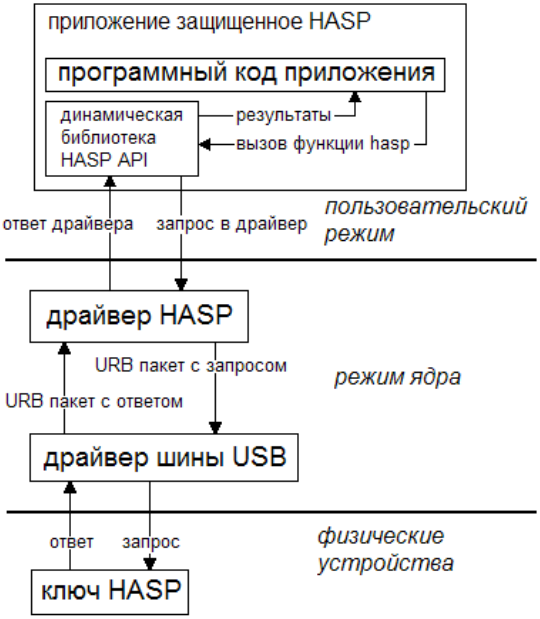


Рис. 1. Обмен данными между программой и HASP

Ключ шифрования нужен для копирования физического HASP и взлома программ с помощью эмуляторов, но если цель не взлом программ, а моделирование работы HASP, то данный ключ шифрования совершенно не нужен. Эмулятор будет вести себя как физический HASP и с любым другим ключом шифрования. Поэтому, добавив в эмулятор вымышленный ключ шифрования, можно создать эмулятор не для взлома, а для обучающих целей.

Работа с эмулятором будет выглядеть так, как будто бы к компьютеру подключен физический ключ. Если применить эмулятор для обучения, это позволит создавать множество виртуальных ключей, с помощью которых можно будет проводить лабораторные работы, давать эмулятор студентам для самостоятельного изучения HASP. Также на основе эмулятора можно создать систему для изучения HASP API. Изучение HASP API позволит специалистам по защите информации защищать программы наиболее надежным способом.

Если есть возможность обратить созданный для взлома эмулятор, в обучающий эмулятор для подготовки специалистов по безопасности, было бы разумно ее использовать.

ЛИТЕРАТУРА

1. Ассемблер, системное и низкоуровневое программирование [Электронный ресурс]. Режим доступа: http://www.wasm.ru

2. *Агуров П.В.* Практика программирования USB. СПб.: БХВ-Петербург, 2006. 624 с.

3. *Солдатов В.П.* Программирование драйверов Windows. 2-е изд., перераб. и доп. М.: ООО «Бином-Пресс», 2004. 480 с.

СИСТЕМА КОНКУРЕНТНОГО РАННЕГО ПРЕДУПРЕЖДЕНИЯ УГРОЗ ДЛЯ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

И.И. Ерофеева, студентка

Научный руководитель Н.И. Баяндин, зав. каф. КОИБАС

г. Москва, МЭСИ, КОИБАС, ierofeeva@mesi.ru

Деятельность современной организации во многом определяется динамикой информационной среды. С учетом жесткого конкурентного противоборства становится жизненно важными возможность выявления угроз организации на ранних стадиях возникновения и наличие системы управления рисками.

Оценка рисков – сложная аналитическая работа, основанная на мониторинге и анализе большого количества информационных источников различной степени достоверности и полноты. Американский аналитик Бен Джилад (Benjamin Gilad) в своих работах предложил методологию разработки системы конкурентного раннего предупреждения (КРП), позволяющую выявлять индикаторы угроз на ранних стадиях возникновения и оценивать наступление благоприятных возможностей раньше конкурентов.

В предложенной работе сделана попытка оценки возможностей реализовать идеи Б. Джилада для системы КРП государственного образовательного учреждения высшей школы.

Основной задачей системы КРП является предотвращение негативных последствий для организации, связанных с возникновением неожиданных ситуаций в конкурентной среде.

Алгоритм работы системы КРП состоит из трех основных шагов.

Каждый из этих шагов является критически важным для эффективной деятельности организации.

Рассмотрим эти шаги:

Шаг 1. Идентификация (идентификация зон стратегических угроз, рисков и шансов). Осуществляется группой аналитиков путем по-

строения моделей угроз, рисков и шансов и определением их признаков и индикаторов.

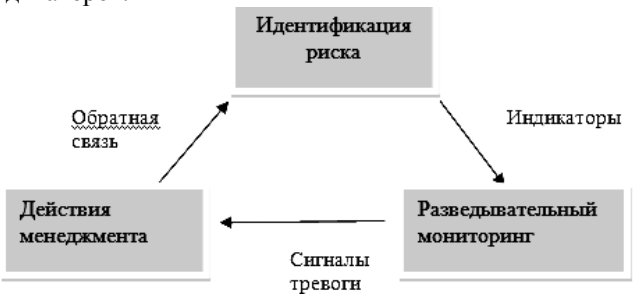


Рис. 1. Механизм КРП

Для идентификации изменения Б. Джилад вводит понятие отраслевых *«драйверов»* изменений (драйвер (driver) – фактор, вызывающий необходимость действия). Отраслевые драйверы изменений представляют собой события или переменные, управляющие развитием отрасли и/или конкурентной среды.

Основные отраслевые драйверы могут быть представлены, например, в виде:

- новой технологии или научного достижения,
- нового государственного регулирования,
- появления новых законов и подзаконных актов.

Для образовательной конкурентной среды в качестве драйверов могут выступать изменения в государственной политике в области образования, введение новых образовательных стандартов, переход на двухуровневую модель образования, введение ЕГЭ, появление новых специальностей, «демографическая яма» и др.

Для образовательных учреждений, таких как университеты, можно выделить группы информационных и репутационных рисков, связанных со следующими основными видами угроз:

1. Утечка конфиденциальной информации (персональные данные, результаты НИР, методические разработки и т.д.).

2. Создание негативного имиджа университета путем использования методов черного PR.

3. Хищение и модификация информации из электронной среды (электронный документооборот, электронное обучение).

Следуя матрице драйверов, аналитики и менеджеры могут строить прогнозы о направлениях дальнейшего развития организации и сценарии поведения конкурентной образовательной среды. Сценарии по определению являются гипотезами будущих событий. В отличие от статистических методов прогнозирования, которые представляют

тренд как результат предыдущих событий, в сценариях учитываются возможные угрозы.

Шаг 2. Разведывательный мониторинг (мониторинг информационного пространства с целью выявления признаков и индикаторов появления угроз, рисков и шансов).

Сбор информации должен быть плановым, в соответствии с разрабатываемым сценарием. Для решения такой задачи организовывается мониторинг внешних и внутренних информационных источников. Большая часть разведданных о внешней окружающей среде уже существует внутри компании. Доступ к ней может быть организован через создание внутренней информационной сети.

В качестве сотрудников сети мониторинга могут выступать такие подразделения, как ИТ-отдел (контроль за утечкой информации из электронной среды), служба конкурентной разведки и отдел по связям с общественностью (борьба с имиджевыми угрозами), подразделения информационной безопасности (контроль конфиденциальной информации о результатах НИР).

Контроль внешних источников может контролироваться службой КР с помощью сети Интернет, информационно-аналитических систем (например, Галактика-Zoom, Арион, Семантический архив и др.) и профессиональных баз данных (Lexis-Nexis, Factiva, Интегрум и др.).

Информация от вышеперечисленных структурных подразделений организации поступает к аналитикам, для её последующей обработки и представления менеджерам или руководству.

Шаг 3. Управленческие действия (адекватные действия менеджмента на появившиеся угрозы и оценку рисков). Проводится руководством организации в соответствии с выявленными признаками угроз и оценкой рисков, в том числе и по планам чрезвычайных ситуаций.

Выводы. Система КРП позволяет подготовить управленческие решения задолго до момента наступления негативных последствий.

Рассмотренная система раннего предупреждения применима не только к обычным предприятиям, но и к образовательным учреждениям высшего образования.

ЛИТЕРАТУРА

1. *Баяндин Н.И.* Технологии безопасности бизнеса: введение в конкурентную разведку. М.: Юристъ, 2002. 320 с.

2. *Астахов А.М.* Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.

3. *Джилад Б.* Конкурентная разведка. Как распознавать внешние риски и управлять ситуацией. СПб.: Питер, 2010. 320 с. (Early warning: using competitive intelligence to anticipate market shifts, control risk, and create powerful strategies).

ОПРЕДЕЛЕНИЕ ПОЛА АВТОРА КОРОТКОГО ЭЛЕКТРОННОГО СООБЩЕНИЯ

А.О. Гальвас, студент, А.С. Романов, доцент, к.т.н.
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, galart@t-sk.ru

С развитием высоких технологий, появлением компьютеров и увеличением объёмов хранимой в электронном виде текстовой информации открываются новые возможности для исследования естественного языка. Компьютер, способный автоматически обрабатывать большие объёмы информации, позволяет широко применить статистические методы в лингвистике. В частности, одной из задач компьютерной обработки текстов является определение пола автора по его текстам. К настоящему времени исследования по количественному определению пола автора короткого электронного русскоязычного сообщения не проводились. Суть данной работы состоит в том, чтобы определить пол автора короткого текста по статистическим характеристикам. Сложность заключается как в выборе этих характеристик, так и в способе их сравнения для разных авторов. Основным предположением является то, что мужчины и женщины при написании текста могут характеризоваться определенными признаками, которые вносятся авторами неосознанно.

Целью работы является создание комплексной методики для определения пола автора коротких электронных сообщений и программной системы на её основе.

В общем случае для реализации данной цели необходимо решить ряд задач:

– анализ предметной области;

– разработка программного обеспечения для сбора материала для исследований;

– формирование базы данных коротких электронных сообщений;

– разработка алгоритмов и программного обеспечения для решения задачи определения пола;

– исследование характеристик текста;

– формирование обобщенной методики.

Исходными данными к проекту являются сообщения с форумов сети Интернет, в которых пользователи указывают свою принадлежность к тому или иному полу. Для сбора сообщений используется разработанная программа-парсер, предназначенная для разбора html-кода страницы и выделения из него информации для исследований: текстовой части, псевдонима автора и его пола. Программа позволяет накопить объемную базу сообщений в автоматическом режиме, что существенно снижает временные затраты исследователя.

Для решения задачи определения пола автора сообщений, следует использовать алгоритмы бинарной классификации. Одним из таких алгоритмов является метод опорных векторов. Данный метод сводится к нахождению гиперплоскости, разделяющей объекты двух классов. В случае линейной разделимости классов такую гиперплоскость всегда можно записать в виде линейной комбинации «опорных векторов» [1]. В задаче классификации с выборкой в случае нелинейной разделимости существует идея отображения данных в пространство, в котором разделяющая гиперплоскость будет линейной либо близкой к ней.

Искусственные нейронные сети, основанные на принципах работы биологических нейронов, также можно использовать в качестве одного из методов классификации. Идея состоит в том, чтобы, подавая на вход нейронов импульсы в виде произведения их значения и весов, на выходе получать некоторый выходной вектор, элементы которого интерпретируются как принадлежность к классу [2].

Отметим, что данные классификаторы успешно применялись при решении задачи определения автора короткого сообщения [3].

Основная сложность, с которой сталкиваются исследователи, заключается в отсутствии однозначного мнения о том, какие из признаков текста однозначно характеризуют пол автора. Однако комбинации характеристик текста, а также применение ансамблей нейронных сетей и машин опорных векторов могут дать приемлемые результаты, применимые для решения практических задач в специализированных учреждениях.

При формировании обобщенной методики стоит также учитывать возраст, образование, сферу деятельности авторов-мужчин и авторов-женщин и т.д. С учетом этих особенностей подбирать корпуса текстов для исследований и вводить корректирующие коэффициенты в итоговую методику.

ЛИТЕРАТУРА

1. *Vapnik V.N.* The nature of statistical learning theory. N.Y.: Springer-Verlag, 2000. 332 p.

2. *Хайкен С.* Нейронные сети: полный курс. 2-е изд. М.: Вильямс, 2006. 1104 с.

3. *Романов А.С.* Идентификация авторства коротких текстов методами машинного обучения / А.С. Романов, Р.В. Мещеряков // Компьютерная лингвистика и интеллектуальные технологии: По матер. ежег. Междунар. конф. «Диалог» (Бекасово, 26–30 мая 2010 г.). М.: Изд-во РГГУ, 2010. Вып. 9 (16). С. 407–413.

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ОТРАБОТКИ НАВЫКОВ ЗАЩИТЫ СЕРВЕРА

И.Г. Ганюшкин, В.Е. Шильненков, студенты 4-го курса
Научный руководитель Р.В. Мещеряков, доцент, д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, GanyushkinIG@gmail.com

Исходя из очевидного утверждения, что информационная безопасность компании зависит от снижения рисков, можно утверждать, что эффективное управление рисками способствует обеспечению непрерывности бизнеса, где риск информационной безопасности – это потенциальная возможность использования определённой уязвимости [1].

Вследствие изучения рынка услуг в сфере защиты информации мы пришли к выводу, что IT-специалисты в большинстве своём не имеют опыта поиска и устранения уязвимостей вычислительных сетей, также отсутствуют инструментальные средства повышения их квалификации, что приводит к применению неэффективных мер защиты. Для выхода из сложившейся ситуации предлагается внедрение систем, позволяющих проводить проверку на соответствие имеющихся у специалиста навыков в области информационной безопасности, а именно, предлагается создание комплекса для отработки превентивных навыков защиты сервера, примитивная структура которого представлена на рис. 1.

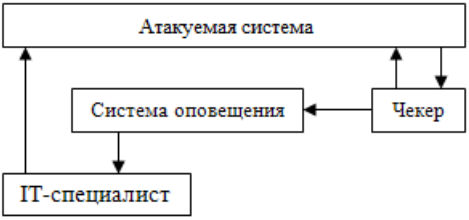


Рис. 1. Структура тренажёра

На сегодняшний момент мы имеем результаты исследований для понимания поведения и предпочтений потребителей, конкурентов и рынков. Исследования проводились путём сбора и анализа информации, с целью уменьшения неопределённостей при принятии исследовательских решений. Для изучения предпочтений были написаны и запущены конкурсы по взлому сервера. Параллельно ведётся подготовка к проведению международных соревнований Capture the Flag (CTF) на территории Томска. Структура соревнований CTF представлена на рис. 2. Также разработана архитектура комплекса, которая устроена таким образом, что обучение может осуществляться как в статическом режиме, так и в динамическом. Реализация второго построена на возможности проведения on-line соревнований.

Уязвимости, которые были предложены для эксплуатации в конкурсах, в дальнейшем будут включены в библиотеку уязвимостей разрабатываемого комплекса.

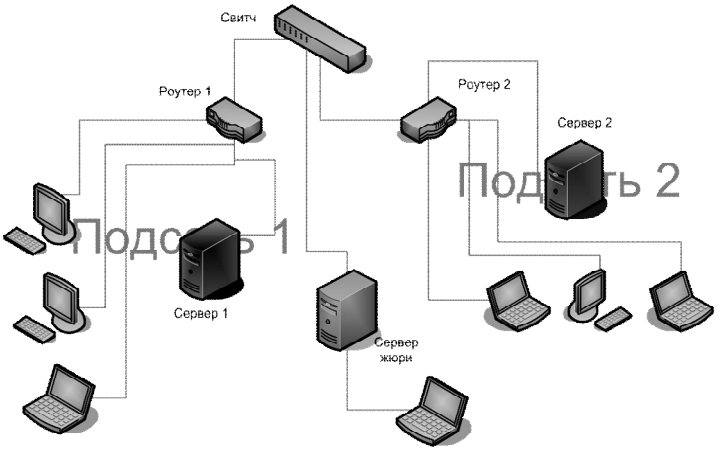


Рис. 2. Структура соревнований

Суть идеи создания программного комплекса заключается в том, что предлагается применять более эффективные методы управления рисками. Применение превентивных мер, а именно снижение количества уязвимостей хотя бы на 20%, приводит к снижению рисков на 80%, что связано с тем, что около 80% злоумышленников могут использовать около 20% уязвимостей [2].

Принцип работы с тренажёром отражает диаграмма Шухарта – Деминга, представленная на рис. 3.

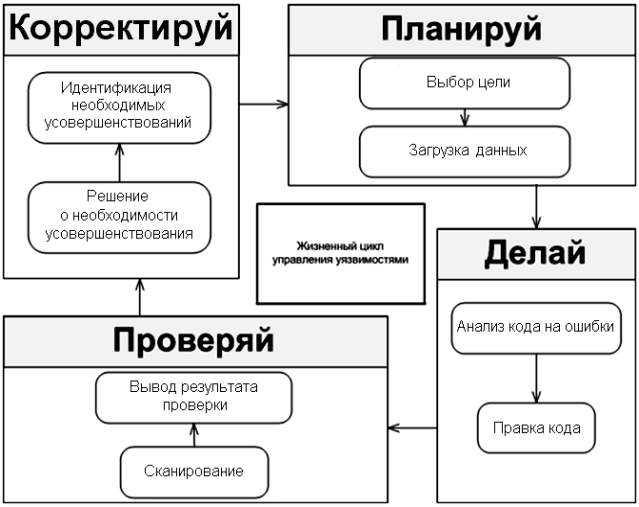


Рис. 3. Жизненный цикл устранения уязвимостей

С помощью данного комплекса предполагается решение следующих задач:

• допуск к работе лиц, удовлетворяющих соответствующим квалификационным требованиям в сфере IT-безопасности;

• обеспечение проведения подготовки и аттестации работников предприятий и учреждений в области IT-безопасности;

• отработка основных приёмов в критических или чрезвычайных ситуациях;

• обучение работников служб безопасности действиям при критических или чрезвычайных ситуациях.

• анализ причин возникновения инцидентов и принятие мер по устранению выявленных причин.

ЛИТЕРАТУРА

1. Британский стандарт «Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности» от 06 октября 2008 г. BS ISO/IEC 27005:2008 ru

2. Превентивные меры снижения рисков считаются самыми эффективными [Электронный ресурс]: Электрон. дан. [Москва]. Режим доступа: http://www.penetrationtest.ru/service/Preventive_measures_detail.html, свободный. Загл. с экрана.

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

И.М. Гавриленко, студент 5-го курса,
М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, soyer-mail@mail.ru

В современных условиях быстро меняющейся рыночной ситуации возникают проблемы управляемости предприятий и организаций. На практике эти проблемы выражаются в том, что менеджеры всех уровней практически «задыхаются» под тяжестью непрерывного потока документов и задач, требующих немедленного решения. Естественно, что в таких условиях качество и оперативность принятия решений серьезно страдают.

Бумажный документооборот имеет целый ряд минусов, из-за которых стоит задуматься о внедрении электронного документооборота. Из этих минусов:

– медленный поиск документов;

– трудности отслеживания движения документа на всех этапах его жизненного цикла;

– сложность организации эффективного контроля и отчетности по исполнению резолюций;

– длительность сроков подготовки и согласования документов;

– сложность организации документооборота, если с одними и теми же документами одновременно работает несколько пользователей;

– невозможность или трудоемкость получения сводных отчетов и журналов.

Реальным выходом из создавшейся ситуации служат системы электронного документооборота (СЭД). Они решают такие задачи, как накопление, управление и доступ к электронной информации; оптимизация бизнес-процессов и автоматизация механизма их выполнения и контроля; исключение необходимости хранения бумажных документов и многое другое.

На экране компьютера видны все документы, задачи и поручения. Ход всех бизнес-процессов, например, реализация заказов клиентов, прием на работу, текущее состояние исполнения договоров, можно контролировать в режиме реального времени в ходе их выполнения. Степень взаимодействия филиалов и представительств существенно возрастает, укрепляются их информационные связи с центральным офисом. Оперативность предоставления данных снижает количество потенциальных фактических ошибок в документах, поступающих к руководству.

Но не стоит ошибочно полагать, что внедрение СЭД проходит гладко и просто. На самом деле этот процесс сопровождается рядом проблем, в частности это высокая стоимость систем и их обслуживания. А для предприятий малого бизнеса использование дорогостоящих систем не приемлемо.

Главной задачей моей дальнейшей работы будет организация защищенного электронного (ЭДО) документооборота на базе свободнораспространяемого программного обеспечения.

В результате исследований документооборота были выделены критерии, по которым проводилось сравнение систем электронного документооборота. В процессе анализа программного обеспечения набор критериев был расширен. Для описания каждого программного продукта использовалось 16 критериев:

1) электронное хранилище документов (EDM);

2) поиск документов;

3) контроль исполнения заданий;

4) архив;

5) создание шаблонов документов;

6) управление учетными записями;

7) настройка бизнес-процессов;

8) механизм ведения версий документа;
9) комментирование документов;
10) уведомление по электронной почте;
11) разграничение доступа;
12) графический интерфейс;
13) СКЗИ;
14) кроссплатформенность;
15) открытый код (Open Source);
16) регистрация бумажных документов.

В качестве рассмотренных были выбраны только свободно распространяемое ПО. В ходе исследования каждый продукт был установлен на систему Windows XP, полностью проверялся функционал систем.

Из списка исследованных программных продуктов были исключены:

– NauDoc Free;
– PayDox Personal;
– Globus START;
– OpenKM;
– Archivista;
– Comsoft Docs.

Эти СЭД не удовлетворяют функциям безопасности, а именно – у них отсутствует криптографическая защита и разграничение доступа к документам.

Достаточно важными критериями СЭД являются «Настройка бизнес-процессов» и «Регистрация бумажных документов». Им не соответствуют следующие СЭД:

– Доцеро;
– РДО – Araxgroup;
– Pyrus DMS Demo;
– Nuxeo;
– УправДок.

В связи с этим также исключаем их из списка исследуемых СЭД.

Главной задачей является организация защищённого ЭДО, поэтому важней всего в СЭД функции безопасности: «Разграничение доступа» и «СКЗИ». Этим критериям удовлетворяют 2 программных продукта:

– Alfresco;
– Bb workspace.

Приведённые ниже СЭД критериям безопасности удовлетворяют не максимально, но имеют хороший функционал, благодаря которому ЭДО осуществляется удобно и эффективно:

– Documentolog Demo;
– Documetr;
– LocalOff;
– FossDoc.

По основным критериям были выбраны 2 СЭД: Alfresco и Bb workspace. Они удовлетворяют всем функциям безопасности. Благодаря этому на их основе возможна организация защищенного электронного документооборота.

ЛИТЕРАТУРА

1. Независимый портал о СЭД [Электронный ресурс]. Web-портал. URL: http://www.doc-online.ru/

2. Внедрение систем электронного документооборота [Электронный ресурс]. Статья. URL: http://www.iteam.ru/publications/it/section_64/article_2687/

3. Преимущества ЭДО [Электронный ресурс]. URL: http://www.it-konsultant.ru/knowledge/22.html

4. Перспективы электронного документооборота [Электронный ресурс]. URL: http://doc-system.ru/sistema-elektronnogo-dokumentooborota/articles/preimushhestva-i-perspektivy.html

5. Проблемы внедрения и использования СЭД [Электронный ресурс]. URL: http://www.relga.ru/Environ/WebObjects/tgu-www.woa/wa/Main?textid=1066&level1=main&level2=articles

АРХИТЕКТУРА ПАРАЛЛЕЛЬНЫХ БАЗ ДАННЫХ

Ю.В. Гирная, Т.В. Остапчук, студенты 4-го курса
Научный руководитель М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, каф. КИБЭВС, gyv_yulya@mail.ru

Появление в 80-х годах персональных компьютеров и локальных сетей самым серьезным образом изменило организацию корпоративных вычислений. Но двумя основными проблемами построения вычислительных систем для важных приложений, связанных с обработкой транзакций, управлением базами данных и обслуживанием телекоммуникаций, стали обеспечение высокой производительности и продолжительного функционирования систем. В настоящее время широкое распространение получила технология параллельных баз данных. Это наиболее эффективный способ достижения заданного уровня производительности. Эта технология позволяет множеству процессоров разделять доступ к единственной базе данных. Распределение заданий по множеству процессорных ресурсов и параллельное их выполнение позволяют достичь более высокого уровня пропускной способности транзакций, поддерживать большее число одновременно ра-

ботающих пользователей и ускорить выполнение сложных запросов. Существуют три различных типа архитектуры, которые поддерживают параллельные базы данных:

– Симметричная многопроцессорная архитектура с общей (разделяемой) памятью (Shared Memory SMP Architecture). Эта архитектура поддерживает единую базу данных, работающую на многопроцессорном сервере под управлением одной операционной системы. Увеличение производительности таких систем обеспечивается наращиванием числа процессоров, устройств оперативной и внешней памяти.

К системам параллельных баз данных с разделяемой памятью относятся XPRS [Stonebraker et al., 1988], DBS3 [Bergsten et al., 1991] и Volcano [Graefe, 1990], а также перенесенные на мультипроцессоры с разделяемой памятью наиболее известные промышленные СУБД. Первым примером такой системы была реализация СУБД DB2 на IBM3090 с шестью процессорами. Во всех известных на сегодня коммерческих продуктах (таких как Ingres и Oracle) используется только межзапросный (но не внутризапросный) параллелизм.

– Архитектура с общими (разделяемыми) дисками (Shared Disk Architecture). Это типичный случай построения кластерной системы. Эта архитектура поддерживает единую базу данных при работе с несколькими компьютерами, объединенными в кластер (обычно такие компьютеры называются узлами кластера), каждый из которых работает под управлением своей копии операционной системы. В таких системах все узлы разделяют доступ к общим дискам, на которых собственно и располагается единая база данных. Производительность таких систем может увеличиваться как путем наращивания числа процессоров и объемов оперативной памяти в каждом узле кластера, так и посредством увеличения количества самих узлов.

Примеры параллельных СУБД с разделяемыми дисками: продукт IMS/VS Data Sharing (IBM), а также продукты VAX DBMS и Rdb компании DEC. Реализация Oracle на компьютерах VAXcluster (DEC) и NCUBE также использует разделение дисков, поскольку этот подход требует минимальных расширений в ядре СУБД. Отметим, что во всех этих системах применяется только межзапросный параллелизм.

– Архитектура без разделения ресурсов (Shared Nothing Architecture). Как и в архитектуре с общими дисками, в этой архитектуре поддерживается единый образ базы данных при работе с несколькими компьютерами, работающими под управлением своих копий операционной системы. Однако в этой архитектуре каждый узел системы имеет собственную оперативную память и собственные диски, которые не разделяются между отдельными узлами системы. Практически в таких системах разделяется только общий коммуникационный

канал между узлами системы. Производительность таких систем может увеличиваться путем добавления процессоров, объемов оперативной и внешней (дисковой) памяти в каждом узле, а также путем наращивания количества таких узлов.

Примерами систем параллельных баз данных являются продукты DBC (Teradata) и NonStop-SQL (Tandem), а также ряд прототипов, таких как BUBBA [Boral et al., 1990], EDS [EDS, 1990], GAMMA [DeWitt et al., 1990], GRACE [Fushimi et al., 1986], PRISMA [Apers et al., 1992] и ARBRE [Lorie et al., 1989].

Таким образом, среда для работы параллельной базы данных обладает двумя важными свойствами: высокой готовностью и высокой производительностью. В случае кластерной организации несколько компьютеров или узлов кластера работают с единой базой данных. В случае отказа одного из таких узлов оставшиеся узлы могут взять на себя задания, выполнявшиеся на отказавшем узле, не останавливая общий процесс работы с базой данных. Поскольку логически в каждом узле системы имеется образ базы данных, доступ к базе данных будет обеспечиваться до тех пор, пока в системе имеется по крайней мере один исправный узел. Производительность системы легко масштабируется, т.е. добавление дополнительных процессоров, объемов оперативной и дисковой памяти, и новых узлов в системе может выполняться в любое время, когда это действительно требуется.

Параллельные базы данных находят широкое применение в системах обработки транзакций в режиме on-line, системах поддержки принятия решений и часто используются при работе с критически важными для работы предприятий и организаций приложениями, которые эксплуатируются по 24 часа в сутки.

Выполнено в рамках ГПО КИБЭВС-0902 – «Инженерия баз данных».

ЛИТЕРАТУРА

1. Журнал «Системы управления базами данных». №4. 1996. Изд. дом «Открытые системы».

2. URL: http://wm-help.net/books-online/book/73690/73690.html (дата обращения: 03.03.2011).

ВЫБОР МЕТОДА АВТОРИЗАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ СЕТЬЮ

С.Ю. Исхаков, аспирант, А.Ю. Исхаков, студент 3-го курса

г. Томск, ТУСУР, каф. КИБЭВС, iskhakov90@mail.ru

В рамках разрабатываемой для ГОУ ВПО СибГМУ Минздравсоцразвития системы управления сетью (СУС) «Sowa» [1] появилась необходимость разграничения прав доступа пользователей.

Управление разрабатываемой СУС реализуется на базе Web-интерфейса. В качестве web-сервера используется Apache 2.2, интерпретатор PHP [2] подключается в виде модуля mod_php; данные хранятся в СУБД Mysql 5.5. Доступ к приложению осуществляется по протоколу HTTP [2], что обеспечивает распределенность системы и возможность использования графического интерфейса. Ключевым моментом в является выбор метода авторизации пользователей [3].

Сходство всех методов состоит в том, что пользователю требуется ввести его логин и пароль [3]. После успешной авторизации необходимо организовать способ передачи секретных данных между отдельными страницами. Ниже представлены варианты реализации хранения этих данных.

1. Авторизация с использованием cookies [4].

Данные пользователя для входа в систему хранятся у него на компьютере, поэтому нет возможности отслеживать возможные манипуляции с ними. Для функционирования требуются минимальные ресурсы сервера.

2. Авторизация с использованием механизма сессий [5].

Каждой сессии присваивается идентификатор, который указывает на данные пользователя, хранящиеся на сервере. Недостатком является необходимость значительных ресурсов оперативной памяти сервера при большом количестве работающих пользователей.

3. Авторизация средствами Web-сервера Apache.

В конфигурационных файлах Apache указывается имя файла, при наличии которого в той или иной папке Web-сервер выполнит по отношению к ней указания, содержащиеся в этом файле. Наиболее часто файл называется «.htaccess» [2].

4. Авторизация с помощью http-заголовков [4].

При входе в систему данные пользователя сохраняются в виде значений глобальных переменных, которые можно использовать в остальных сценариях страницы. Если данные не введены, странице не передаются никакие переменные. Данные посетителя хранятся до закрытия браузера.

Важным критерием для выбора способа авторизации была возможность выхода из учетной записи пользователя без необходимости закрытия браузера. Третий и четвертый методы из вышеперечисленных не предоставляют такой возможности.

Исходя из этого был выбран механизм авторизации с использованием сессий. В отличие от cookies пароли пользователей хранятся непосредственно на сервере, что является самой главной преградой для злоумышленника. Сессии тоже используют cookies браузера, однако значения переменных в cookies содержат лишь идентификатор сессии,

который генерируется PHP и представляет собой случайную строку из 32 символов.

Алгоритм генерации SID [5] позволяет гарантировать его уникальность, поэтому исключена возможность того, что две сессии будут иметь один и тот же идентификатор сессии. SID передается на сервер вместе с каждым запросом со стороны клиента и возвращается на компьютер клиента вместе с результатами обработки запроса. Его удаление происходит по окончании сессии.

Было установлено «время жизни» [5] каждой сессии – 10 мин. Если пользователь не проявляет активности в течение указанного времени, сессия считается недействительной – необходима повторная авторизация. Пример процедуры авторизации представлен на рис. 1.

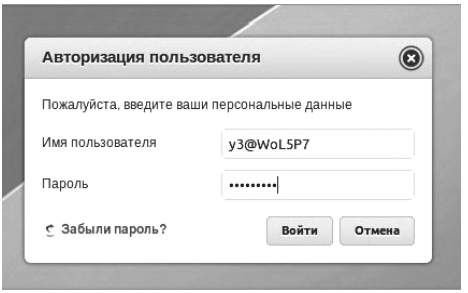


Рис. 1. Окно для ввода имени пользователя и пароля

Процедура авторизации выделена в отдельный модуль, который подключается к каждой странице системы управления сетью. Во избежание возможности прямого доступа к модулю, в листинге каждого php-файла первой строчкой присваивается определённая константа. При подключении блока авторизации происходит сравнения необходимого значения этой константы. Если злоумышленник попытается обратиться к модулю прямым указанием его адреса, работа скрипта будет приостановлена.

Для предотвращения возможных SQL-инъекций используется функция mysql_real_escape_string [2], экранирующая специальные символы в строках выражений SQL. Предварительно проводится проверка параметра magic_quotes_gpc. Чтобы избежать двойного экранирования применяется функция stripslashes [4].

Учётные записи пользователей хранятся в таблице базы данных, причём пароли содержатся не в открытом виде, а представляют собой хеш значение sha1 от строки содержащей имя пользователя, пароль и так называемую «соль» – некоторую последовательность символов. Пользователю присваивается определённый идентификатор класса доступа [3].

Для того чтобы разграничить доступ к элементам каждой страницы, всё содержимое каждого документа разбивается на блоки. Скрипт

блока обрабатывается только после успешной проверки его соответствия конкретной группе пользователей. Данное разграничение прав доступа является наиболее гибким для СУС, ввиду малого количества групп пользователей системы управления сетью.

Применение предложенного подхода описывает базовые элементы методов авторизации и учитывает лишь их основные уязвимости.

Выполнено в рамках проекта ГПО КИБЭВС-1002 – «Построение автоматизированной системы администрирования локально-вычислительных сетей».

ЛИТЕРАТУРА

1. *Исхаков С.Ю.* Анализ структуры сети учреждения здравоохранения: Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Научная сессия ТУСУР-2010», Томск, 4–7 мая 2010 г. Томск: В-Спектр, 2010. Ч. 3. С. 40–42.

2. *Колисниченко Д.Н.* PHP 5/6 и MySQL 6. Разработка Web-приложений. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2010. 560 с.

3. *Шелупанов А.А., Груздев С.Л., Нахаев Ю.С.* Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам: учеб. пособие для вузов. М.: Горячая линия – Телеком, 2009. 552 с.

4. *Орлов А.И.* Авторизация доступа [Электронный ресурс]. URL: http://www.xakep.ru/post/16586/default.asp.

5. *Грималовский А.* Сессии [Электронный ресурс]. URL: http://www.woweb.ru/publ/59-1-0-373.

ОЦЕНКА ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ В ИНФОРМАЦИОННОЙ СЕТИ ПРЕДПРИЯТИЯ

А.В. Иванова, студентка, С.В. Ширяев, аспирант каф. КСИБ
Научный руководитель С.К. Варлатая, проф., к.т.н.
г. Владивосток, ДВГТУ, ФИКТ, sk-varl@yandex.ru, anna.likia@gmail.com

Мероприятия по определению того, какие ресурсы корпоративной сети и от каких угроз необходимо их защищать, а также в какой степени те или иные ресурсы нуждаются в защите, инициализируются процедурой оценки рисков. Риск определяется вероятностью причинения ущерба, и его оценка состоит в том, чтобы выявить существующие угрозы и оценить их влияние на величину риска.

Как правило, уровень риска зависит от вероятности реализации определенной угрозы в отношении определенного объекта, а также от величины возможного ущерба.

На основе предлагаемой оценки вероятности рисков выбираются средства защиты, которые могут уменьшить или устранить идентифи-

цированный риск. Оценка величины рисков, выработка эффективных и экономичных мер их снижения, а также установление приемлемых рамок для них составляют суть процедуры управления рисками:

– оценка рисков существующей (создаваемой) системы информационной безопасности

– выбор эффективных управленческих, программно-аппаратных, экономичных решений.

Процесс управления рисками делится на следующие этапы: выбор анализируемых объектов, анализ угроз и их последствий. На основании проведенных мероприятий осуществляется выбор ответных мер и их реализация, производится оценка остаточного риска. В случае если остаточный риск слишком велик, происходит возврат к первоначальной итерации.

Основой построения системы защиты корпоративной сети является подробный анализ информационной системы предприятия с целью определения компонентов, подлежащих защите: сетевой инфраструктуры, представляющей собой рабочие станции пользователей; серверов; коммутаторов; маршрутизаторов.

Для управления процессом анализа рисков рекомендуется сгруппировать некоторые объекты информационной сети в более крупные структуры. Наибольшей угрозе безопасности подвергаются серверы, на которых хранится информация или которые предоставляют сети услуги контроллера домена, прокси-сервера и т.д.; рабочие станции; сетевая инфраструктура. Уровень угрозы для рассматриваемых структур сети рассчитывается путем перемножения показателей критичности и вероятности реализации угрозы для конкретной уязвимости [1].

Основным методом снижения риска является применение соответствующих средств защиты, выбор которых осуществляется по следующей методике:

– присвоение приоритетов действиям;

– оценка рекомендуемых вариантов защиты, т.е. анализ их осуществимости;

– анализ затрат и результатов;

– выбор средств защиты;

– разработка плана реализации средств защиты;

– применение выбранных средств защиты, которые могут уменьшить уровень риска.

Для устранения угроз используются методы, которые обладают оптимальным сочетанием цена/качество, либо закрывают одновременно несколько угроз. Например, уязвимость «невыполнение требований прикладного ПО к аппаратной конфигурации с учетом максимальной нагрузки» устраняется путем установки более производительных ком-

понентов или установки дополнительного сервера, который позволяет устранить уязвимость «не используется система балансировки сетевой нагрузки» и повысить надежность. Использование встроенных возможностей лицензионных программных средств (MS Outlook, Secure Disk) позволяет устранить уязвимости, связанные с криптографической защитой потоков информации и ЭЦП. Повышение эффективности, стабильности и безопасности функционирования сети обеспечивается рациональной системой подключения межсетевого экрана.

Применение средств защиты не гарантирует уничтожение риска, всегда остается какой-то уровень риска, называемый остаточным.

Оценка эффективности предложенных мер защиты корпоративной сети предприятия рассчитывается по формуле [2]:

$$E = (R - R_0)/R,$$

где R – уровень риска до применения средств защиты, а R_0 – уровень остаточного риска.

Как видно из таблицы, принятые меры защиты существенно снизили уровень рисков.

Сравнительная характеристика первоначального и остаточного рисков и значения эффективности

Объект защиты	Уровень угроз до снижения	Уровень угроз после снижения	Значение эффективности
Сервер	0,97	0,22	0,77
Рабочая станция	0,77	0,37	0,5
Сетевая инфраструктура	0,99	0,25	0,75

Таким образом, оценив уровни рисков для наиболее уязвимых структур корпоративной сети на основе предложенной методики снижения рисков, выбраны приоритеты защиты основных ресурсов, определены необходимые средства защиты и оценена эффективность их использования для корпоративной сети. Результаты анализа по предложенной методике могут использоваться в целях аудита для подготовки компании к сертификации по международным и российским стандартам.

ЛИТЕРАТУРА

1. ISO/IEC 27001:2005. Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC).

2. Digital Secure Office [Электронный ресурс]. Режим доступа: http://www.dsec.ru/about/articles/

ЗАЩИЩЕННЫЙ КАНАЛ СВЯЗИ

В.К. Карташов, В.И. Наханов, Э.Р. Старухина, А.А. Поляков, Д.В. Поляков, К.С. Рошкован, С.А. Рубанов, А.А. Межевалов, студенты

Научный руководитель Р.В. Мещеряков, доцент каф. КИБЭВС

г. Томск, ТУСУР, ФВС

Проект рассчитан на широкий круг пользователей, от простых людей, желающих обезопасить своё общение, до крупных организаций, которые обмениваются конфиденциальной информацией и нуждаются в данной защите.

Целью работы являются создание системы мгновенного обмена сообщениями и реализация механизмов защиты.

На начальном этапе работы были созданы тестовые приложения «клиент» – Homer, «сервер» – Achilles для более детального анализа механизмов передачи данных в компьютерных сетях на языке C++ [1, 2].

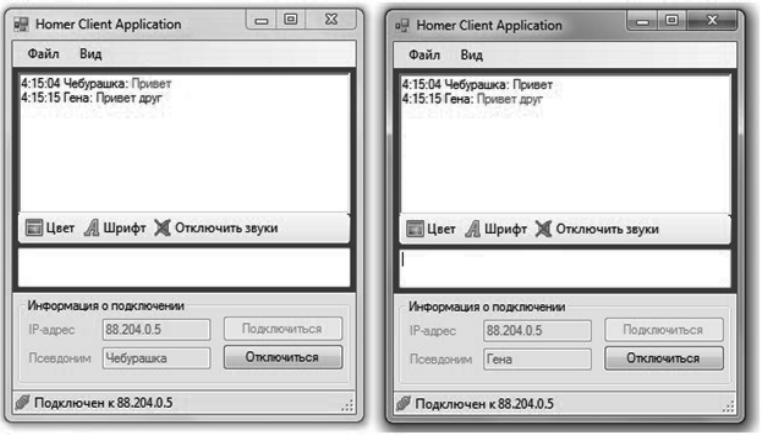


Рис. 1. Клиентское приложение Homer

С помощью программы – сетевого анализатора трафика (сниффера) был проведен анализ защищенности полученной системы, выявлены слабые места: возможность чтения, изменения сообщений посторонним лицом в ходе передачи их по линиям связи. На основе полученных результатов нами были определены необходимые механизмы обеспечения безопасности канала связи: аутентификация, шифрование, имитозащита сообщений.

В ходе выполнения работы в группе группового проектного обучения были исследованы существующие решения по защите канала

связи [3–5] что позволило выделить наиболее существенные угрозы каналу связи.

Спроектирована модель приложения для обмена сообщениями. Выбраны поддерживаемые протоколы мгновенной передачи текстовых сообщений (OSCAR, XMPP).

Предполагается, что следующим направлением будет использование приложения в качестве постоянного IM-клиента.

ЛИТЕРАТУРА

1. *Трей Н.* C# 2010: ускоренный курс для профессионалов. М., 2010. 587 с.

2. *Шилдт Г.* Полный справочник C#: Пер. с англ. М.: Изд. дом «Вильямс», 2004. 752 с.

3. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы технологии, протоколы: учеб. для вузов. СПб.: Питер, 2007. 960 с.

4. *Фергюсон Н., Шнайер Б.* Практическая криптография: Пер. с англ. М.: Изд. дом «Вильямс», 2005. 424 с.

5. Тестинг.ru URL: http://protesting.ru

РЕЧЕВОЙ КОРПУС ДЛЯ СИСТЕМ АНАЛИЗА И РАСПОЗНАВАНИЯ РЕЧИ

В.С. Хлебников, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, vovka_x@yandex.ru

В настоящее время на территории Российской Федерации ведется большое количество научных исследований, ориентированных на выявление параметров звуковых единиц русского языка. Исследованиям такого рода необходим базовый речевой материал для анализа, включающий в себя звуковые сигналы дикторов различного пола, возраста, диалектической принадлежности, а также детальное структурированное описание этих сигналов.

В данной статье приводится описание созданного речевого корпуса, удовлетворяющего потребности современных систем анализа и распознавания речи. Речевой корпус включает в себя речевые сигналы и базу данных, содержащую их структурированное описание, а также средства автоматической обработки, позволяющие пользователю вести поиск по определенным параметрам звуковых сигналов.

Процесс создания базы данных, содержащей описание речевого материала, подробно описан в [1], там же приведена ее структурная схема. Опишем лишь ключевые особенности созданной базы данных:

– возможность учета дикторов с дефектами речи, заболеваниями речевого тракта, акцентом;

– наличие дикторов различной диалектической принадлежности, возраста и пола;

– наличие сигналов с различной эмоциональной окраской;

– возможность пополнения созданного корпуса новыми сигналами;

– наличие ручной сегментации ряда речевых сигналов для контроля качества автоматической сегментации.

Отдельно необходимо описать процесс сбора речевого материала. Этот процесс состоит из 5 этапов: выбор дикторов, создание алфавита звуковых единиц, выбор речевых единиц, ручная сегментация части речевых единиц и занесение всей собранной информации в базу данных.

Вопрос выбора дикторов играет важную роль, необходимо достичь максимального разнообразия фонетических характеристик записываемых сигналов. К подбору дикторов были предъявлены следующие требования: наличие дикторов мужского и женского пола, наличие людей разных возрастных категорий, наличие дикторов с дефектами речи, наличие дикторов различной диалектической принадлежности. В соответствии с приведенными требованиями было отобрано 192 диктора.

Создание алфавита необходимо для того, чтобы различать типы звучания одного и того же базового звука, соответствующего букве русского языка. В данной работе разделение звуковых единиц на различные типы опирается на классификацию звуковых единиц, данной в научном труде [2]. Все звуковые единицы разделены на классы: гласные и согласные. Согласные звуки делятся на звонкие и мягкие. Гласные, в свою очередь, делятся на подклассы: ударные и безударные. Ударные гласные звуки делятся на 4 категории в зависимости от взаимного расположения с согласными звуками в слове. Классификация безударных гласных звуков более сложна. Во-первых, звучание безударных гласных зависит от мягкости предыдущего согласного звука, во-вторых, от положения безударной гласной относительно ударной гласной. В результате получается 5 типов звучания. Всего же алфавит содержит 76 звуковых единиц [3].

В качестве речевых единиц для анализа были выбраны фразы из художественной и научно-популярной литературы, а также пословицы и скороговорки. Критерием выбора являлось наличие каждого варианта звуковой единицы из разработанного алфавита как минимум в трех фразах. В дальнейшем фразы были транскрибированы на звуковые элементы разработанного звукового алфавита. Ниже приведен пример орфографической записи речевой единицы и ее транскрипции.

Орфографическая запись: корреспондент американской газеты Арчибальд Скайлс, проходя мимо, увидел стоявшую перед объявлени-

ем босую молодую женщину в ситцевом опрятном платье, – она читала, шевеля губами.

Транскрипция: (к)(ат2)(р’)(эм2)(с)(п)(ат1)(н)(д’)(Эмт)(н)(т)
(ат1)(м’)(эм2)(р’)(им1)(к)(Атт)(н)(с)(к)(ат2)(й’) (г)(ат1)(з’)(Эмт)(ы)
(ат1)(р)(ч’)(им1)(б)(Атм)(л’)(т) (с)(к)(Атм)(й’)(л)(с)
(п)(р)(ат2)(х)(ат1)(д’)(Амт) (м’)(Имт)(м)(ат2)
(ут1)(в’)(Имм)(д’)(эм3)(л) (с)(т)(ат1)(й’)(Амт)(ф)(ш)(ут2)(й’)(ум2)
(п’)(Эмм)(р’)(эм3)(т) (ат1)(б)(й’)(ам1)(в)(л’)(Эмм)(н’)(им2)(й’)(эм3)(м)
(б)(ат1)(с)(Утм)(й’)(ум2) (м)(ам2)(л)(ам1)(д)(Утм)(й’)(ум2)
(ж)(Этт)(н)(щ’)(им2)(н)(ут2) (ф) (с’)(Имт)(т)(ц)(эт2)(в)(ат2)(м)
(а)(п)(р’)(Амт)(т)(н)(ат2)(м) (п)(л)(Атм)(т’)(й’)(эм3) (ат1)(н)(Атт)
(ч’)(им1)(т)(Атт)(л)(ат2) (ш)(эт2)(в’)(эм1)(л’)(Амт)
(г)(ут1)(б)(Атм)(м’)(им2)

Системам автоматической сегментации речевого сигнала необходимы эталонные данные для контроля качества проведенной сегментации. Таким материалом могут быть результаты сегментации ряда сигналов, выполненные экспертом «вручную». Это означает, что эксперту необходимо прослушать сигнал и зафиксировать время начала и окончания каждой услышанной звуковой единицы. Для того чтобы выбрать речевые сигналы для ручной сегментации, было написано программное приложение, вычисляющее выборку с наименьшим количеством сигналов, содержащую каждую из единиц звукового алфавита как минимум 3 раза. Это было сделано для того, чтобы сегментированные экспертом речевые сигналы отвечали требованию полноты звуковых единиц. В результате было выбрано 7 речевых сигналов.

На данный момент речевой корпус продолжает наполняться, добавляются новые дикторы, речевые сигналы и их описание. Сейчас корпус содержит данные о 192 дикторах, 80 речевых единиц, около 1000 речевых сигналов суммарной длительностью более 7000 с, результаты ручной сегментации 103 речевых сигналов.

ЛИТЕРАТУРА

1. *Хлебников В.С., Черных Д.В.* Создание речевого корпуса для систем автоматического распознавания речи // Интеллектуальный потенциал XXI века: ступени познания: Сб. матер. IV Междунар. студенческой науч.-практ. конф.: в 2 ч. Ч. 2 / Под общ. ред. С.С. Чернова. Новосибирск: Изд-во НГТУ, 2010. 239 с.

2. *Буланин Л.Л.* Фонетика современного русского языка. М.: Высшая школа, 1970. 207 с.

3. *Хлебников В.С., Черных Д.В.* Выделение ключевых слов в слитной речи применительно к информационной безопасности // Научная сессия ТУСУР–2009: Матер. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых 12–15 мая 2009 г., Томск, Россия: В 5 ч. Ч. 3. Тематический выпуск «Системная интеграция и безопасность». Томск: В-Спектр, 2009. 392 с.

РЕАЛИЗАЦИЯ КРИПТОСИСТЕМЫ КЛЕТОЧНЫХ АВТОМАТОВ МЕТОДАМИ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ

Ю.В. Колесников, студент, О.О. Евсютин, аспирант
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, kolesnikov_yuri@hotmail.com

Высокая эффективность системы защиты информации достигается комплексным подходом к ее разработке, который заключается в сбалансированном сочетании разносторонних мер, средств и мероприятий [1]. Одним из важных компонентов комплексной системы защиты является криптография, основная задача которой – ограничение доступа к информации путем ее обратимого преобразования, исключающего прочтение посторонним лицом, то есть обеспечение конфиденциальности.

Существенная проблема криптографии состоит в том, что любой шифр подвержен анализу и с течением времени даже сильные шифры могут быть взломаны. В связи с этим постоянно остается актуальной разработка новых криптографических алгоритмов, и здесь достаточно перспективно выглядит применение клеточных автоматов, логика работы которых удачно накладывается на принцип построения симметричных блочных шифров.

Еще одна немаловажная проблема заключается в том, что использование сложных математических преобразований в процессе шифрования приводит к значительному замедлению системы, содержащей подсистему защиты информации. Из-за этого становится затруднительным применение криптографических методов в системах реального времени, например при потоковой обработке информации. Кроме того, криптографическая защита, внедренная в систему передачи информации, не должна оказывать заметного влияния на скорость информационного обмена и оставаться максимально незаметной для пользователей системы.

Возникла задача создать высокоскоростную криптосистему, в основе которой лежит математический аппарат клеточных автоматов. Поскольку клеточный автомат по определению является параллельной структурой, то программная реализация такой криптосистемы на машине с одним процессором не позволит достигнуть высокой скорости криптографических преобразований, однако ситуацию можно исправить с помощью методов параллельного программирования.

В качестве исходной была взята криптосистема на основе клеточного автомата на разбиении, который отличается от клеточных автоматов базового типа тем, что свойство однородности у клеточного автомата такого типа относится не к отдельно взятым клеткам, а к группам клеток, объединенных в блоки, и аналогичным образом меняется смысл понятий «окрестность» и «соседи».

Кроме того, для клеточного автомата на разбиении можно достаточно легко получать обратимые правила развития путем построения таблицы замен определенного вида, что является важным условием для построения алгоритма шифрования [2, 3].

Для программной реализации была выбрана библиотека OpenMP, использование которой позволяет организовать параллельное выполнение отдельных фрагментов программы, что положительно отразится на скорости выполнения криптографического преобразования.

OpenMP – это набор директив препроцессора, библиотечных процедур и переменных окружения, которые предназначены для программирования многопоточных приложений на многопроцессорных системах с единой памятью на языках C, C++ и Fortran. OpenMP реализует параллельные вычисления с помощью многопоточности, в которой главный (master) поток создает набор подчиненных (slave) потоков и задача распределяется между ними. Предполагается, что потоки выполняются параллельно на машине с несколькими процессорами (количество процессоров не обязательно должно быть больше или равно количеству потоков) [4].

В результате проделанной работы было создаано несколько вариантов параллельных алгоритмов, один из которых успешно реализован. Скорость шифрования криптосистемой увеличилась примерно в пять раз. Такого прироста скорости удалось достичь при помощи оптимизации доступа к файлу и выполнении функции криптопреобразования в двух потоках на двух ядрах процессора.

Достигнутые результаты позволяют продолжить работу над проектом. В перспективе следует модернизировать реализацию криптосистемы, используя другие методы высокопроизводительного программирования. Например, применив библиотеку MPI, которая тоже является стандартом в области многопоточного программирования. Еще одним возможным развитием проекта может быть разработка версии криптосистемы для распределенных вычислительных систем с помощью инновационного подхода к высокопроизводительным вычислениям. Кроме того, необходимо заняться более детальным исследованием криптостойкости алгоритма и, возможно, усилить его устойчивость к криптоаналитическим атакам.

Выполнено в рамках проекта ГПО КИБЭВС-0722 – «Криптосистемы клеточных автоматов».

ЛИТЕРАТУРА

1. *Мещеряков Р.В.* Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. Томск: В-Спектр, 2007. 278 с.

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

3. *Шалыто А., Наумов Л.* Клеточные автоматы – реализация и эксперименты [Электронный ресурс]. Режим доступа: http://www.osp.ru/pcworld/2003/08/166226/.

4. *Левин М.П.* Параллельное программирование с использованием OpenMP [Электронный ресурс]. Режим доступа: http://www.intuit.ru/department/se/openmp/.

ПРИЛОЖЕНИЕ ШИФРОВАНИЯ ДАННЫХ НА ПЛАТФОРМЕ ANDROID

С.Е. Кожевников, студент

Научный руководитель Ю.М. Филимонов, доцент, к.ф.-м.н.

г. Томск, ТУСУР, ФВС, kce@yandex.ru

Android – операционная система для мобильных телефонов, планшетных компьютеров, нетбуков и смартбуков, основанная на ядре Linux. В отличие от других современных мобильных платформ, Android сам по себе наиболее доступен и удобен для производителей, а главное – он нацелен на наиболее массовую аудиторию.

На данный момент Android является наиболее открытым, доступным, массовым и гибким игроком на рынке мобильных платформ – в этом и кроется главное преимущество Android над конкурентами. Благодаря своей открытости, Android легко может быть модифицирован конкретным производителем под свои нужды для конкретного устройства, а его интеграция с различными сервисами Google является образцово-показательной [1]. В отличие от значительной доли современных конкурентов, Android позволяет устанавливать сторонние приложения не только из фирменного магазина, но и из сторонних источников. При этом операционная система Android в стандарте поддерживает полноценную многозадачность, а ее функционал и поддержка различных технологий постоянно ширятся. С технической точки зрения, Android может похвастаться множеством правильных архитектурных решений, которые делают ОС более универсальной и совместимой с большим количеством различных устройств. При этом качество ОС и ее удобство пользования находятся на довольно-таки высоком уровне. Вполне очевидно, что, обладая таким широким спектром позитивных качеств и поддержкой такой компании как Google, платформа Android выглядит самой перспективной на рынке.

С большим развитием и использованием платформы Android повышается и потребность в приложениях для данной платформы. С

1 октября 2010 г. для жителей России появилась возможность выкладывать платные приложения в Android Market. Данное событие открыло большие возможности для разработчиков приложений в России.

Все больше людей приобретают устройства на платформе Android и используют их для своих целей, к таким целям относится и хранение информации, которую нужно скрыть от посторонних лиц, например фотографии, видео, текстовой документ и т. д.

Высокая перспективность развития платформы Android, а из этого следует и высокая перспективность развития рынка приложений для Android, в сочетании с потребностью пользователей в безопасном хранение информации, позволяет с полной уверенностью говорить о востребованности приложения шифрования данных на платформе Android.

После проведения обзора существующих аналогов и после сделанного анализа результатов этого обзора был выявлен ряд недостатков существующих приложений. Также было прочитано множество комментариев, сообщений и статей о том, что именно хотят пользователи от приложений шифрований данных и о причинах популярности одного приложения над другим, хотя их функциональность идентична. По результатам проделанной работы были выявлены ряд требований, которым должно соответствовать создаваемое прложение.

Стабильность работы

Стабильность приложения является важным качеством продукта. Хотя кажется, что это и так понятно и не нужно акцентировать на это сильное внимание, но обзор существующих приложений показал, что многие из разработчиков не уделяют должного внимания к данному моменту. Это приводит к ошибкам работы приложений, а данные приложения используют с целью защитить свою информацию, а при частых ошибках причиной потери информации может стать само приложение. И это становится основным моментом для отказа использования приложения данного типа.

Красивый дизайн и продуманность интерфейса

При изучении материалов описывающих причины большого количества использования одного продукта для Android по сравнению с другим, хотя их функциональность сильно не отличаются, опираясь на свой личный опыт, был сделан вывод, что хороший дизайн и удобство интерфейса сильно влияют на количество скачивания приложений. У многих рассмотренных приложений плохо продуман интерфейс. Неудобство использования приложения негативно влияет на количество пользователей, которые будут эксплуатировать данный продукт. По этим причинам нужно уделить особое внимание к продуманности и удобству интерфейса.

Алгоритм шифрования

Разрабатываемое приложение ориентировано на зарубежный и российский рынок. Поэтому было выбрано два алгоритма шифрование: ГОСТ 28147–89 и AES (Advanced Encryption Standard). ГОСТ 28147–89 алгоритм шифрования является российским стандартом симметричного шифрования, и он ориентирован на российский рынок. Advanced Encryption Standard – симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США. Алгоритм AES ориентирован на зарубежный рынок. Для удобства в приложение будет автоматически выставлены алгоритмы шифрования, в меню выбора алгоритма шифрования, в зависимости от выбранного языка. В программе будет реализовано два языка: английский и русский.

Благодаря проделанной работе были выявлены основные моменты, на которых нужно акцентировать внимание для того, чтобы получился продукт, удовлетворяющий потребности пользователей. Также были проведены подготовительные работы, включающие в себя установку и настройку среды разработки приложений для Android. В дальнейшем предполагаются работы по рассмотрению потребностей пользователей с целью реализации этих моментов в приложении.

ЛИТЕРАТУРА

1. Habrahabr: Режим доступа [Электронный ресурс]. URL: http://habrahabr.ru/blogs/android/105352/

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ ПРИ ПРОВЕДЕНИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Г. Краснов, А.С. Куракин, аспиранты каф. ПКС

г. Санкт-Петербург, Санкт-Петербургский государственный университет информационных технологий, механики и оптики

В настоящее время проблемы информационной безопасности (ИБ) имеют наивысший приоритет при организации информационного обмена, являющегося неотъемлемой частью жизнедеятельности каждой организации, ведущей электронный документооборот. Данная тенденция является следствием постоянного совершенствования средств автоматизации и роста их доступности. Все эти изменения упростили процессы копирования, распространения и использования информации, циркулирующей в информационных системах как частных, так и государственных организаций. В результате этого, опасность возникновения утечек значительно возросла, тем самым поставив роль аудита информационной безопасности на место одной из са-

мых первостепенных задач, особенно для корпоративных информационных систем (КИС). Данная задача для КИС в основном заключается в объективной оценке текущего состояния ИБ организации, а также ее адекватности поставленным целям и задачам бизнеса в части достижения цели по увеличению эффективности и рентабельности экономической деятельности организации.

Возможны два варианта аудита ИБ: аудит организации в целом и аудит только информационной системы. Нами будет рассмотрен аудит ИБ системы на основе анализа информационных рисков организации.

Подход на основе анализа информационных рисков организации является наиболее интересным и значимым для практики аудита безопасности. Это объясняется тем, что анализ риска позволяет эффективно управлять ИБ организации. Для этого в начале работ по анализу риска необходимо определить, что именно подлежит защите в организации, воздействию каких угроз это подвержено, и выработать рекомендации по практике защиты.

Анализ информационных рисков необходимо проводить исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера.

Для проведения анализа информационных рисков необходимо определить или адаптировать для конкретной организации:

– общую стратегию и тактику проведения атак потенциальным нарушителем;

– возможные способы проведения атак на систему обработки и защиты информации;

– сценарий осуществления деструктивных воздействий;

– характеристики каналов утечки информации и несанкционированного доступа;

– перечень возможных угроз;

– вероятности реализации угроз;

– способы применения и тактико-технические характеристики средств ведения технической разведки;

– модель нарушителя;

– методику оценки ИБ.

Кроме того, для построения надежной системы защиты информации организации необходимо:

– выявить все возможные угрозы безопасности информации;

– оценить последствия их проявления;

– определить необходимые меры и средства защиты с учетом требований нормативных документов, экономической целесообразности, совместимости и бесконфликтности с используемым программным обеспечением;

– оценить эффективность выбранных мер и средств защиты.

Степень ИБ определяется не только средствами и способами защиты, но и особенностями построения КИС. И при проектировании КИС в защищенном исполнении необходимо выбрать архитектуру (топологию) системы обработки информации, расположение средств обработки конфиденциальной информации, способы ее хранения и передачи таким образом, чтобы в значительной степени уменьшить количество мест доступа к информации.

Таким образом, варьируя варианты построения системы защиты информации и архитектуры КИС, становится возможным представить и рассмотреть различные значения суммарного риска за счет изменения вероятности реализации угроз. Здесь весьма важным шагом является выбор одного из вариантов в соответствии с выбранным критерием принятия решения. Таким критерием может быть допустимая величина риска или отношение затрат на обеспечение ИБ к остаточному риску.

После того как произведен анализ информационных рисков, проводится окончательная оценка мероприятий по обеспечению ИБ с подготовкой аудиторского отчета о защищенности информационных ресурсов. В аудиторский отчет включаются все материалы анализа рисков и рекомендации по их снижению.

Отметим, что анализ информационных рисков и оценка потерь при проведении аудита информационной безопасности требуют глубоких системных знаний и аналитического мышления во многих смежных областях проблемы защиты информации. В противном случае дать адекватную аудиторскую оценку о защищенности информационных ресурсов невозможно.

РАЗГРАНИЧЕНИЕ ФУНКЦИЙ ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ, ЗАДЕЙСТВОВАННЫХ В ЭКСПЛУАТАЦИИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ООО «ГАЗПРОМ ТРАНСГАЗ ТОМСК»

Д.В. Кручинин, студент 5-го курса, каф. КИБЭВС,
С.В. Кирсанов, зам. начальника отдела информационной безопасности СКЗ ООО «Газпром трансгаз Томск»
г. Томск, ТУСУР, kru_div@mail.ru

В настоящее время многие предприятия используют те или иные методы электронной обработки и обмена документами. Использование подобных систем позволяет значительно сократить время, затрачиваемое на оформление сделки и обмен документацией, усовершенство-

вать и удешевить процедуру подготовки, доставки, учета и хранения документов, построить корпоративную систему обмена документами. Для реализации подобного взаимодействия используются специальные структуры, удостоверяющие центры. Удостоверяющий центр предназначен для обеспечения участников корпоративных информационных систем средствами и спецификациями для использования сертификатов открытых ключей в целях обеспечения:

− применения электронной цифровой подписи;

− контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;

− аутентификации участников информационных систем в процессе взаимодействия;

− конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

В рамках обеспечения функционирования удостоверяющего центра возникает необходимость разграничения работ, связанных с настройкой, эксплуатацией средств криптографической защиты информации (далее – СКЗИ) и ключевых носителей, с обучением персонала и контрольно-инспекторской работы, направленной на обеспечение выполнения требований российского законодательства в области использования СКЗИ, по конфиденциальности информации.

С целью оптимизации технологического процесса необходимо наличие функциональных разграничений на уровне подразделений, задействованных в обеспечении функционирования удостоверяющего центра, при помощи организационных мер защиты информации. При этом целесообразно создание двух функциональных подразделений, ответственных за эксплуатацию и контроль.

Функции подразделения по эксплуатации заключаются в:

− обучении пользователей удостоверяющего центра правилам работы с СКЗИ и ключевыми носителями;

− проведении инженерно-технических мероприятий по инсталляции программного обеспечения СКЗИ, деинсталляция СКЗИ, проведение регламентных работ, разрешение нештатных ситуаций и прочие работы, связанные с эксплуатацией и настройкой СКЗИ;

− обеспечении надежной, бесперебойной эксплуатации программно-аппаратных средств, необходимых для работы пользователей удостоверяющего центра, в соответствии с требованиями технической и эксплуатационной документации;

− учете и контроле работы с СКЗИ и ключевыми документами.

Функции контрольно-инспекторского подразделения заключаются:

− в контроле своевременности и полноты проведения мероприятий по защите информационных ресурсов удостоверяющего центра (мониторинг журналов межсетевого экранирования, антивирусная защита, обновления программного обеспечения, резервное копирование и т.д.);

− в контроле соблюдения пользователями удостоверяющего центра требований и положений регламента удостоверяющего центра, другой нормативной документации по вопросам применения средств ЭЦП и шифрования;

− в контроле автоматизированных рабочих мест пользователей удостоверяющего центра;

− в организации и участии в работах по разбору конфликтных ситуаций;

− в разработке нормативно-методических документов по вопросам информационной безопасности, применения средств ЭЦП и шифрования.

С учетом описанных процедур становится возможным обеспечить полнофункциональную, более четкую и прозрачную работу удостоверяющего центра.

ЛИТЕРАТУРА

1. Эксплутационно-техническая документация штатных средств удостоверяющего центра: http://www.CryptoPro.ru

2. Методические рекомендации по организации работы органа криптографической защиты информации в ОАО «Газпром», его дочерних обществах и организациях.

КРИПТОСТОЙКОСТЬ РЕЖИМОВ ШИФРОВАНИЯ ГОСТ 28147–89, ОБЕСПЕЧИВАЮЩИХ КОНФИДЕНЦИАЛЬНОСТЬ ОБРАБАТЫВАЕМЫХ ДАННЫХ

И.А. Кукало, аспирант каф. РЗИ

г. Томск, ТУСУР, i@kukalo.ru

Отечественный алгоритм криптографического преобразования ГОСТ 28147–89 определен в стандарте [1] и является единственным алгоритмом симметричного шифрования, разрешенным к использованию на территории РФ. Этот стандарт определяет алгоритм шифрования $E: K \times \{0,1\}^{64} \to \{0,1\}^{64}$, три режима симметричного шифрования $SE = (\kappa, \varepsilon, D)$, с соответствующими уравнениями зашифрования ε и расшифрования D, а также режим выработки имитовставки. С момента

опубликования и перевода стандарта на английский язык, в отечественной и зарубежной литературе появилось большое количество работ, посвященных анализу криптостойкости алгоритма шифрования ГОСТ 28147–89 [2, 3]. Однако оценка криптостойкости режимов шифрования, определенных в стандарте, до настоящего времени не проводилась, хотя согласно [4] данная задача является актуальной для современной криптографии.

Основным показателем криптостойкости режимов шифрования согласно [5] является возможность неразличимости против атаки по выбранным открытым текстам (IND-CPA). Данный показатель ориентирован на практическую оценку безопасности режима шифрования [6] против конкретного злоумышленника, с ограниченными в использовании ресурсами.

Определим произвольную криптосхему $SE = (\kappa, \varepsilon, D)$ и злоумышленника A, который произвольно выбирает два сообщения одинаковой длины и передает их специальной подпрограмме-оракулу (ППО). Модель злоумышленника A определяется количеством запросов к ППО – σ и соответствует количеству блоков шифрования. ППО осуществляет шифрование одного из сообщений и передает зашифрованный текст злоумышленнику. Криптосхема считается безопасной, если злоумышленнику за приемлемое время не удается предсказать, какое из сообщений было зашифровано.

$$Adv_{SE}^{ind-cpa}(A) = \Pr[Exp_{SE}^{ind-cpa-1}(A)=1] - \Pr[Exp_{SE}^{ind-cpa-0}(A)=1], \quad (1)$$

где $Adv_{SE}^{ind-cpa}(A)$ – возможность злоумышленника A против атаки по выбранным открытым текстам (CPA); $\Pr[Exp_{SE}^{ind-cpa-1}(A)=1]$ – вероятность определения злоумышленником A номера сообщения 1 для ППО, которая шифрует сообщение 1; $\Pr[Exp_{SE}^{ind-cpa-0}(A)=1]$ – вероятность определения злоумышленником A номера сообщения 1 для ППО, которая шифрует сообщение 0.

Согласно формуле (1) это достигается при величине $Adv_{SE}^{ind-cpa}(A) \to 0$. В рамках данной работы были определены значения $Adv_{SE}^{ind-cpa}(A)$ для всех режимов работы ГОСТ 28147–89, обеспечивающих конфиденциальность информации. Теоретические результаты работы приведены в табл. 1.

Практические значения $Adv_{SE}^{ind-cpa}(A)$ для каждого из режимов шифрования приведены в табл. 2.

Таблица 1

Теоретические характеристики криптостойкости отечественных режимов шифрования

Название режима шифрования	Теоретическое значение $Adv_{SE}^{ind-cpa}(A)$
Простая замена	$Adv_{ECB[\text{GOST-89}]}^{ind-cpa}(A)=1$
Гаммирование	$Adv_{CTR_{gost}[\text{GOST-89}]}^{ind-cpa}(A)\le 2\cdot Adv_{\text{GOST-89}}^{prf}(B)+\frac{2\cdot\sigma^2}{2^{64}}$
Гаммирование с обратной связью	$Adv_{CFB_{gost}[\text{GOST-89}]}^{ind-cpa}(A)\le 2\cdot Adv_{\text{GOST-89}}^{prf}(B)+\frac{\sigma^2}{2^{64}}$

Таблица 2

Практические характеристики криптостойкости отечественных режимов шифрования

Название режима шифрования	Практическое значение $Adv_{SE}^{ind-cpa}(A)$	Значение σ, обеспечивающее криптостойкость
Простая замена	$Adv_{ECB[\text{GOST-89}]}^{ind-cpa}(A)=1$	$\sigma = 1$
Гаммирование	$Adv_{CTR_{gost}[\text{GOST-89}]}^{ind-cpa}(A)\le\frac{4\cdot\sigma^2}{2^{64}}$	$\sigma \le 2^{31}$
Гаммирование с обратной связью	$Adv_{CFB_{gost}[\text{GOST-89}]}^{ind-cpa}(A)\le\frac{3\cdot\sigma^2}{2^{64}}$	$\sigma \le 2^{31}$

Количество запросов злоумышленника к ППО позволяет определить продолжительность сессии защищенного обмена данными при использовании проколов [7, 8] в системах криптографической защиты информации. Согласно полученному значению σ:

- для режима простой замены безопасным является шифрование данных размером в один блок, т.е. 64 бит или 8 байт;
- для режима гаммирования безопасным является шифрование данных размером 2^{31} блоков, т.е. 17179869184 байт или 16,777216 Гбайт;
- для режима гаммирования с обратной связью безопасным является шифрование данных размером 2^{31} блоков, т.е. ≈19837604196 байт или ≈19,3726 Гбайт.

Таким образом, в работе выполнена оценка криптостойкости стандартных режимов шифрования на основе отечественного криптоалгоритма ГОСТ 28147–89 против атаки по выбранным открытым текстам. Для каждого режима определен размер данных, гарантирующий

сохранение конфиденциальности информации. Показано, что максимальный объем данных, который может быть зашифрован с помощью одного секретного ключа, зависит от значения $Adv_{SE}^{ind-cpa}(A)$ режима шифрования *SE*.

ЛИТЕРАТУРА

1. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введ. 01.07.90. М.: Государственный комитет СССР по стандартам: Изд-во стандартов, 1989. 28 с.

2. *Biryukov A.* Advanced Slide Attacks / A. Biryukov, D. Wagner. [Электронный ресурс] 2000. Режим доступа: http://now.cs.berkeley.edu/~daw/papers/advslide-ec00.ps

3. *Rudskoy M.* On zero practical significance of «Key recovery attack on full GOST block cipher with zero time and memory» [Electronic resource]. 2000. Режим доступа: http://eprint.iacr.org/2010/111.pdf

4. *Bellare M.* Introduction to Modern Cryptography/ M. Bellare, P. Rogaway [Электронный ресурс] .2005. Режим доступа: http://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf

5. *Goldwasser S.* Lecture Notes on Cryptography / S. Goldwasser, M. Bellare. [Электронный ресурс]. 2001. Режим доступа: http://cseweb.ucsd.edu/~mihir/papers/gb.html

6. *Bellare M.* Practice-oriented provable-security [Электронный ресурс] 1998. Режим доступа: http://cseweb.ucsd.edu/~mihir/papers/pops.pdf

7. Security Architecture for the Internet Protocol [Электронный ресурс]. Режим доступа: http://tools.ietf.org/html/rfc1825

8. The TLS Protocol [Электронный ресурс]. Режим доступа: http://www.rfc-editor.org/rfc/rfc2246.txt

ИССЛЕДОВАНИЕ УСПЕВАЕМОСТИ СТУДЕНТОВ МЕТОДОМ КЛАСТЕРНОГО АНАЛИЗА

Н.В. Кумушбаева, Е.В. Шмитько, студенты 4-го курса

г. Томск, ТУСУР, каф. КИБЭВС, madmasele@sibmail.com

Кластерный анализ – математическая процедура, позволяющая на основе схожести количественных значений нескольких признаков, свойственных каждому объекту (например, испытуемому) какого-либо множества, сгруппировать эти объекты в определенные классы, или кластеры. Задача кластеризации относится к статистической обработке, а также к широкому классу задач обучения без учителя [1].

Кластер – группа элементов, характеризуемых общим свойством, главная цель кластерного анализа – нахождение групп схожих объектов в выборке. Спектр применений кластерного анализа очень широк: его используют в археологии, медицине, психологии, химии, биоло-

гии, государственном управлении, филологии, антропологии, маркетинге, социологии и других дисциплинах.

Целью нашего исследования было разделение студентов третьего курса специальности «комплексное обеспечение информационной безопасности» на отдельные подгруппы в соответствии с их суммарным экзаменационным баллом за три года обучения. Работа осуществлялась с применением методов математической статистики. Результатом стало построение гистограммы распределения.

На первом этапе был построен вариационный ряд (данные располагаются в порядке возрастания варьирующего признака) (табл. 1), затем дискретный ряд (записываются те значения параметра, которые получаются при измерениях и подсчитывается их частота, по частотам вычисляются частотности) (табл. 2).

Таблица 1

Вариационный ряд

60	60	60	64	65	65	65
66	70	73	73	74	75	78
78	79	81	83	84	85	85
85	86	87	90	90	97	

Из табл. 1 видно, что самый низкий суммарный экзаменационный балл равен 60, самый высокий равен 97.

При построении интервального ряда выбор количества интервалов, при объеме выборки $n \leq 100$ рассчитывается по правилу Старджеса (табл. 3).

После выбора количества интервалов определяется ширина интервалов h путем деления размаха варьирования R на количество интервалов l.

Для построения гистограммы на каждом из интервалов, как на основании, строятся прямоугольники. Площадь каждого прямоугольника пропорциональна частоте или частности в соответствующем интервале. По оси ординат откладываются плотности распределения частот или частотностей. Общая площадь

Таблица 2

Дискретный ряд

Параметры	Частоты	Частотности
60	3	0,11
64	1	0,04
65	3	0,11
66	1	0,04
70	1	0,04
73	2	0,07
74	1	0,04
75	1	0,04
78	2	0,07
79	1	0,04
81	1	0,04
83	1	0,04
84	1	0,04
85	3	0,11
86	1	0,04
87	1	0,04
90	1	0,04
97	1	0,04

гистограммы для случая, когда по оси ординат откладывают относительную плотность распределения p_i/h_i, должна быть равна единице, поскольку площадь должна совпадать с суммой частотностей.

Таблица 3

Интервальный ряд

Интервал l	Границы a–b	Частоты	Частности	Накопленные частоты	Накопленные частотности
1	59,1–64,9	4	0,15	4	0,15
2	64,9–70,7	5	0,19	9	0,34
3	70,7–76,5	4	0,15	13	0,49
4	76,5–82,3	4	0,15	17	0,64
5	82,3–88,1	7	0,26	24	0,89
6	88,1–93,9	3	0,11	27	1

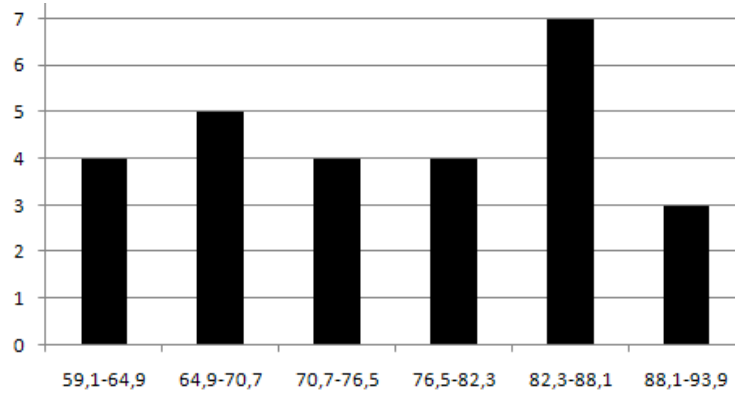


Рис. 1. Гистограмма

Исходя из рис. 1 видно, что в группу с баллами 82,3–88,1 входит наибольшее число учащихся.

Из результата проделанной работы можно заключить, что приемы статистической обработки подходят для использования в кластерном анализе при разделении студентов по подгруппам согласно их успеваемости. Однако нужно учитывать, что для более точной и наглядной картины гистограммы число испытуемых должно быть более ста человек.

ЛИТЕРАТУРА

1. *Гитис Л.Х.* Статистическая классификация и кластерный анализ. М.: Изд-во Моск. гос. горного ун-та, 2003. 157 с.

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ

А.А. Кускова, инженер, Р.В. Мещеряков, доцент, к.т.н.
г. Томск, ТУСУР, РКФ, каф. КИБЭВС, kaa@security.tomsk.ru

Развитие средств, методов и форм автоматизации процессов обработки информации привело к тому, что информационные технологии используются практически повсеместно, от некоторых информационных систем зависит благополучие, а иногда и жизнь многих людей. Этим обусловлен рост таких показателей, как объем передаваемой между участниками информационного обмена конфиденциальной информации, стоимость потери конфиденциальности, стоимость скрытого нарушения целостности, стоимость утраты информации. В связи с этим неуклонно растут актуальность и необходимость применения процедур оценки рисков информационной безопасности.

Современные подходы к анализу защищенности информационной системы, как правило, позволяют сделать временной срез, т.е. показывают текущее состояние. Но на практике все чаще встает вопрос о необходимости прогнозирования состояний информационной системы.

Определение состояний для будущих моментов времени на основании истории функционирования системы является основной задачей теории случайных процессов. Частным является случай, когда будущее состояние (X_{n+1}) зависит только от текущего состояния системы (X_n) и не зависит от остальных ранее пройденных состояний ($X_1, X_2, ..., X_{n-1}$). В таком случае говорят о цепи Маркова [1].

В каждый дискретный момент времени информационная система может быть либо в работоспособном состоянии (все её элементы функционируют нормально), либо реализуется одна из угроз информационной безопасности. Данные события представляют собой множество состояний процесса $X = \{x_i\}$.

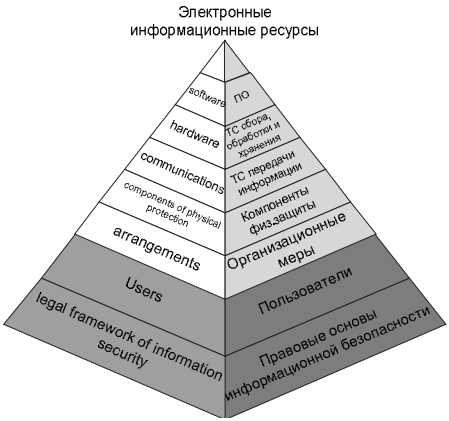


Рис. 1. Уровни защищенности электронных информационных ресурсов

Угрозы информационной безопасности можно условно разделить на 7 групп, которые представлены на рис. 1. Нарушение безопасности на одном из уровней может привести к реализации угрозы на вышестоящих уровнях.

Например, в случае потери сотрудником организации своего служебного пропуска может иметь место следующая цепочка событий (рис. 2) [2]:

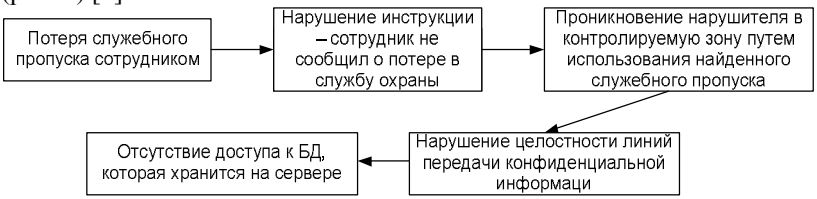


Рис. 2. Взаимосвязь реализации угроз безопасности разных уровней

Для моделирования будущего состояния системы задаются вероятности состояний цепи Маркова на начальном шаге:

$$a_i^{(0)} = P\{X_0 = i\}.$$

Также необходимым входным параметром является матрица переходных вероятностей марковского процесса, строки соответствуют текущему состоянию системы, а столбцы – состоянию на следующем шаге. На их пересечении стоят вероятности соответствующих переходов. Определение данных параметров осуществляется путем анкетирования экспертов.

На основании матрицы переходов строится граф переходов, представленный на рис. 3.

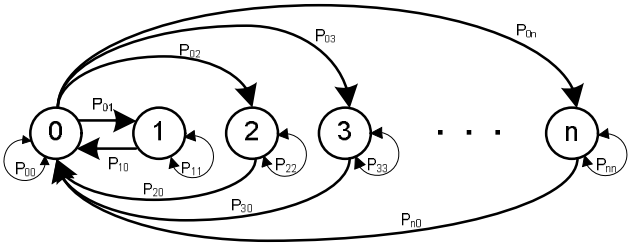


Рис. 3. Граф переходов

В случае оценки информационных рисков под интенсивностью потоков отказов (λ) будем понимать интенсивность реализации угрозы. Для расчета данной величины необходима статистика нарушений по каждой угрозе за определенный период (как правило, за месяц). Интенсивность реализации угрозы определяется как отношение количества реализаций угрозы за месяц к количеству часов (в среднем в месяце около 720 ч).

Алгоритм моделирования цепи Маркова:

Шаг 0. Выработать равномерно распределенное в интервале (0,1) случайное число R и определить состояние цепи Маркова X_0 в момент времени 0:

$$X_0 = \min\left\{t = 1,2,\ldots,k: R < a_1^{(0)} + a_2^{(0)} + \cdots + a_i^{(0)}\right\}.$$

Положить $i = X_0$, $t = 1$.

Шаг t=1, 2, .., n. Выработать равномерно распределенное в интервале (0,1) случайное число R и определить состояние цепи Маркова X_t на t-м шаге:

$$X_t = \min\left\{j = 1,2,\ldots,k: R < p_{i,1} + p_{i,2} + \cdots + p_{i,j}\right\}.$$

Положить $i = X_t$, $t = t + 1$.

На выходе данного алгоритма получается траектория цепи Маркова до n-го шага включительно.

Прогнозирование состояний информационной системы помогает своевременно предпринимать необходимые меры по предотвращению угроз информационной безопасности и по увеличению уровня защищенности тех или иных объектов защиты.

ЛИТЕРАТУРА

1. *Андронов А.М., Копытов Е.А., Гринглаз Л.Я.* Теория вероятностей и математическая статистика: учеб. для вузов. СПб.: Питер, 2004. С. 209–215.

2. IT-Grundschutz Catalogues 2005 // [Электронный ресурс]. Электрон. каталог. 2005. URL: http://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ download/it-grundschutz-cataloge_2005_pdf_en_zip (дата обращения: 18.02.2011).

РАЗРАБОТКА СИСТЕМЫ СКРЫТОЙ ОЦЕНКИ ПСИХОФИЗИОЛОГИЧЕСКОГО СОСТОЯНИЯ СУБЪЕКТА

Е.А. Левитская, аспирант, каф. ИБ

Научный руководитель Б.Н. Епифанцев, проф., д.т.н.

г. Омск, Сибирская государственная автомобильно-дорожная академия (СибАДИ), laska_kb@mail.ru

В настоящее время актуальна проблема скрытого контроля за психофизиологическим состоянием сотрудников, работающих с защищаемой информацией, с целью исключения доступа к информации, содержащей коммерческую тайну или имеющей гриф секретности, лиц в состоянии алкогольного или наркотического опьянения.

Особую сложность представляет выявление лиц, употребляющих такие наркотические вещества, как каннабиоиды (препараты, приготовленные из различных частей конопли, наиболее распространенные:

марихуана (смесь листьев, соцветия), гашиш (смолка, гашишное масло) [1]), так как в этом случае ярко выраженных признаков наркотического опьянения может не быть.

Решением данной проблемы может стать создание такой системы идентификации психофизиологического состояния сотрудника, которая при установлении факта нахождения каннабиоидных веществ в организме субъекта осуществляла бы подачу сигнала и «доведение» информации до администратора системы безопасности. Кроме того, система должна быть приемлемой, т.е. не должна вызывать чувство дискомфорта у людей.

С целью решения поставленной задачи достаточно установить содержание и концентрацию аммиака в выдыхаемом воздухе субъекта (содержание аммиака в выдыхаемом воздухе курильщика конопли в 40–60 раз превышает аналогичный показатель нормальных людей [2]), используя основные положения абсорбционной ИК-спектроскопии [3].

Суть предлагаемого способа заключается в следующем. В направлении лица субъекта осуществляются посылки импульсов оптического излучения на длине волны поглощения паров аммиака λ_{2u} и так называемой опорной к ней длине волны, т.е. длине волны, близкой, но не лежащей в полосе поглощения (например, $\lambda_{20} = 3$ мкм) [4].

Учитывая, что доля отраженного от лица человека излучения зависит от расстояния до субъекта и поглощения энергии при его распространении, предпочтительнее использовать в качестве λ_{2u} длину волны, равную 2,81 мкм, ввиду более мощной полосы поглощения и наличия в этом диапазоне «окна прозрачности» атмосферных газов [5].

Прежде чем определять непосредственно концентрацию аммиака требуется локализовать лицо субъекта, так как именно в направлении лица будет наибольшее скопление паров. С этой целью достаточно аналогичным образом обнаружить меланин. Для этого произвести посылки импульсов оптического излучения на длинах волн $\lambda_{10} = 1{,}08$ мкм и $\lambda_{1u} = 1{,}2$ мкм [6]. После локализации лица субъекта возможно проведение измерения концентрации аммиака в выдыхаемом человеком воздухе по закону Бугера–Ламберта.

Для уменьшения шумов в приемопередающих каналах каждая из принимаемых последовательностей отраженных сигналов суммируется и в соответствии с фундаментальным принципом теории борьбы с помехами отношение сигнал/помеха в благоприятном случае возрастает пропорционально $\sqrt{n}$, где n – число актов суммирования. Исследования по выбору оптимальной частоты счета и количеству актов суммирования показали, что при 50 актах суммирования и частоте 15 кГц достигается допустимая для решения прикладных задач величина погрешности.

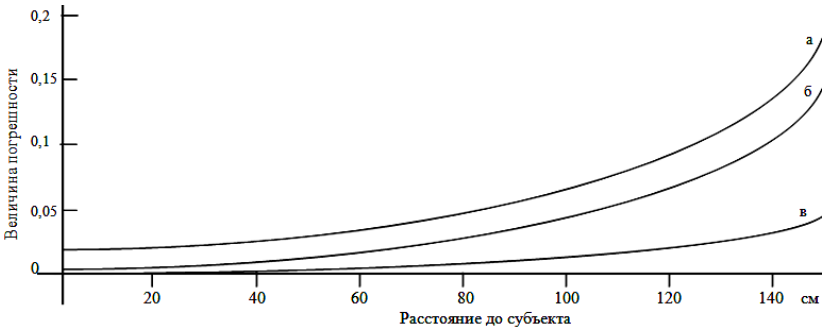


Рис. 1.Зависимость величины погрешности от расстояния: *а* – при 1 испытании; *б* – 5 испытаниях; *в* – 50 испытаниях

Реализация данного способа оценки концентрации наркотических веществ в выдыхаемом человеком воздухе предусматривает использование в качестве импульсных излучателей соответствующих длин волн излучательных диодов с их маскировкой другими подобными по виду «стекляшками» на панели дисплея оператора. При превышении концентрации аммиака допустимой для здорового человека нормы система осуществляет подачу сигнала и вывод информации на дисплей администратора системы безопасности.

На рис. 2 представлена блок-схема устройства, реализующего представленный способ скрытого дистанционного установления факта наличия наркотических веществ в организме субъекта.

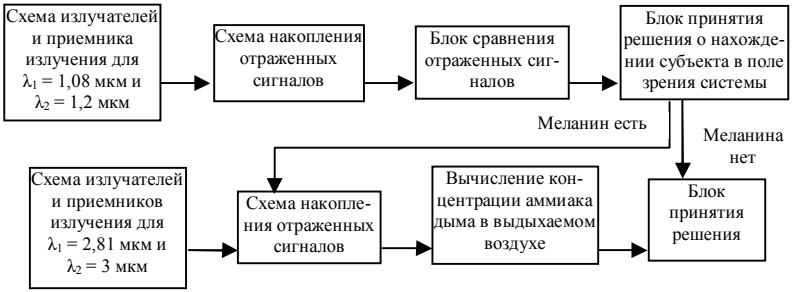


Рис. 2. Блок-схема работы устройства скрытой оценки психофизиологического состояния субъекта

ЛИТЕРАТУРА

1. Энциклопедия наркотических средств. Конопля [Электронный ресурс]. Режим доступа: http://narcotics.su/

2. *Moskalenko K.L., Nadezhdinskii A.I., Stepanov E.V.* Tunable diode laser spectroscopy applicatrion for ammonia and methane content measurements in hu-

man breath // Optical Sensing for Envi-ronmental Monitoring. Proc. SPIE. 1993. Vol. 2205. P. 448–452.

3. *Брицке М.Э.* Атомно-абсорбционный спектрохимический анализ (Методы аналитической химии). М.: Химия, 1982. 224 с.

4. NIST Chemistry WebBookhttp [Electronic resource]. Mode acess: http://webbook.nist.gov/

5. Прозрачность земной атмосферы[Электронный ресурс]. Режим доступа: http://www.astronet.ru/

6. *Пушкарева А.Е.* Методы математического моделирования в оптике биоткани: учеб. пособие. СПб.: СПбГУ ИТМО, 2008. 103 с.

ПРИМЕНЕНИЕ ТРИАНГУЛЯЦИИ ДЕЛОНЕ К ПРОЕКТИРОВАНИЮ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

А.В. Лисин, студент магистратуры

г. Омск, ОмГТУ, каф. ССИБ, andrey.lisin@gmail.com

Триангуляцией называют планарный граф, все внутренние области которого являются треугольниками [1]. Если для каждого треугольника в триангуляции выполняется условие, что любая точка, не принадлежащая этому треугольнику, находится вне описанной вокруг него окружности, то такая триангуляция называется триангуляцией Делоне.

Учитывая, что зона обзора камеры видеонаблюдения представляет собой треугольник при проецировании на плоскость, то видится логичным использование алгоритмов триангуляции для автоматизации нахождения вариантов покрытия охраняемых территорий видеонаблюдением, а некоторые свойства триангуляции Делоне делают её весьма привлекательной для подобного рода задачи.

В [2] описан алгоритм покрытия выпуклых тел плоскими углами, который может быть использован для случая, когда охраняемая территория является выпуклым телом. Его недостатками являются сложность разбиения невыпуклых тел на выпуклые и неоднозначность в случае наличия «запрещённых» участков на территории объекта. В общем случае эти проблемы могут быть решены с использованием различных эвристических алгоритмов, с помощью которых можно достигнуть удовлетворительного результата, однако сложность таких алгоритмов высока [3], а реализация требует значительных усилий. В противовес им триангуляция Делоне применима для любого вида тел, имеет невысокую трудоёмкость ($O(N\log N)$ [2]), а также хорошо детерминированные алгоритмы построения, удобные в реализации [2].

Треугольник зоны обзора видеокамеры однозначно определяется её фокусным расстоянием F и углом обзора α. Основной идеей алгоритма является поиск наиболее похожих на треугольники зон обзора видеокамер треугольников в построенной триангуляции. Критерием «похожести» может служить, например, величина площади пересечения двух треугольников при их совмещении вершинами таким образом, чтобы биссектриссы их углов совпадали (рис. 1). То есть необходимо найти $S_{\max} = \max\left(\{S_i\}\right)$, где S_i – площадь пересечения треугольника зоны обзора с *i*-м треугольником триангуляции. Важно заметить, что поскольку триангуляция Делоне на плоскости обладает минимальной суммой радиусов окружностей, описанных около треугольников, среди всех возможных триангуляций [1] это наличие в триангуляции множества треугольников, близких к равнобедренным, что соответствует равнобедренным треугольникам зон обзора.

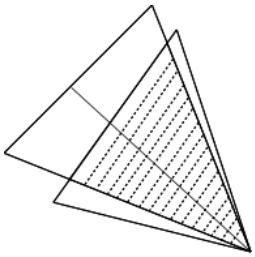


Рис. 1. Пересечение треугольников (заштрихованная область)

Итак, в упрощённом виде алгоритм покрытия охраняемой территории выглядит следующим образом:

1) выбираются сайты триангуляции, соответствующие точкам, где может быть произведён монтаж камеры видеонаблюдения;

2) по сайтам строится триангуляция Делоне;

3) среди набора зон обзора и треугольников, принадлежащих триангуляции, ищутся наиболее похожие пары и совмещаются;

4) в случае неудовлетворительных результатов производят новый выбор сайтов или устанавливают новые и переходят к шагу 2.

Данный алгоритм подходит для ситуации, когда вся охраняемая территория равнозначна и не содержит участков повышенной ответственности.

Представленный выше алгоритм покрытия может быть усовершенствован для случая неравнозначности охраняемой территории, т. е. для случая, когда в пределах охраняемой территории имеются участки повышенной ответственности, которые бы хотелось контролировать в первую очередь. В этом случае территория делится на участки произвольной формы, которым присваиваются весовые коэффициенты. Таким образом, участки с более высоким рейтингом покрываются в первую очередь.

Усовершенствованный алгоритм покрытия проделывает следующий шаги:

1) выбираются сайты триангуляции;

2) по выбранным сайтам строится триангуляция Делоне;

3) каждому треугольнику триангуляции приписывается вес, равный весу области, в которой он находится;

4) в случайном порядке выбираются треугольники с наибольшим весом, для каждого из них выбирается пара из треугольников зон обзора; та же операция последовательно проделывается для всех остальных весов в порядке убывания;

5) если количество треугольников покрытия равно нулю или вся территория покрыта, то конец алгоритма.

Для проверки работы предложенного алгоритма была разработана программа на языке C++. При её разработке был учтён опыт из [1], в качестве структуры хранения данных о триангуляции была использована структура «Узлы и треугольники», а в качестве алгоритма построения триангуляции Делоне использовался простой итеративный алгоритм. В качестве входных данных в программу подавались изображения из GIS-систем, на которых пользователю предоставлялась возможность расставить сайты. В ходе практических экспериментов были сделаны выводы о преимуществах и недостатках разработанного алгоритма.

Преимущества алгоритма:

– независимость от формы охраняемой территории;

– простота реализации.

Недостаток: сложность определения оптимальности полученного решения, т. к. поиск действительно оптимальной расстановки является сложной многовариантной задачей.

Алгоритм проявил себя наилучшим образом в условиях наличия больших возможностей в выборе расположения сайтов, например в условиях плотной застройки. В условиях же открытой местности качество покрытия было значительно худшим.

ЛИТЕРАТУРА

1. *Скворцов А.В.* Триангуляция Делоне и её применение. Томск: Изд-во Том- ун-та, 2002. 128 с.

2. *Лисин А.В.* Задача покрытия тела плоскими углами / А.В. Лисин, Р.Т. Файзуллин // Научная сессия ТУСУР–2010: Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых учёных: в 5 ч. Томск: В-Спектр, 2010. Ч. 3. С. 147–150.

3. *Еремеев А.В.* Задача о покрытии множества: сложность, алгоритмы, экспериментальные исследования / А.В. Еремеев, Л.А. Заозерская, А.А. Колоколов // Дискретный анализ и исследование операций. Омск: Изд-во Ин-та математики, 2000. С. 22–46.

МОДЕЛЬ ОПИСАНИЯ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И СОСТОЯНИЙ ПРИ ОРГАНИЗАЦИИ УПРАВЛЕНИЯ РАБОТЫ С НОСИТЕЛЕМ ИНФОРМАЦИИ

Е.В. Лялин, студент
г. Томск, ТУСУР, ФВС, zexqll@gmail.com

Оценивать опасность можно по-разному. Можно, например, ждать каких-либо проявлений угроз, оценивать эти проявления, определять пути ликвидации и ждать следующего проявления. Однако, этот вариант дорог и, по всей вероятности, вряд ли вызовет энтузиазм у собственников защищаемой информации. Можно попробовать учиться на чужих ошибках, но этот вариант не всегда сможет дать объективную картину. Самым разумным остается сначала представить все возможные варианты угроз, а затем отобрать наиболее применимые к конкретному случаю. Такая методология анализа и оценки возможностей реализации угроз информационной безопасности должна быть основана на построении модели угроз.

Модели угроз должны стать отправными точками для проектирования будущих систем защиты персональных данных операторами. Поэтому грамотно составленные модели угроз позволят адекватно защитить информацию [1]. Но чтобы приступить к составлению модели угроз, нужно описать все информационные процессы и состояния, которые происходят при работе с носителем информации.

Рис. 1. Информационные процессы и состояния при работе с носителем информации

В ходе работы была составлена модель организации управления работой с носителем информации. В ней есть состояния, в которых может находиться носитель:

1) зона работы с носителем;
2) хранилище;
3) доставка;
4) хранилище чистых носителей;
5) носители общедоступной информации,

а так же информационные процессы, которые могут возникать между этими состояниями:

1) выдача (из хранилища);
2) передача (на хранение);
3) отправка;
4) получение;
5) создание;
6) уничтожение;
7) нанесение реквизитов;
8) снятие реквизитов.

ЛИТЕРАТУРА

1. [Электронный ресурс]: Электрон. дан. Режим доступа: http://dsec.ru/products/grift/fulldesc/classification.

ОРГАНИЗАЦИОННАЯ ДОКУМЕНТАЦИЯ В ОБЛАСТИ БЕЗОПАСНОСТИ

Е.В. Максюта, студент
г. Томск, ТУСУР, ФВС, eu.max@yandex.ru

В основе организационных мер защиты информации лежат политики безопасности. В современной практике термин «политика безопасности» может употребляться как в широком, так и в узком смысле слова. В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению безопасности организации. В узком смысле под политикой безопасности обычно понимают локальный нормативный документ, определяющий требования безопасности, систему мер либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения безопасности. Примерами таких документов могут служить «Политика управления паролями», «Политика управления доступом к ресурсам корпоративной сети», «Политика обеспечения безопасности при взаимодействии с сетью Интернет» и т.п.

Разработка политик безопасности – длительный и трудоемкий процесс, требующий высокого профессионализма, отличного знания нормативной базы в области безопасности и, помимо всего прочего, писательского таланта. Этот процесс обычно занимает многие месяцы

и не всегда завершается успешно. Большинство организаций не располагают собственными людскими ресурсами, необходимыми для квалифицированной разработки и внедрения политик безопасности. Отыскать готовые политики безопасности, которые бы оказались применимыми в вашей организации, соответствовали бы ее структуре и требованиям безопасности, нереально. Несмотря на доступность соответствующих, в основном англоязычных, ресурсов в сети Интернет, они зачастую являются непригодными для практического использования [1].

Эти документы необходимы любой организации для разработки локальной нормативной базы в области информационной безопасности при внедрении системы управления информационной безопасностью, документировании процессов и требований безопасности, распределении ролей и назначении ответственных за безопасность.

Целью работы является составление набора шаблонов типовых организационно-распорядительных документов, которые могут использоваться для разработки локальной нормативной базы организации в области информационной безопасности (политик, инструкций, стандартов, и т.п.), и обоснование достаточности этих документов для обеспечения безопасности.

В результате была проделана работа, включающая в себя анализ интернета на наличие всех уже имеющихся инструкций и политик безопасности. Были найдены: 31 инструкция и политика по информационной безопасности; 26 инструкций персонала по работе с тем или иным объектом, а также были найдены 49 должностных инструкций.

Так как было найдено очень много различных документов направленных в одну и ту же область, например политик по парольной защите было 9 разных видов, были сделано объединение всех этих документов в соответствующие группы. После этого, в каждой группе был создан документ (политика ИБ, инструкции и т.п.), объединяющий в себе всё группу.

Затем в каждом таком общем документе распределили все пункты по трём критериям: создание, изменение, удаление. Это было необходимо, чтобы систематизировать работу по составлению шаблонов документов.

Также были созданы шаблоны по составлению политик безопасности и должностных инструкций.

В итоге была разработана схема возможных событий происходящих с сотрудником. Разработаны частные случаи этой схемы, и комплекты организационной документации в области безопасности для каждого.

ЛИТЕРАТУРА

1. [Электронный ресурс] / «Чтиво». Электрон. дан. Режим доступа: http://www.4tivo.com/inf_tech/271-normativnye-dokumenty-i-instrukcii-po.html

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОГО ИНФИЦИРОВАНИЯ БОЛЬШОЙ СИСТЕМЫ

В.В. Макаров, М.А. Маслов
Научный руководитель Ю.М. Филимонов, доцент, к.ф.-м.н.
г. Томск, ТУСУР, labilis1@gmail.com

Глобальные проблемы, стоящие перед человечеством, весьма многочисленны и разнообразны. И каждая конкретная проблема имеет конкретную причину своего появления. Возникают новые проблемы, которые также имеют конкретную причину своего появления.

Одним из возможных подходов к единому пониманию стоящих перед человечеством проблем является рассмотрение каждой проблемы как состоящей из множества взаимосвязанных элементов, т.е. как системы.

В настоящее время существует немало математических методов исследования систем [1]. Однако рассматриваемые системы имеют ряд особенностей, которые затрудняют или даже делают невозможным применение существующих методов исследования.

Первая особенность – высокая размерность исследуемых систем. Каждая из этих систем и вся совокупность проблем в целом описывается большим числом различных показателей, что позволяет говорить о них как о больших системах.

Большая система – комплекс большого количества взаимосвязанных и взаимодействующих между собой элементов. Образуя особое единство, она обеспечивает выполнение сложных функций.

Большой системе присущи четыре характерных качества.

Первое: любая большая система представляет собой сложнейший комплекс взаимосвязанных элементов.

Второе: любая большая система образует собой единство с внешней средой.

Третье: любая большая система представляет собой элемент системы более высокого порядка.

Четвертое: элементы, составляющие большую систему, выступают как системы более низкого порядка.

Теория больших систем формулирует определенные закономерности и принципы, общие для самых различных областей деятельности.

В ходе работы была смоделирована система следующего вида. Предполагаем, что существует большая система P, называемая популяцией, каждый элемент которой назовем особью o_i. Особь характеризуется двумя показателями: агрессии a_i и лояльности l_i. Эти показатели связаны соотношением

$$l_i + a_i = 1 .$$

Каждая особь, входящая в систему P, способна взаимодействовать с любым числом других особей, входящих в систему P, в любой момент времени t_j. При взаимодействии особей a_i и a_k показатель агрессивности у менее агрессивной особи увеличится следующим образом:

$$a_{t_{j+1}} = a_{t_j} + e^{a_i - a_k}.$$

Показатель агрессивности более агрессивной особи на данном уровне абстракции не изменяется при встрече.

В рамках системы только особи посредством взаимодействий влияют друг на друга, это значит, что среда изначально не несет в себе никакой функциональной составляющей. Исходя из этого рассуждения, следует все функции и условия влияния особью и на особь переместить непосредственно на особь.

После этого появляется возможность несколько дифференцировать популяцию. Например, разумной кажется мысль, что все особи на момент начала эксперимента имеют различные показатели агрессивности. Также видится существенным, что небольшая доля особей может быть крайне агрессивна или крайне лояльна изначально. Некоторые особи могут гораздо слабее поддаваться влиянию других особей. С другой стороны, некоторые особи могут, напротив, влиять гораздо сильнее прочих. Сила влияния особи может изменяться со временем, имитируя нечто вроде авторитета или же доверия.

Итак, далее предполагаем у модели особи наличие следующих составляющих:

1. a – коэффициент агрессивности.
2. r – коэффициент резистивности.
3. v – коэффициент влиятельности.

Предполагаем, что коэффициенты резистивности, агрессивности и влиятельности у всех особей на момент начала эксперимента разные. Однако стоит рассмотреть различные законы распределения псевдослучайных величин, назначаемых этим коэффициентам, и проведение всей полной группы экспериментов с различными законами распределения.

Стоит рассмотреть несколько моделей опыта:

– все особи изначально нейтральны;

– все особи изначально агрессивны более, чем лояльны;

– все особи изначально лояльны более, чем агрессивны;

– смешанный состав популяции.

Результирующие данные по всем экспериментам необходимо сопоставить и сравнить для возможности выработки дальнейших предположений и усложнений модели популяции.

Были проведены эксперименты в достаточном для накопления большого количества статистических данных количестве и подтверждены теоретические предположения о поведении модели.

В работе выполняется моделирование процесса информационного инфицирования сложной системы. Для этого приняли для начальных экспериментов простую абстрактную модель элементарных взаимодействий элементов внутри системы, постепенно усложняя модель исходя из различных соображений и различных предпосылок.

Впоследствии планируется продолжать расширять данную модель и усложнять механизмы влияния особей друг на друга внутри популяции для достижения большего приближения к реальным механизмам постепенного информационного инфицирования больших систем.

ЛИТЕРАТУРА

1. *Прангишвили И.В.* Системный подход и общесистемные закономерности. М.: СИНТЕГ, 2000. 528 с.

ДЕКОМПИЛЯЦИЯ И ИЗУЧЕНИЕ ПРОГРАММЫ

А.Е. Малахов, студент 5-го курса
Научный руководитель Е.М. Давыдова, доцент
г. Томск, ТУСУР, каф. КИБЭВС, malahov.alexander@gmail.com

Обфускация – одно из средств защиты программ, но не стоит забывать, как пишет Крис Касперский [1], что обфускация была создана хакерами. Хакеры, как и защитники, активно используют различные алгоритмы обфускации и при этом цели, как и у защитников, так и хакеров одинаковые, и те и другие хотят защитить свою программу от изучения. Только в отличие от защитников, хакеры используют обфускацию для своих вредоносных программ, в том числе и вирусов. В результате очень сложно обнаружить измененный вирус и еще сложнее понять, как он устроен, а это необходимо для создания эффективной защиты от этого вируса.

Все средства исследования ПО разделяют на 2 класса: статические и динамические. Статические средства обрабатывают исполняемый файл программы и строят ее алгоритм без ее исполнения. Динамические средства, в отличие от статических средств, изучают и составляют алгоритм во время ее исполнения и могут построить алгоритм программы только на основании ее конкретной трассы. Можно сказать, что статические средства более мощные, в том смысле, что теоретически могут получить алгоритм всей программы, даже те блоки, которые никогда не выполняются.

Для получения максимально возможного полного алгоритма программы используют статические и динамические средства как дополнение друг друга. При отсутствии каких-то частей программы после статического изучения чаще всего возможно получение этих частей программы динамическими средствами путем прохода по той трассе с теми параметрами, которые требуются.

Можно выделить два средства, наиболее применяемые для изучения – дизассемблеры и отладчики.

Дизассемблеры относятся к статическим средствам и применяются при отсутствии исходных кодов программы. На вход подают исполняемый файл программы и на выходе получают исходный код программы на языке Ассемблера. Для перевода программы на более высокий язык программирования применяются трансляторы или дискомпиляторы.

Отладчики очень часто используются разработчиками для отладки своих программ. Они могут быть применены и для отладки программы при ее модификации без исходных кодов.

Применяются также и трассировщики, которые в свою очередь сначала запоминают каждую инструкцию, проходящую через процессор, а затем переводят набор инструкций в форму, удобную для статического исследования, автоматически выделяя циклы, подпрограммы.

Также активно используют следящие системы, позволяющие получить дополнительную информацию о программе, такие как вызываемые API, обращение к реестру, запись/чтение файлов и вызов библиотек.

Подробнее об инструментах исследования написано в источнике [2].

В некоторых случаях возможно использование декомпиляторов, если не применялась обфускация на низком уровне, иначе декомпилятор либо не сможет выполнить декомпиляцию, либо выдаст совершенно не тот код.

После получения исходного кода программы деобфускация может занять огромное количество времени.

Один из способов уменьшить время на деобфускацию – это получить исходный код с помощью трассировщика. Он откинет тот мусор, который никогда не выполняется.

Дальше изучение необходимо проводить с помощью дополнительных программ, таких как ollydbg, IDA Prof.

IDA Prof – мощный дизассемблер. Отдельно стоит выделить, что он позволяет написать собственные скрипты, что в свою очередь расширяет его возможности и позволит автоматизировать рутинную работу.

Ollydbg –удобный отладчик, но не такой мощный, как SoftICE. Можно выделить то, что он позволяет работать с ассемблерным кодом

программы до ее запуска. Позволяет запустить и проверить внесенные изменения, выставляя точки останова.

Несмотря на мощность применяемых инструментов, все же остается проблема деобфускации из-за неизвестности применяемого алгоритма обфускации. Полностью получить чистый код не получится, на это может быть затрачено слишком много времени.

ЛИТЕРАТУРА

1. *Касперский К.* Обфускация и ее преодоление [Электронный ресурс]. URL: http://www.xakep.ru/magazine/xs/066/008/1.asp (дата обращения: 02.03.2011).

2. *Касперский К.*, *Рокко Е.* Искусство дизассемблирования. СПб: БВХ-Петербург, 2008. 892 с.

ОБФУСКАЦИЯ ИСХОДНОГО КОДА ПРОГРАММЫ

А.Е. Малахов, студент 5-го курса

Научный руководитель Е.М. Давыдова, доцент

г. Томск, ТУСУР, каф. КИБЭВС, malahov.alexander@gmail.com

В настоящее время актуальным вопросом становится защита программ от изучения. Создается множество программ, которые так или иначе защищены от нелегального использования. При всей мощности использования элементы защиты не позволяют добиться нужного результата, и со временем разработчики сталкиваются с тем, что в их программах удаляют те части, которые отвечают за защиту от не легального использования, или же попросту заменяют на ту часть, которая известна злоумышленнику.

Как указано в статье 1280 п. 3 Гражданского кодекса РФ, «лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст». Соответственно, пользователь может изучать логику программы по полученному исходному коду. После декомпиляции пользователь может копировать, удалять или изменять часть программного кода для своих целей, конечно же, это уже будет незаконно, но доказать, что эта часть исходного кода скопирована именно из вашей программы, крайне сложно или даже невозможно. Обфускация программы позволяет запутать исходные коды, значительно усложнив изучение программы.

Простые запутыватели удаляют таблицы символов и отладочную информацию из скомпилированных классов и заменяют исходные имена методов бессмысленными короткими именами.

Более сложные программы используют преобразования графа потока управления программы и её структур данных.

Применяемые методы при обфускации выделяют в три большие группы:

1) лексическая обфускация;
2) обфускация данных;
3) обфускация хранения.

Отдельно выносят метод превентивной обфускации, который предназначен для предотвращения применения злоумышленником деобфускаторов, декомпиляторов и остальных программных средств деобфускации. Но, как объясняет Крис Касперский в статье [1], такой способ противодействия может спровоцировать пользователя на применение отладочных средств, с целью удаления данных способов защиты.

Лексическая обфускация наиболее простая, заключается в форматировании кода программы, изменении его структуры, таким образом, чтобы он стал нечитабельным, менее информативным и трудным для изучения.

Обфускация данных, связанная с трансформацией структур данных, считается более сложной, является наиболее продвинутой и часто используемой и делится на следующие группы:

1) обфускация хранения – заключается в трансформации хранилищ данных, а также самих типов данных;

2) обфускация соединения – заключается в усложнении представления используемых программой структур данных;

3) обфускация разделения переменных;

4) обфускация переупорядочивания – заключается в изменении последовательности объявления переменных, внутреннего расположения хранилищ данных, а также переупорядочивании методов, массивов.

Обфускация управления осуществляет запутывание потока управления, т.е. последовательности выполнения программного кода. В свою очередь делится на следующие группы:

1) использование устойчивых непрозрачных предикатов;

2) обфускация вычисления – заключается в изменении главной структуры потока управления;

3) обфускация соединения – заключается в объединении или разделении определенных фрагментов кода программы, для того чтобы убрать логические связи между ними;

4) обфускация последовательности – заключается в переупорядочивании блоков (инструкций переходов), циклов, выражений.

Более подробно об обфускации можно ознакомиться в источнике [2].

Также остро встает вопрос о целесообразности применения того или иного метода обфускации. Для обоснования выбора методов об-

фускации, в последующем ее реализации был использован метод анализа иерархий Саати [3].

Метод основан на декомпозиции задачи и представлении ее в виде иерархической структуры, что позволяет включить в иерархию все имеющиеся у лица, принимающего решение, знания по решаемой проблеме и последующей обработке суждений лиц, принимающих решения. В результате может быть выявлена относительная степень взаимодействия элементов в иерархии, которые затем выражаются численно. Метод анализа иерархий включает процедуры синтеза множественных суждений, получения приоритетности критериев и нахождения альтернативных решений.

В результате было определено, что применяемые алгоритмы можно разделить на 4 группы, а именно:

1) самый легкий алгоритм, в поле которого происходит минимальное увеличение размера программы и мало влияет на производительность защищаемой программы;

2) алгоритм, который умеренно влияет на увеличение размера защищаемой программы и мало влияет на производительность защищаемой программы;

3) полный алгоритм, который значительно влияет на увеличение размера защищаемой программы и умеренно влияет на производительность защищаемой программы;

4) алгоритм высокой защиты, который очень сильно влияет на увеличение размера защищаемой программы и умеренно влияет на производительность защищаемой программы.

Выбор правильного алгоритма влияет не только на степень защищённости программы, но и на ее производительность, соответственно не стоит применять алгоритм с высокой защищенностью для критичных в производительности программ.

ЛИТЕРАТУРА

1. *Касперский К.* TOP10 ошибок защитников программ [Электронный ресурс]. URL: http://www.insidepro.com/kk/078/ 078r.shtml (дата обращения: 28.02.2011).

2. *Чернов А.В.* Анализ запутывающих преобразований программ // Тр. Ин-та системного программирования РАН, 2003.

3. *Саати Т.Л.* Принятие решения при зависимостях и обратных связях: Пер. с англ. / Науч. ред. А.В Андрейчиков, О.Н. Андрейчикова. М.: ЛКИ, 2008. 360 с.

СХЕМА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ, ПРОИСХОДЯЩИХ С ИНФОРМАЦИЕЙ И ЕЁ НОСИТЕЛЯМИ

И.С. Мельников, студент
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, xwiz@gmail.com

В современных условиях информация может иметь гораздо более высокую ценность, чем материальные вещи. Утечка информации для любого предприятия может иметь весьма негативные последствия, начиная от небольших финансовых затрат и заканчивая полным развалом этого предприятия. Для того чтобы обезопасить информацию, работающую с ней технику и персонал, необходимо строить систему защиты. Самым лучшим вариантом будет та система защиты, которая обеспечивает уровень защиты, соответствующий статусу информации, и при этом не имеет избыточных, возможно, весьма дорогостоящих средств. Чтобы построить такую систему, необходимо изучить все возможные варианты угроз, а затем отобрать наиболее применимые к конкретному случаю. Такая методология анализа и оценки возможностей реализации угроз информационной безопасности должна быть основана на построении модели угроз.

Построение собственной модели угроз будет происходить на основе схемы информационных процессов, так как это позволит получить удобную классификацию, охватывающую самый широкий спектр угроз.

В ходе работы была составлена схема информационных процессов, происходящих с информацией и ее носителями. В схеме отображены переходы, объекты и преобразователи в следующих средах:

1) виртуальная среда – визуальная среда;
2) виртуальная среда – акустическая среда;
3) акустическая среда – среда сигналов;
4) визуальная среда – среда сигналов;
5) виртуальная среда – среда сигналов;
6) визуальная среда – визуальная среда;
7) среда акустики – среда акустики;
8) виртуальная среда – виртуальная среда;
9) среда сигналов – среда сигналов.

Описание переходов информации между виртуальной и визуальной средой:

1) носитель в виртуальной среде.

Объекты: файл, БД, адресное пространство;

2) носитель в визуальной среде.

Объекты: человек;

3) информационное состояние – преобразователь 1.

Объекты: устройства вывода (монитор, принтер);

4) информационное состояние – преобразователь 2.

Объекты: устройства ввода (клавиатура, мышь, сканер, цифровая камера).

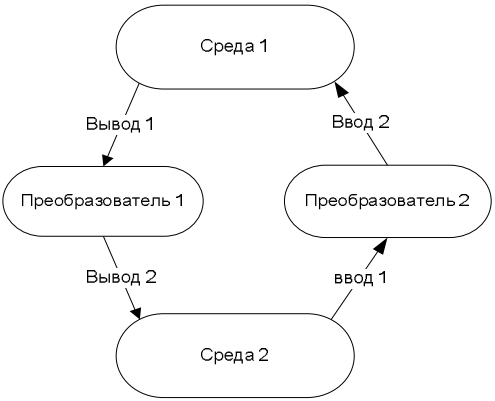


Рис. 1. Типовая схема информационных процессов, происходящих между двумя средами

Описание переходов информации между виртуальной и акустической средой:

1) носитель в виртуальной среде.

Объекты: файл, БД, адресное пространство;

2) носитель в акустической среде.

Объекты: человек;

3) информационное состояние – Преобразователь 1.

Объекты: устройства вывода (динамик);

4) информационное состояние – преобразователь 2.

объекты: устройства ввода (цифровые устройства с микрофонами, вибродатчиками, гидроакустическими датчиками).

В ходе выполнения преддипломной практики была получена схема информационных процессов, происходящих с информацией и ее носителями, описаны объекты и преобразователи, с которыми будет идти работа при построении модели угроз.

МОДЕЛЬ ПРОГРАММНОГО ПРОТИВОДЕЙСТВИЯ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛАМ ПЭМИ

Ю.А. Михайлов, аспирант каф. информационной безопасности

Научный руководитель А.А. Захаров, проф., д.т.н.

г. Тюмень, ИМиКН ТюмГУ, windym@rambler.ru

Побочное электромагнитное излучение (ПЭМИ) – один из возможных каналов утечки информации. ПЭМИ излучают все устройства компьютера, в том числе и периферийные, которые служат своеобразными антеннами, увеличивающими радиус излучения.

Все существующие методы борьбы с утечкой информации по каналам ПЭМИ можно разделить на две группы: активные и пассивные.

К активным методам относятся аппаратные средства – генераторы шума, которые излучают сигнал, создающий помехи для приема сигнала от ПЭМИ. Данные способы защиты информации рассмотрены в статье [1]. Такие устройства требуют точной настройки, систематического обслуживания и контроля их эффективности во всем радиусе излучения. Кроме этого, данные устройства являются дополнительными источниками излучения, что негативно сказывается на здоровье сотрудников. Также данные устройства обладают демаскирующим эффектом, так как применение генераторов шума сигнализирует злоумышленникам о наличии секретной информации и о применяемых способах защиты.

К пассивным методам относятся экранирование и расположение рабочего места относительно стен, дверей и окон. Метод экранирования позволяет существенно снизить излучение, исходящее от ЭВМ, однако экранировать абсолютно все части компьютера либо невозможно, либо способ экранирования будет являться не самым оптимальным. Кроме этого, применение экранов может снизить эргономику рабочего места, а также остается вероятность утечки информации через перехват отраженного светового излучения от устройств вывода видеоизображения. При этом не рассматриваются способы контроля параметров вывода изображения на современных мониторах, а продолжаются попытки снижения ПЭМИ от мониторов, основанных на технологии ЭЛТ [2], применение которых в настоящее время крайне редко, особенно в системах обработки секретной информации.

Анализируя существующие методы защиты информации от утечки по каналам ПЭМИ, можно выделить основные их недостатки: стоимость приобретения и содержания, необходимость в обслуживании, демаскирующий эффект, их постоянное действие без адаптации под технические особенности современных средств вывода видеоизображения и изменяющиеся внешние условия, отсутствие зависимости типа обрабатываемой информации от устройств защиты, невозможность дистанционного управления. Большинство этих проблем вызвано отсутствием взаимодействия между источником излучения и средствами защиты от излучения.

За основу программного противодействия утечки информации по каналам ПЭМИ предполагается взять два метода, которые можно рассматривать как имитацию существующих активных и пассивных способов защиты. Это программный метод снижения ПЭМИ от устройств вывода видеоизображения и программный метод генерирования шумов.

В основе работы программного метода снижения ПЭМИ от устройств вывода видеоизображения будет реализация возможности изменять показатели излучения в зависимости от типа обрабатываемой

информации, технических особенностей подключенного устройства вывода и изменяющихся параметров освещенности в течение рабочего дня. В результате постоянного контроля и изменения параметров видеосигнала появится возможность поддерживать минимально допустимый уровень светового излучения монитора, что будет способствовать снижению уровня ПЭМИ. Кроме снижения вероятности утечки информации по каналам ПЭМИ, применение данного метода позволит сохранять комфортные условия рабочего места в течение дня, а также за счет снижения уровня излучения снизить энергопотребление, что приведет к положительному экономическому и экологическому эффекту.

За основу методики адаптации параметров видеоизображения предполагается взять зависимость минимально допустимых параметров видеосигнала от типа выводимой информации и от типа устройства вывода информации. Данная зависимость будет получена в результате опытов по измерению уровня излучения от современных устройств вывода видеоизображения. За основу методики расчета и измерения уровня излучения взята статья [3]. При проведении опытов необходимо учесть конструктивные особенности современных устройств вывода видеоизображения для получения соответствующих коэффициентов. Одним из параметров, который можно контролировать на программном уровне, – это яркость пикселя. Яркость (L) каждого пикселя определяется по формуле

$$L = B + xC,$$

где B – параметр, настроенный на мониторе, C – уровень контрастности, x – параметр, передаваемый с компьютера.

Из формулы видно, что яркость пикселя не зависит только от сигнала, передаваемого с компьютера, а получается с учетом собственных настроек на устройстве вывода. Поэтому в передаваемом сигнале необходимо учесть такие параметры, как полученный экспериментально коэффициент для каждого типа устройств вывода (Sk), корректирующий коэффициент (Kk), который отражает тип выводимой информации, и рабочий коэффициент (Wk), отражающий изменения освещенности в течение рабочего дня. В итоге значение x будет рассчитываться по формуле

$$X = X \times Sk \times Kk \times Wk,$$

Корректирующий коэффициент (Kk) зависит от типа выводимой информации. Так, например, в случае если на монитор выводится текстовая информация, то данный коэффициент будет ниже, чем в случае, когда на монитор выводится графическая информация. Рабочий коэффициент (Wk) – параметр, изменяющийся в течение рабочего дня, изависит от типа используемого освещения, для расчета данного коэффи-

циента необходим алгоритм, отражающий его изменение в течение дня.

Работа программного обеспечения по данному методу приведет к снижению уровня ПЭМИ и светового излучения от работающей ЭВМ, данный эффект будет подобен эффекту экранирования, который снижает уровень ПЭМИ.

В процессе работы ЭВМ излучает ПЭМИ, которое может являться каналом утечки информации. Методы перехвата информации по таким каналам хорошо известны и активно используются, но у этих методов был один важный недостаток – это необходимость в ожидании вывода на монитор компьютера или другое периферийное устройство необходимой информации. Однако данный недостаток был решен с помощью программы-вируса, которая ищет необходимую информацию в памяти компьютера и путем обращения к различным устройствам компьютера вызывает появление побочных излучений, в которые вставляет свои сообщения с требуемой злоумышленникам информацией. Если на программном уровне можно генерировать канал ПЭМИ и осуществлять по нему передачу необходимой информации, то на программном уровне можно бороться с потенциально-информативными каналами ЭМИ путем генерирования сигналов, аналогичных сигналам, излучаемым генераторами шума. При этом данный метод генерирования шумов будет лишен ряда недостатков, которые присутствуют при использовании аппаратных генераторов шума. Это снижение демаскирующего эффекта за счет того что источником помех является то же оборудование, что и источник потенциально-информативных сигналов. В ряде случаев не постоянное генерирование шумов, а только когда идет обращение к устройству, вызывающему ПЭМИ.

Таким образом, модель программного противодействия утечки информации по каналам ПЭМИ будет состоять из метода снижения уровня излучения за счет адаптации параметров видеоизображения под текущие условия работы и из метода генерирования шумов на программном уровне, путем обращения к различным устройствам компьютера, имитируя, таким образом, работу генератора шума. Применение программного обеспечения, которое будет работать по данным методам, позволит снизить затраты на обеспечение информационной безопасности, снизить вероятность утечки информации по каналам ПЭМИ и улучшить качество рабочих мест.

ЛИТЕРАТУРА

1. *Иванов В.П., Залогин Н.Н.* Побочные электромагнитные излучения электронной вычислительной техники и их маскировка. Защита информации // INSIDE. 2010. №1.

2. *Семакова Л.М., Ситникова С.В.* Побочные электромагнитные излучения видеомонитора персональной ЭВМ, ПГУТИ, Самара: Спецвыпуск T-Comm. 2009. август.

3. *Шелупанов А.А., Зайцев А.П.* Оценка ПЭМИ электронных устройств // Доклады ТУСУРа. 2008. № 2 (18), ч. 1, июнь.

ТРЕБОВАНИЯ К СИСТЕМАМ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ЮРИДИЧЕСКИ ЗНАЧИМОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ ТОНКОГО КЛИЕНТА

Н.С. Михайлов, аспирант, В.Д. Зыков, инженер

Научный руководитель А.А. Шелупанов, зав. каф. КИБЭВС, проф., д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, dem@ms.tusur.ru

В настоящее время активно развиваются сервисы, основанные на технологии тонких веб-клиентов. Эти технологии существенно повышают простоту использования. Они позволяют конечным пользователям применять всегда актуальную версию сервиса и не требуют дополнительного программного обеспечения, за исключением интернет-браузера.

При использовании данных технологий в областях, связанных с повышенными финансовыми, репутационными и информационными рисками (системы интернет-банкинга, системы электронных торгов, порталы государственных услуг, системы сдачи электронной отчётности через Интернет), остро встают вопросы информационной безопасности. Необходимо обеспечивать:

– целостность и конфиденциальность информации, передаваемой по открытым каналам связи;

– строгую аутентификацию участников информационного обмена (клиента и сервера);

– аутентичность передаваемой информации.

На стороне клиента должно использоваться минимум программного обеспечения, драйверов, служебных сервисов и пр., установка и последующая работа с которыми может вызвать неудобства у клиента. В первую очередь, речь идёт о средствах криптографической защиты информации (СКЗИ), драйверах для устройств хранения ключевой информации, системах подключаемых модулей и элементов управления в браузерах.

Данное требование в первую очередь влияет на выбор системы защиты информации. Существующие программные СКЗИ не позволяют решать эту задачу. Перспективной альтернативой являются отчуж-

даемые СКЗИ в виде USB-брелка или смарт-карты с аппаратной реализацией криптографических алгоритмов. Они работают посредством драйверов стандартного класса USB-устройств – USBCCID (IntegratedCircuit(s) CardInterfaceDevice). Драйвер данного класса USB-устройств присутствует во всех современных операционных системах: Windows Vista и выше, Linux, Mac OS [1].

Современные браузеры построены таким образом, что веб-страницы и скрипты выполняются в некоторой изолированной среде. Это не позволяет содержимому веб-страницы получить доступ к данным пользователя, а также блокирует несанкционированное использование программного и аппаратного обеспечения компьютера.

Но для использования в рамках веб-приложения криптографических возможностей СКЗИ, как программного или программно-аппаратного, так и отчуждаемого, необходимо получить доступ к вычислительным возможностям компьютера из контекста браузера. Это позволяет сделать технология подключаемых модулей (Plugin, плагин).

В этом случае веб-страница получает доступ к функциям подключаемого модуля, работающего в контексте браузера, который, в свою очередь, как и любое программное обеспечение, имеет доступ к программным и аппаратным возможностям компьютера.

Основная проблема в том, что различные браузеры используют разные API (Application Program Inter-face) для подключения плагинов. На сегодняшний момент нет однозначно доминирующего браузера. Кроме того, при создании плагина необходимо учитывать используемую операционную систему, что приводит к необходимости создания большого количества плагинов для различных операционных систем и браузеров.

Решением может стать разработка набора плагинов для современных распространенных браузеров (Microsoft Internet Explorer, Firefox, Opera, Google Chrome, Safari). Все плагины должны иметь одинаковый интерфейс для веб-станиц, позволяющий работать с отчуждаемыми СКЗИ из контекста веб-страницы посредством языка написания сценариев JavaScript.

Это позволит разработчикам веб-ориентированных систем создавать веб-страницы, которые могут использовать все возможности СКЗИ, независимо от используемого браузера и операционной системы.

Принимая во внимание приведенные выше ограничения, единственным выходом становится проведение процедуры аутентификации из контекста веб-страницы. С использованием плагина веб-сервер имеет возможность провести строгую двухфакторную аутентификацию пользователя с помощью технологий электронной цифровой подписи

и, в случае необходимости, инфраструктуры открытых ключей (Public Key Infrastructure).

На рис. 1 приведена упрощенная схема взаимодействия сервера и клиента, использующего отчуждаемое СКЗИ.

Существует несколько протоколов аутентификации, основанных на использовании криптографии с асимметричными ключами, но наиболее полно эта процедура описана в протоколе SSH (Secure Shell) [2].

Рис. 1. Схема взаимодействия клиента и сервера

Поэтому строгую двухфакторную аутентификацию клиента сервером и сервера клиентом было решено производить на основе асимметричной криптографии с использованием «российских» алгоритмов на основе протокола SSH. Это позволяет при создании прикладных систем реализовать защищенную двухфакторную аутентификацию (наличие USB-брелока и знание пароля к нему) пользователя с последующим предоставлением ему определенных полномочий.

Так как «закрытие» канала информационного обмена при помощи SSL/TLS на отечественных алгоритмах в общем случае невозможно, то все передаваемые в канал данные необходимо защищать с помощью криптографических преобразований для обеспечения целостности и конфиденциальности.

С помощью плагина можно создавать зашифрованные и подписанные сообщения в формате CMS (PKCS#7), которые после формирования передаются в канал передачи данных. Формат CMS позволяет контролировать целостность (путем постановки/проверки ЭЦП) и конфиденциальность (путем шифрования) передаваемых данных с использованием «российских» криптографических алгоритмов.

Дополнительно сам канал может быть «закрыт» стандартными средствами браузера и сервера: односторонним или двусторонним SSL/TLS на «западных» алгоритмах, что позволит дополнительно аутентифицировать сервер и защитить канал передачи.

Аутентичность информации в веб-приложениях обеспечивается использованием ЭЦП, которая вырабатывается в отчуждаемом СКЗИ посредством вызовов из веб-страницы через плагин к браузеру. СКЗИ также позволяет производить проверку ЭЦП, подтверждая на стороне клиента аутентичность сообщений и данных от сервера.

СКЗИ, реализуя алгоритм генерации/проверки электронной цифровой подписи ГОСТ Р 34.10–2001, позволяет удостоверять волеизъявления пользователя, придавая им юридическую значимость, что необходимо при создании таких систем юридически значимого документооборота, как дистанционное банковское обслуживание, документооборот с органами государственной власти и т.д.

ЛИТЕРАТУРА

1. Microsoft Class Drivers for USB CCID Smart Cards [Электронный ресурс]. URL:http://msdn.microsoft.com/en-us/windows/hardware/gg487509 (дата обращения: 25.02.2011).

2. RFC 4252. The Secure Shell (SSH) Authentication Protocol [Электронный ресурс]. URL: http://tools.ietf.org/html/rfc4252 (дата обращения: 02.03.2011).

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ЮРИДИЧЕСКИ ЗНАЧИМОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ ТОНКОГО КЛИЕНТА

Н.С. Михайлов, аспирант

Научный руководитель А.А. Шелупанов, проф., д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, dem@ms.tusur.ru

В системах электронного юридически значимого документооборота в связи с повышенными финансовыми, репутационными и информационными рисками остро встают проблемы информационной безопасности. Необходимо обеспечивать конфиденциальность, целостность и аутентичность передаваемой информации, а также строгую аутентификацию участников обмена.

Современные программные средства, в том числе и интернет-браузеры, позволяют решать эти задачи при помощи уже ставших стандартными средств:

– целостность и конфиденциальность обеспечивается «закрытием» канала средствами протоколов SSL/TLS;

– аутентификация участников обмена также обеспечивается SSL/TLS в процессе установки соединения;

– аутентичность передаваемой информации обычно подтверждается электронной цифровой подписью (ЭЦП) [1], которая генерируется перед отправкой информации другой стороне.

Современные браузеры имеют различную архитектуру, но в каждом из них предусмотрена поддержка криптографических протоколов SSL/TLS. Указанные протоколы обеспечивает строгую аутентификацию клиента и сервера по цифровым сертификатам, а также целост-

ность и конфиденциальность при обмене информацией. Реализации современных браузеров ориентированы на западные криптографические алгоритмы (обычно RSA и AES), в то время как для обеспечения юридической значимости и защиты конфиденциальной информации на территории Российской Федерации требуется использовать реализованные в сертифицированных средствах криптографической защиты информации (СКЗИ) отечественные алгоритмы [2].

Некоторым браузерам (например, Microsoft Internet Explorer) для использования отечественных алгоритмов достаточно установки сертифицированного СКЗИ, другим требуется дополнительная установка специализированных программ или вмешательство в исходный код браузера.

Возникает потребность в создании решения, которое бы удовлетворяло требованиям «легкости» и безопасности для клиента:

− не используется ничего, кроме браузера, привычного для пользователя;

− должна быть обеспечена целостность и конфиденциальность передаваемой информации, строгая аутентификация участников обмена, аутентичность передаваемой информации.

Современные СКЗИ, реализующие отечественные криптографические алгоритмы, можно разделить на 2 класса:

1) встраиваемые в систему (например, программные или программно-аппаратные криптопровайдеры);

2) отчуждаемые (работающие во время непосредственного подключения к компьютеру).

Встраиваемые в систему СКЗИ требуют установки, в процессе которой происходит тесная их интеграция с операционной системой, что влечет за собой обязательное наличие прав администратора. К тому же установка требует дополнительных знаний и умений у пользователя.

Современные отчуждаемые СКЗИ, такие как USB-токены с аппаратной реализацией криптографических алгоритмов, работают посредством драйверов стандартного класса USB-устройств – USBCCID (IntegratedCircuit(s) CardInterfaceDevice). Драйвер данного класса USB-устройств присутствует во всех современных операционных системах: Windows Vista и выше, Linux, Mac OS.

Это позволяет путем вызова USB-токена или смарт-карты из контекста браузера использовать их криптографические возможности без установки дополнительного программного обеспечения или драйверов.

Стоит учесть, что в системах, где используются программные СКЗИ, также актуален вопрос сохранения в тайне закрытого ключа ЭЦП. Существуют риски компрометации закрытого ключа путём его хищения с памяти ключевого носителя или оперативной памяти, поскольку программные СКЗИ для совершения криптографических опе-

раций считывают закрытый ключ в оперативную память. Именно в этот момент программная закладка может получить доступ к закрытому ключу пользователя.

Решением данной проблемы может являться использование отчуждаемых СКЗИ, выступающих также в качестве средства хранения ключевой информации. Реализацией такого отчуждаемого СКЗИ является eToken ГОСТ производства компании «Аладдин Р.Д.». Данный продукт выполняется в форм-факторе USB-ключа или смарт-карты и реализует алгоритмы ГОСТ Р 34.10–2001, ГОСТ Р 34.11–94 и позволяет начать работу сразу после подключения к компьютеру [3].

Закрытый ключ генерируется внутри устройства и никогда не покидает его памяти. Все операции по генерации/проверке ЭЦП и выработке сеансовых ключей шифрования производятся внутри eToken ГОСТ.

ЛИТЕРАТУРА

1. Федеральный закон от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи» (в ред. Федерального закона от 08.11.2007 № 258-ФЗ).

2. *Ильиных Е.В., Козлова М.Н.* Комментарий к ФЗ «Об электронной цифровой подписи» // Юстицинформ. 2005. С. 45–52.

3. *Афанасьев А.А., Веденьев Л.Т., Воронцов А.А.* Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам // М.: Горячая Линия-Телеком, 2009. С. 125–142.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В БАНКОВСКИХ СИСТЕМАХ РОССИЙСКОЙ ФЕДЕРАЦИИ

В.Г. Миронова, аспирантка

г. Томск, ТУСУР, каф. КИБЭВС, mvg@security.tomsk.ru

Разработка отраслевых стандартов, целью которых является обеспечение безопасности персональных данных, является необходимостью, с которой столкнулось большинство организаций различных отраслей.

Согласно [2] информация, отнесенная к сведениям, составляющим коммерческую тайну, служебную тайну, персональные данные и т.д. являются конфиденциальной информацией, порядок доступа к которой ограничен федеральными законами.

Существует ряд стандартов, разработанных на основании нормативно-методической документации Федеральной службы по техническому и экспертному контролю (ФСТЭК) России, Федеральной службы безопасности (ФСБ) России и внутренних документов, принятых в организации.

ФСТЭК России разработаны базовые нормативно-методические документы, которые предполагают типовой подход к решению проблемы обеспечения безопасности персональных данных (ПДн) и другой конфиденциальной информации. Поэтому существует необходимость разработки стандарта определенной отрасли предприятий, который позволит быстро и эффективно защитить конфиденциальную информацию. Сегодня существует ряд таких отраслевых стандартов, например, отраслевой стандарт для учреждений здравоохранения, труда и занятости населения, для учреждений, оказывающих услуги связи, для банковских структур и т.д.

Один из индивидуальных подходов обеспечения безопасности ПДн представлен в отраслевом стандарте Банка России. В соответствии с действующим стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее – СТО БР ИББС-1.0) модель угроз и нарушителей должна быть основным инструментом организации банковской системы Российской Федерации (БС РФ) при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности.

Существует ряд различий методических рекомендаций ФСТЭК России и отраслевого стандарта БС РФ, часть из которых представлена в таблице.

Различия рекомендаций ФСТЭК России и БС РФ

	Стандарт Банка России	Методические рекомендации ФСТЭК России
1	2	3
1	«Угроза безопасности персональных данных – угроза нарушения свойств безопасности персональных данных – доступности, целостности или конфиденциальности персональных данных организации БС РФ» [1]	«Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных» [3]
2	«Актуальная угроза безопасности ПДн – угроза безопасности ПДн, риск реализации которой не является допустимым для организации БС РФ по результатам проведения оценки рисков нарушения безопасности ПДн, обрабатываемых в ИСПДн» [1]	«Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн. Подход к составлению перечня актуальных угроз состоит в следующем» [3]

Продолжение таблицы

1	2	3
3	Для оценки степени соответствия информационной безопасности (ИБ) организации требованиям СТО БР ИББС–1.0 используются групповые и частные показатели ИБ. Оценка $EVM_{i.j}$ частного показателя формируется на основании выявленной аудиторской группой степени выполнения требований посредством экспертного оценивания. Для частных показателей, выполнение которых обязательно, устанавливается следующая шкала степени их выполнения: «нет», «частично», «да». Для частных показателей, выполнение которых рекомендуется, устанавливается следующая шкала степени их выполнения: «да», «нет». При этом необходимо выполнить процедуру нормировки коэффициентов значимости оставшихся частных показателей ИБ в рамках группового показателя. Оценка группового показателя (EV_{Mi}), за исключением группового показателя М9 «Общие требования по обработке персональных данных в организации БС РФ», вычисляется из оценок входящих в него частных показателей ($EV_{Mi.j}$) с учетом коэффициентов значимости $\alpha_{i.j}$, определяющих важность частного показателя для оценивания группового показателя: $$EV_{Mi} = \sum_{j} \alpha_{i.j} \cdot EV_{Mi.j} \ .$$ При формировании коэффициентов значимости учитывалось следующее условие нормировки: $$\sum_{j=1}^{k} \alpha_{ij} = 1 \ ,$$ где k – число частных показателей в i-м групповом показателе	Исходная степень защищенности определяется согласно [4], имеет следующую шкалу: «высокая», «средняя», «низкая». При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1. Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя: «маловероятно», «низкая вероятность», «средняя вероятность», «высокая вероятность». При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2. Коэффициент реализуемости угрозы Y будет определяться соотношением $$Y = (Y_1 + Y_2)/20 \cdot$$ По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом: «низкая», «средняя», «высокая» и «очень высокая». Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов определяется вербальный показатель опасности для ИСПДн. Этот показатель имеет три значения: «низкая», «средняя», «высокая»

При построении адекватной системы защиты ПДн для банковских систем необходимо руководствоваться моделью угроз и нарушителей, действующим стандартом Банка России.

Из таблицы видно, что в отраслевом стандарте БС РФ существуют отличия от типовых документов ФСТЭК России как в формулировке терминов, так и в расчете актуальности угроз безопасности ПДн. Это связано с тем, что банковские системы должны соответствовать и нормативно-методическим документам регуляторов (ФСТЭК России, ФСБ России), и стандарту Центра Банка России. Существенным фактором является индивидуальная методика оценки актуальности угроз, что отличает банковские системы от типовых информационных систем ПДн.

ЛИТЕРАТУРА

1. Обеспечение информационной безопасности организаций БС РФ. Методика оценки рисков нарушения информационной безопасности Банка России РС БР // ИББС. 2009. №2, вып. 2.

2. Об информации, информационных технологиях и защите информации: Федеральный закон №149-ФЗ, утвержден Президентом Российской Федерации 14 июля 2006 г.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России от 15.02.2008 г.

4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёна ФСТЭК от 15.02.2008 г.

5. *Шелупанов А.А., Миронова В.Г., Ерохин С.С., Мищель А.А.* Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Докл. Том. гос. ун-та систем управления и радиоэлектроники. 2010. №1(21), ч. 1. С. 14–22.

КОМБИНИРОВАННЫЙ СПОСОБ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В.Г. Миронова, аспирантка

Научный руководитель А.А. Шелупанов, проф., д.т.н.

г. Томск, ТУСУР, ФВС, каф.КИБЭВС, mvg@security.tomsk.ru

Сегодня системы защиты информации востребованы как среди государственных, муниципальных, так и среди коммерческих организаций. Ввиду повсеместно распространившихся краж информации, превратившихся в проблему мирового масштаба, персональные данные (ПДн) нуждаются в надежной защите.

Серьезность и острота проблемы потребовали от органов государственной власти принятия конкретных мер по ее урегулированию. В 2007 г. в России вступил в силу Федеральный закон № 152-ФЗ «О персональных данных», направленный на обеспечение необходимых мер

по защите информации, используемой коммерческими и государственными организациями.

В соответствии с [1], каждое предприятие должно обеспечить защиту ПДн своих сотрудников, клиентов и партнеров и принять все необходимые меры во избежание правонарушений и других незаконных действий, указанных в [1].

Поскольку под понятие «персональные данные» попадают такие данные о человеке, как фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, информация о доходах и многое другое – система защиты персональных данных (СЗПДн) нужна фактически любой организации.

В случае нарушения закона компания может быть привлечена к судебному разбирательству (вплоть до приостановления действий, аннулирования соответствующих лицензий), а виновные лица – к гражданской, уголовной, административной, дисциплинарной ответственности. Согласно [1], информационные системы персональных данных (ИСПДн) должны быть приведены в соответствие с требованиями законодательства не позднее 1 июля 2011 г.

Уполномоченными органами были разработаны нормативно-методические документы, одним из которых является [2], где предлагается использование подхода, основанного на практическом опыте конкретного эксперта. Этот подход предполагает использование знаний и практического опыта специалистов в области защиты информации. Безусловно, одним из достоинств этого метода является отсутствие существенных временных и материальных затрат. Но существует и ряд недостатков, например, трудности при обосновании необходимости реализации мер защиты ПДн. В связи с наличием экспертного подхода к оцениванию угроз безопасности ПДн возникает вероятность недостаточно компетентной оценки. Недооценка угроз безопасности ПДн может привести к слабой системе защиты персональных данных (СЗПДн) и возможным несанкционированным действиям злоумышленника. Поэтому результат проведения обследования ИСПДн, зависящий от субъективного подхода и личных побуждений эксперта, неэффективен.

Предлагается использовать комбинированный подход оценки эксперта, который позволит провести анализ угроз безопасности ПДн и оценить уровень защищенности ИСПДн, учитывая деловую значимость организации. Наличие рекомендаций, основу которых составляет комбинированный подход, позволит свести к минимуму субъективную оценку угроз, временные и материальные затраты. Комбиниро-

ванный подход оценки защищенности ИСПДн состоит из следующих этапов:

1. Определени минимального набора защитных мер для защиты ПДн, обрабатываемых в ИСПДн (удовлетворительная защита ПДн может быть обеспечена путем использования справочных материалов (каталогов) по защитным мерам безопасности, в которых можно подобрать набор средств защиты информации (СЗИ) от часто встречающихся угроз).

2. Идентификация уязвимостей окружающей среды, организации, процедур, персонала, аппаратных и программных средств, узлов связи, которые могут быть использованы источником для нанесения ущерба гражданам РФ и организации в целом.

3. Определение угрозы безопасности ПДн на основании методических рекомендаций уполномоченных органов.

4. Определение вероятности реализации угроз и их актуальности для ИСПДн.

Степень уязвимости следует оценивать по отношению к каждой из определенных угроз отдельно, для этого должна быть разработана специальная шкала оценки уязвимостей и угроз. После завершения оценки уязвимостей должны быть определены степень вероятности реализации угроз, их опасность для ИСПДн и актуальность, после чего выбираются пути устранения актуальных угроз.

Каждый шаг комбинированного подхода должен сопровождаться табличными данными, которые определены математическим путем и которые позволяют актуально оценивать исходный уровень защищенности ИСПДн и строить адекватную СЗПДн.

ЛИТЕРАТУРА

1. О персональных данных: Федеральный закон № 152-ФЗ, утвержден Президентом Российской Федерации 27 июля 2006 г.

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

3. Информационная технология. Методы и средства обеспечения безопасности. Ч. 3. Методы менеджмента безопасности информационных технологий: ГОСТ Р ИСО/МЭК ТО 13335-3–2007.

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержден заместителем директора ФСТЭК России 15 февраля 2008 г.

5. *Шелупанов А.А., Миронова В.Г., Ерохин С.С.,Мицель А.А.* Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Докл. Том. гос. ун-та систем управления и радиоэлектроники. 2010. №1(21), ч. 1. С. 14–22.

6. *Шелупанов А.А., Мещеряков Р.В.* Специальные вопросы информационной безопасности. Томск: Ин-т оптики и атмосферы СО РАН., 2003. 224 с.

7. *Мещеряков Р.В., Шелупанов А.А.* Комплексное обеспечение информационной безопасности автоматизированных систем. Томск Изд-во: В-Спектр, 2007. 278 с.

ИССЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ ПОТОКОВ В ПРОЦЕССИНГОВОМ ЦЕНТРЕ

М.А. Молчанов, студент
г. Томск, ТУСУР, каф. КИБЭВС, ФВС, qwerb@mail.ru

Процессинговый центр – это организация, обеспечивающая информационное, коммуникационное и технологическое взаимодействие между участниками расчетных взаимоотношений [1].

Процессинг – деятельность, включающая в себя сбор, обработку и рассылку участникам информации по операциям с банковскими картами, осуществляемая процессинговым центром.

Пунктами приёма банковских карт могут быть:

– пункты выдачи/приёма наличных – структурные подразделения эквайреров (кассы кредитной организации или её подразделений, обменные пункты, банкоматы и т.д.), выдающие или принимающие наличные денежные средства с использованием банковских карт;

– торгово-сервисные предприятия – организации, принимающие карты в качестве платёжного инструмента для расчётов за реализуемые держателям карт товары и услуги.

При работе с пунктами приёма банковских карт в процессинговом центре возникают информационные потоки, которые содержат критические данные, с точки зрения защиты информации.

Критичные данные состоят из магнитной полосы, подтверждающего кода карты и PIN. Они не должны сохраняться после прохождения процедуры авторизации (даже в зашифрованном виде) [2].

Для обеспечения безопасности конфиденциальной информации, обрабатываемой и хранимой в процессинговом центре, проводят деление компонентов сети на зоны [3]. Существуют 4 основные зоны, согласно стандартам безопасности Visa и MasterCard: неконтролируемая зона, демилитаризованная зона, внутренняя банковская сеть и зона высокой безопасности. Каждая зона имеет свой уровень ограничения доступа, соответственно, это позволяет распределять потоки конфиденциальных данных и доступ к ним, а также дает возможность построить эффективную систему защиты конфиденциальной информации.

На рис. 1 продемонстрирована схема информационного потока между основными зонами процессинговой сети.

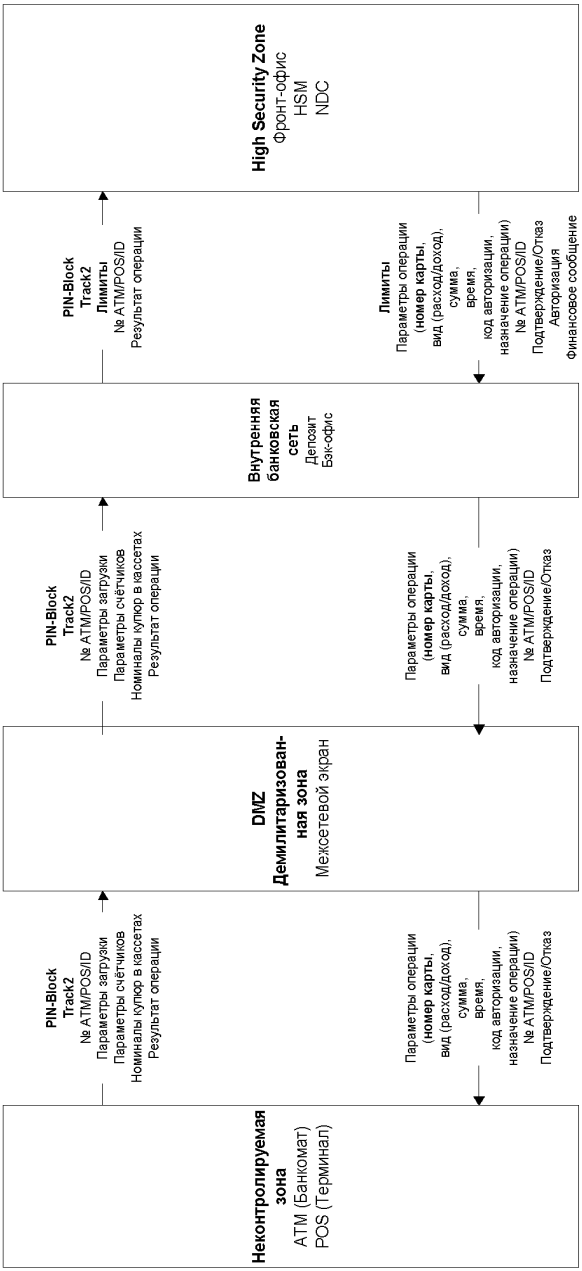


Рис. 1. Информационный поток

ЛИТЕРАТУРА

1. Расчеты и операционная работа в коммерческом банке // Методический журнал. 2006. №12.

2. Стандарт безопасности данных индустрии платежных карт PCI DSS, 2008.

3. Стандарт безопасности Visa.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ПОИСКЕ ОПТИМАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Е.А. Мошников, аспирант

Научный руководитель А.П. Зайцев, проф., к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, john_js@rambler.ru

Теоретические основы выбора оптимальных технических средств защиты информации (ТСЗИ) исключительно сложны и, несмотря на интенсивность исследований в этой предметной области, еще далеки от совершенства.

Оптимальным будет считаться решение, которое в предполагаемых условиях наилучшим образом удовлетворит условиям рассматриваемой задачи. Оптимальность решения достигается за счет наиболее рационального распределения ресурсов, затрачиваемых на построение системы защиты информации.

При решении конкретной задачи оптимизации необходимо прежде всего выбрать математический метод, который приводил бы к конечным результатам с наименьшими затратами на вычисления или же давал возможность получить наибольший объем информации об искомом решении. Выбор того или иного метода в значительной степени определяется постановкой задачи оптимизации, а также используемой математической моделью объекта оптимизации [1].

Классические методы исследования функций можно использовать для решения относительно несложных задач оптимизации без ограничений. Однако большинство задач при выборе оптимальных технических средств защиты информации (ТСЗИ) связано с оптимизацией при наличии некоторого количества ограничений.

Выбор оптимальных ТСЗИ усложняется рядом их особенностей, основными из которых являются:

– необходимость учета большого числа показателей ТСЗИ при оценке и выборе их оптимального варианта;

– преимущественно качественный характер показателей, учитываемых при анализе и синтезе ТСЗИ;

– существенная взаимосвязь и взаимозависимость этих показателей, имеющих противоречивый характер;

– необходимость использования информации, полученной экспертным путем;

– трудность получения исходных данных об ТСЗИ.

Указанные особенности делают практически невозможным применение традиционных методов оптимизации для решения задачи выбора оптимальных ТСЗИ.

Сложность процесса принятия решений, отсутствие математического аппарата приводят к тому, что при оценке и выборе альтернатив возможно (а зачастую просто необходимо) использовать и обрабатывать качественную экспертную информацию. Перспективным направлением разработки методов принятия решений при экспертной исходной информации является лингвистический подход на базе теории нечетких множеств и лингвистической переменной [2].

Теория нечетких множеств в очередной раз подтвердила одну известную всем исследователям истину: применяемый формальный аппарат по своим потенциальным возможностям и точности должен быть адекватен смысловому содержанию и точности исходных данных. Математическая статистика и теория вероятностей используют экспериментальные данные, обладающие строго определенной точностью и достоверностью. Теория нечетких множеств имеет дело с «человеческими знаниями», которые принято называть экспертной информацией.

При принятии решения о выборе оптимального варианта ТСЗИ возникает задача определения важности (веса) требований, предъявляемых к параметрам ТСЗИ. При решении практических задач обоснования требований и выбора оптимальных ТСЗИ возникает естественный вопрос рационального выбора метода определения весовых коэффициентов. Неправильный выбор метода приводит, как правило, к недостаточной обоснованности производимых операций над малодостоверными исходными экспертными данными.

Факторы, влияющие на выбор метода оценки весовых коэффициентов [3].

1. Физическая сущность параметров и отношение между ними.

Параметры определяются исходя из смысла провозглашенной цели. Далее необходимо определить степень взаимосвязей и взаимоотношений между ними, т.е. зависимости или независимости. Характер зависимости или независимости (независимость по полезности, по предпочтению, по безразличию и т.д.) влияет на выбор метода оценки.

2. Сложность проведения экспертизы и трудоемкость получения экспертной информации.

Сложность и трудоемкость экспертизы определяется реальными условиями и возможностями ее проведения.

3. Степень согласованности мнений экспертов.

Степень согласованности в первую очередь зависит от количества привлекаемых экспертов и уровня их квалификации. В то же время на нее влияет выбранный метод оценки весов. Так, наибольшую согласованность экспертов обеспечивает линейная свертка, наименьшую – непосредственная численная оценка весов, при этом ранжирование при всей его простоте позволяет получить весовые коэффициенты, достаточно точные и близкие к их значению, полученному методом линейной свертки.

4. Трудоемкость обработки экспертных данных.

Этот фактор не является главным при современном уровне развития вычислительной техники. Однако применение сложных методов обработки экспертной информации может потребовать разработки специальной программы обработки, что повлияет на сроки проведения экспертизы.

Очевидно, что наиболее простыми методами с этой точки зрения являются ранговые и балльные методы. Учет вышеприведенных факторов позволяет выбрать рациональный вариант оценки весовых коэффициентов.

Сложность процесса принятия решений, отсутствие математического аппарата приводят к тому, что при оценке и выборе альтернатив возможно, (а зачастую просто необходимо) использовать и обрабатывать качественную экспертную информацию. Поэтому перспективным направлением разработки при выборе оптимальных ТСЗИ является лингвистический подход на базе теории нечетких множеств и лингвистической переменной.

ЛИТЕРАТУРА

1. *Трифонов А.Г.* Постановка задачи оптимизации и численные методы ее решения. http://matlab.exponenta.ru/optimiz/book_2/1.php

2. *Кофман А.* Введение в теорию нечетких множеств М.: Радио и связь, 1982. 432 с.

3. *Литвак Б.Г.* Экспертная информация: методы получения и анализа. М.: Радио и связь, 1982. 184 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ОТОБРАЖЕНИЯ ПРОЦЕССОВ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.Ю. Наумов, студент, М.А. Сопов, ст. преподаватель

г. Томск, ТУСУР, ФВС, stas691987@mail.ru

Для отображения моделей в информационной безопасности нет четких стандартов для их отображения. В настоящее время в России резко возрос интерес к общепринятым на Западе стандартам, однако в

реальной практике управления существует один очень показательный момент. Многих руководителей организаций по защите информации до сих пор можно поставить в тупик прямым вопросом об организационной структуре компании или о схеме существующих информационных процессов. Наиболее продвинутые специалисты по информационной безопасности, как правило, начинают чертить понятные только им одним иерархические диаграммы, но и в этом процессе обычно быстро заходят в тупик. То же самое касается сотрудников и руководителей различных служб и функциональных подразделений. В большинстве случаев единственным набором правил отображений моделей, в соответствии с которыми должно функционировать предприятие, является набор отдельных положений и должностных инструкций. Чаще всего такие документы составлялись не один год назад, слабо структурированы и невзаимосвязаны между собой и, вследствие этого, просто не были востребованы. Но все же подобный подход был оправдан, в то время, когда конкуренция практически отсутствовала. В результате этого мы наблюдаем в течение последних двух лет вполне объяснимую картину: крупные компании, выросшие в начале 90-х годов, постепенно сдают свои позиции, вплоть до полного ухода с рынка. Отчасти это обусловлено тем, что на предприятии не были внедрены стандарты для отображения моделей в информационной безопасности. С помощью моделирования различных областей деятельности можно достаточно эффективно анализировать «узкие места» в управлении и оптимизировать общую схему организации. Для такого моделирования в последнее время из самых распространенных применяются такие стандарты, как IDEF0, UML, ARIS.

Когда нужно провести четкий анализ, то мы используем IDEF0. Это помогает следовать конкретной методологии анализа и преодолеть недостаток воображения и широты восприятия множества связанных сущностей и действий в изучаемых процессах.

Когда нужно быстро набросать диаграмму, резюмирующую интервью, мы используем диаграммы прецедентов и последовательностей UML, их легче комментировать и править неподготовленному человеку.

Из плюсов IDEF0 – методология SADT дисциплинирует мышление и дает отличный регламент взаимодействия аналитика с экспертами в предметной области, очень рано выявляет разногласия в терминологии и представлениях о том, что происходит, или о том, что хотелось бы, чтобы происходило. Из минусов IDEF0 – методика SADT не дает четких критериев достаточности модели, очень легко увлечься и углубиться в несущественные детали. Кроме того, концепция декомпозиции проста и понятна лишь до момента необходимости передеком-

позиции. Еще одна проблема заключается в том, что нотация IDEF0 отлично подходит для описания процессов «от функций», что предполагает достаточно ясно определенные сущности (документы, объекты, понятия, термины), которыми оперируют выявляемые функции. Когда это не так, необходимо очень глубокое и уверенное владение методологией SADT, чтобы проводить не описательный, а моделирующий анализ. В этом случае требования к трудоемкости моделирования возрастают экспоненциально. То есть на описание процесса из 5–6 функций требуется 2–3 ч, на описание процесса из 20–30 функций – соответственно 10–20 ч. Однако на моделирование процесса из 5–6 функций требуется 5–6 ч, а на моделирование процесса из 20–30 функций – 100–200 ч.

Из плюсов UML можно выделить:

– UML – объектно-ориентированный, в результате чего методы описания результатов анализа и проектирования семантически близки к методам программирования на современных ОО-языках.

– UML позволяет описать систему практически со всех возможных точек зрения и разные аспекты поведения системы.

– Диаграммы UML сравнительно просты для чтения после достаточно быстрого ознакомления с его синтаксисом.

– UML расширяет и позволяет вводить собственные текстовые и графические стереотипы, что способствует его применению не только в сфере программной инженерии.

– UML получил широкое распространение и динамично развивается.

Из минусов – отсутствие четкой методики анализа и моделирования, которая помогает избежать субъективности в связывании отдельных потоков событий в замкнутые процессы. Построение классов и пакетов принципиально субъективно и может полагаться лишь на шаблоны проектирования, а также на фантазию и искушенность архитектора. При этом проверить правильность проектирования может лишь более опытный архитектор, в отличие от методики SADT, где ошибки может выявить любой тщательно контролирующий правила моделирования и согласие экспертов с терминологией читатель диаграмм.

Что касается ARIS – трудно четко разделить плюсы и минусы в связи с тем, что эта нотация, как и методология, строго описательна. В них нет собственно моделирования, только процессно-функциональная декомпозиция. ARIS – это все-таки больше инструмент построения бизнес-процессов, чем инструмент анализа и моделирования предметной области.

Хотя парадигма построения корпоративного ПО в значительной степени сместилась от функциональных и объектно-ориентированных моделей к процессно-ориентированным, поэтому вполне возможно, что UML сегодня одна из наиболее оптимальных методологий проектирования.

ЛИТЕРАТУРА

1. *Буч Г., Рамбо Д., Якобсон И.* Язык UML. Руководство пользователя. 2-е изд.: Пер. с англ. Н.М. Мухина. М.: ДМК Пресс, 2006. 496 с.

МОДУЛЬНОЕ ТЕСТИРОВАНИЕ И ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

К.А. Нечаев, И.А. Рахманенко, В.М. Козлов, Р.Ю. Ибрагимов, студенты 4-го курса

Научный руководитель М.А. Сопов, ст. преподаватель

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, akadelpher@gmail.com

В настоящее время очень распространены методы так называемой разработки через тестирование (TDD), технике программирования при которой на первый план ставится написание модульных тестов с целью уменьшить возможность появления ошибок в процессе изменения внутренней структуры программы, написания нового функционала и оптимизации кода. Разрабатываемая программа постоянно подвергается тестированию. При этом обычно используются средства, автоматизирующие проведение тестов.

Тесты пишутся для каждого модуля разрабатываемого продукта. Каждый тест заключается в проверке работы отдельной функции или модуля программы на соответствие полученного и ожидаемого результата работы функции. Перед добавлением новой функции разработчик принимает решение, каким способом будет её тестировать (определяет входные и ожидаемые выходные данные), пишется тест, проверяющий функцию, и сама функция. Выполняется проверка корректности работоспособности написанного кода. И затем, при необходимости проводятся рефакторинг и оптимизация. При этом за счет наличия готового теста практически исключается шанс появления незамеченных ошибок в коде. Каждый раз при тестировании программы запускаются тесты всех модулей, таким образом, возможно обнаружение новых ошибок во всех модулях программы и ошибок, связанных с влиянием работы одних модулей на другие.

Одним из наиболее сложных моментов разработки через тестирование являются создание и поддержка тестов интерфейса пользователя (UI). Тестирование интерфейса затруднительно из-за сложности под-

готовки входных данных, а иногда, например в случае использования ASP.NET Web Forms, невозможности создать экземпляр формы (страницы) в тесте. Существуют средства, предназначенные для упрощения тестирования интерфейса, например, WatiN предоставляет удобные средства для создания HTTP запроса и проверки страницы-результата [1].

Но одним из наиболее эффективных способов устранения проблемы тестирования интерфейса является минимизация кода интерфейса. Семейство шаблонов проектирования MVC (Model–View–Controller) основано на четком разделении слоёв интерфейса программы, данных интерфейса и слоя реакции на действия пользователя. При этом все три слоя являются независимыми, и появляется возможность тестировать каждый слой независимо от других. При этом код интерфейса стараются минимизировать, данные для вывода на экран готовятся в слое реакций на действия пользователя, а интерфейс привязывается к ним. Современные технологии разработки интерфейсов изначально включают в себя средства, упрощающие реализацию данного подхода (ASP.NET MVC используется для создания интернет-ресурсов, WPF – упрощает использование паттерна MVVM) [2].

В проекте ГПО «Термино-понятийная система» активно используется шаблон MVVM (Model–View–View Model) и технология WPF [3]. Данная технология имеет средства декларативной привязки данных и команд к элементам управления. Данные, необходимые для работы программы, загружаются в Model (модель), подготавливаются к отображению в View Model (модель представления), и затем View (представление) привязывает полученные данные к элементам интерфейса. При этом в представлении фактически отсутствует программный код, а следовательно, тестировать его нет необходимости. Тестирование интерфейса сводится к визуальной проверке того, все ли элементы формы отображаются корректно.

Выполнено в рамках проекта ГПО: КИБЭВС-0902 – «Иженерия баз данных».

ЛИТЕРАТУРА

1. Dino Esposito. Programming Microsoft ASP.NET MVC. Microsoft Press 2010. 592 с.

2. *Martin Fowler*. Presentation Model [электронный ресурс]. Режим доступа: http://martinfowler.com/eaaDev/PresentationModel.html

3. *Джош Смит*. Приложения WPF с шаблоном проектирования модель–представление–модель представления [Электронный ресурс]. Режим доступа: http://msdn.microsoft.com/ru-ru/magazine/dd419663.aspx

ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В ПРОЦЕССИНГОВОМ ЦЕНТРЕ

О.О. Осипова, студентка
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, scintilla@mail2000.ru

Процессинговый центр – это организация, обеспечивающая информационное, коммуникационное и технологическое взаимодействие между участниками расчетных взаимоотношений [1].

На данный момент в России функционируют около 100 процессинговых центров, не учитывая процессинговые центры локальных платежных систем. Эти процессинговые центры обслуживают порядка 500 российских банков – участников международных платежных систем VISA и MasterCard. Таким образом, каждый четвертый российский банк имеет собственный процессинговый центр (чаще всего в форме in-house).

Процессинг – деятельность, включающая в себя сбор, обработку и рассылку участникам информации по операциям с банковскими картами, осуществляемая процессинговым центром.

На рис. 1 продемонстрирована схема информационного обмена в процессинговой сети. Узлы, процессинг-узлы, процессинговый центр системы образуют процессинговую сеть, обслуживающую участников системы.

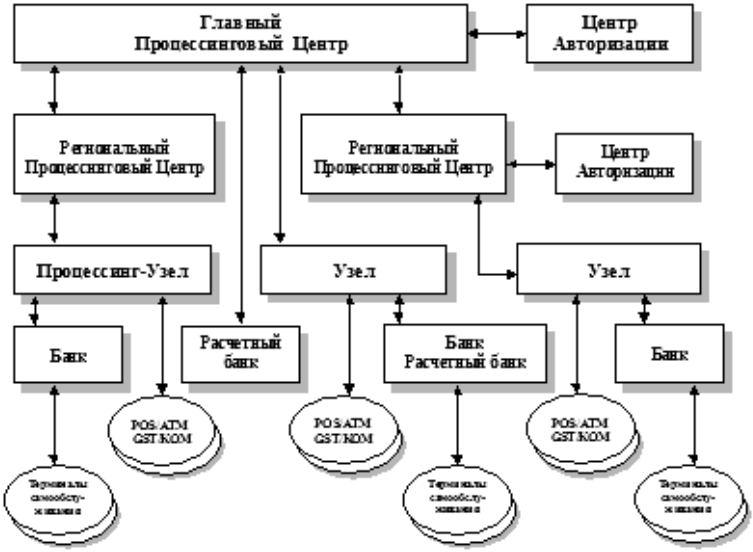


Рис. 1. Процессинговая сеть

Ядром сети является процессинг-центр. На него возложены функции обработки межрегиональных транзакций, регистрации всех элементов системы и управления работой сети. Он обеспечивает безопасность сети и производит обновление и распространение черного списка.

Узлы процессинговой сети предназначены для обслуживания терминалов и банкоматов – сбор транзакций и передача их в процессинг-центр для обработки, обновление черного списка терминалов и синхронизация времени. Узел также осуществляет маршрутизацию запросов от терминалов на авторизацию и проводит авторизацию карт по черному списку в определенных режимах совершения транзакций.

Для обеспечения безопасности конфиденциальной информации, обрабатываемой и хранимой в процессингоом центре, проводят деление компонентов сети на зоны [2]. Существует 4 основные зоны, согласно стандартам безопасности Visa и Mastercard: неконтролируемая зона, демилитаризованная зона, внутренняя банковская сеть и зона высокой безопасности. Каждая зона имеет свой уровень ограничения доступа, соответственно, это позволяет распределять потоки конфиденциальных данных и доступ к ним, а также дает возможность построить эффективную систему защиты конфиденциальной информации.

Информационные потоки данных в процессинговом центре содержат критические данные, которые требуют тщательной защиты. Критичные данные состоят из магнитной полосы, подтверждающего кода карты и PIN. Они не должны сохраняться после прохождения процедура авторизации (даже в зашифрованном виде) [3].

ЛИТЕРАТУРА

1. Расчеты и операционная работа в коммерческом банке: Метод. журнал. 2006. №12.
2. Стандарт безопасности Visa.
3. Стандарт безопасности данных индустрии платежных карт PCI DSS.

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Д.Ю. Осипов, 5-й курс, М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, каф. КИБЭВС, nsman@list.ru

Облачные вычисления (англ. cloud computing) – новая парадигма вычислений, основанная на идее использования через Web-браузер с любого компьютера набора специализированных сервисов, развернутых и доступных для использования через Web на компьютерах мощного центра обработки данных. Эти сервисы можно разделить на три категории:

1) программное обеспечение как сервис;

2) платформа как сервис;

3) инфраструктура как сервис.

Программное обеспечение как сервис (Software as a Service, SaaS) – модель предоставления программного обеспечения как сервиса – обеспечивает возможность аренды приложений. Программное обеспечение как сервис включает платформу как сервис и инфраструктуру как сервис. Модель предоставления программного обеспечения как сервиса является моделью обеспечения доступа к приложениям через Интернет с оплатой по факту их использования. Данная модель является наиболее распространенной моделью предоставления облачных сервисов. Организации могут реализовывать подобную модель предоставления сервиса из частных облаков, используя внутренние сетевые каналы, дополнительно защищенные и не связанные с Интернетом.

Платформа как сервис (Platform as a Service, PaaS) – модель предоставления платформы как сервиса – предоставляет возможность аренды платформы, которая включает операционную систему и прикладные сервисы. Платформа как сервис облегчает разработку, тестирование, развертывание и сопровождение приложений без необходимости инвестиций в инфраструктуру и программную среду. Платформа как сервис также включает и инфраструктуру как сервис.

Инфраструктура как сервис (Infrastructure as a Service, IaaS) – модель предоставления инфраструктуры (аппаратных ресурсов) как сервиса – предоставляет возможность аренды таких инфраструктурных ресурсов, как серверы, устройства хранения данных и сетевое оборудование. Управление всей инфраструктурой осуществляется поставщиком сервисов, а потребитель управляет только операционной системой и установленными приложениями. Такие сервисы обычно оплачиваются по их фактическому использованию и позволяют пользователю увеличивать или уменьшать объем используемой инфраструктуры через специальные порталы, предоставляемые поставщиками сервисов.

Существует несколько моделей владения облаком. Их принято разделять на следующие классы:

Private Cloud – частное облако. Частным облаком называют облачную систему, созданную и эксплуатируемую только одной организацией.

Public Cloud – публичное облако. В данной модели облачная инфраструктура предоставляется для использования всем желающим. Система создана одним из глобальных провайдеров, и услуги продаются через интернет. Любой человек имеет возможность приобрести

нужную ему услугу, оплатив её банковской картой или иным доступным методом.

Hybrid Cloud – смешанное облако. Смешанным облаком называют облачную систему (частную или общую), интегрированную с другой облачной системой.

Основные характеристики:

– самообслуживание по мере необходимости. Потребитель может, по мере необходимости, в одностороннем порядке получить вычислительные ресурсы, такие как серверное время и сетевые ресурсы для хранения данных, в автоматическом режиме, не требующем взаимодействия человека с поставщиком каждой из услуг;

– широкий сетевой доступ. Ресурсы доступны по сети, и доступ к ним осуществляется с помощью стандартных механизмов, способствующих использованию разнородных тонких и толстых клиентских платформ (например, мобильных телефонов, ноутбуков и КПК);

– объединение ресурсов в пул. Вычислительные ресурсы поставщика услуг объединяются в пул для обслуживания ряда потребителей с использованием многопользовательской модели, при этом различные физические и виртуальные ресурсы динамически назначаются и переназначаются в соответствии со спросом со стороны потребителей;

– оперативная гибкость. Ресурсы могут предоставляться быстро и гибко, в некоторых случаях автоматически, обеспечивая быстрое масштабирование и быстрое освобождение ресурсов. С точки зрения пользователя возможности получения ресурсов часто представляются неограниченными и могут быть приобретены в любом количестве и в любое время;

– измеримая услуга. Облачные системы автоматически контролируют и оптимизируют использование ресурсов, опираясь на возможность проведения измерений на определенном уровне абстракции, соответствующем данному виду услуг (это могут быть, например, хранение, обработка, пропускная способность, активные учетные записи пользователей). Использование ресурсов можно отслеживать, контролировать, и о нём можно извещать, обеспечивая прозрачность как для поставщика, так и для потребителя соответствующей услуги.

Преимущества облачных вычислений:

– пользователь оплачивает услугу только тогда, когда она ему необходима, а самое главное, он платит только за то, что использует;

– облачные технологии позволяют экономить на приобретении, поддержке, модернизации ПО и оборудования;

– масштабируемость, отказоустойчивость и безопасность – автоматическое выделение и освобождение необходимых ресурсов в зави-

симости от потребностей приложения. Техническое обслуживание, обновление ПО производит провайдер услуг;

– удаленный доступ к данным в облаке – работать можно из любой точки на планете, где есть доступ в сеть Интернет.

Недостатки облачных вычислений:

– пользователь не является владельцем и не имеет доступа к внутренней облачной инфраструктуре. Сохранность пользовательских данных сильно зависит от компании провайдера;

– недостаток, актуальный для российских пользователей. Для получения качественных услуг пользователю необходимо иметь надежный и быстрый доступ в сеть Интернет;

– отсутствие общепринятых стандартов в направлении безопасности облачных технологий.

ЛИТЕРАТУРА

1. Cloud Computing. Позиция компании Red Hat [Электронный ресурс]. Режим доступа: http://www.bureausolomatina.ru/ru/themes_in_progress/clouds/8

2. Об облачных вычислениях [Электронный ресурс]. Режим доступа: http://www.parallels.com/ru/spp/understandingclouds/

3. Облачные вычисления – это... [Электронный ресурс]. Режим доступа: http://cloudzone.ru/articles/review/1.html

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФЕДЕРАЛЬНЫХ ЭЛЕКТРОННЫХ ТОРГОВЫХ ПЛОЩАДОК

Н.А. Панин, студент 5-го курса

Научный руководитель Р.В. Мещеряков, д.т.н.

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, mrv@keva.tusur.ru

С 1 января 2011 г. вступили в силу изменения в Федеральном Законе № 94 [1], согласно которым все аукционы государственными учреждениями должны проводиться на 5 отобранных федеральных площадках: ММВБ «Госзакупки», ООО «РТС-тендер», ГУП «Агентство по государственному заказу РТ», ЗАО «Сбербанк – автоматизированная система торгов» и ОАО «Единая электронная торговая площадка».

Проведение открытых аукционов для размещения заказов на поставку товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд полностью перешло в электронную форму.

Это позволяет избежать конфликта интересов, сговора между заказчиком и поставщиком или между недобросовестными поставщиками, создает здоровую и эффективную конкурентную среду закупок, обеспечивает открытость и прозрачность государственных закупок, снижение коррупции, экономию бюджетных средств.

Плюсов проведения открытых аукционов в электронной форме, несомненно, много, но это также создает необходимость обеспечения высокого уровня информационной безопасности, ведь речь идет о гигантских финансовых рисках. К примеру с 1 июля по 31 декабря 2009 г. на сайте федеральной торговой площадки ОАО «ЕЭТП» прошло более 800 аукционов на общую сумму более 1,39 млрд рублей.

Обеспечение информационной безопасности электронных торговых систем, главным образом, связано с использованием средств криптографической защиты информации и технологии электронной цифровой подписи (ЭЦП).

Использование ЭЦП регламентируется Федеральным законом № 1 от 10 января 2002 г. «Об электронной цифровой подписи» [2] и «Регламентом получения сертификатов ключей подписи и использования электронной цифровой подписи» [3]. Электронный документ, подписанный электронной цифровой подписью, имеет такую же юридическую силу, как и подписанный собственноручно документ на бумажном носителе, и влечет предусмотренные для указанного документа правовые последствия.

Использование СКЗИ и технологии ЭЦП для электронного документооборота позволяет:

- обеспечить подтверждение подлинности и авторства электронных документов;
- защитить электронные документы от подделки;
- обеспечить контроль целостности информации при передаче и хранении.

Применение ЭЦП в электронных торгах позволяет однозначно судить о том, кто именно в них участвует, а также обеспечивает невозможность отказа от сделки.

Для участия в электронных торгах, участник размещения заказа получает ключ и сертификат ключа подписи в точках выдачи сертификатов ключей ЭЦП одного из авторизованных удостоверяющих центров. В электронных торгах, ключ подписи участника размещения заказа, изготовленный Авторизованным удостоверяющим центром, действует на всех электронных площадках.

Запись ключевой пары и сертификата ключа подписи осуществляется на сертифицированный электронный ключ, такой как eToken [4].

eToken представляет собой защищенное устройство, предназначенное для строгой аутентификации, безопасного хранения секретных данных, выполнения криптографических вычислений и работы с асимметричными ключами и цифровыми сертификатами. eToken выпускается в двух форм-факторах: в виде USB-ключа и в виде смарт-карты (рис. 1).

Потенциальные угрозы, возникающие при работе с обычными съемными ключевыми носителями (дискетами, Flash-дисками):

- утеря, хищение ключевого носителя;
- доступ к ключу во время работы с закрытым ключом посредством вредоносных программ;
- подбор пароля к ключевому носителю.

Сертифицированные электронные ключи разработаны специально для надежного противостояния различным типам атак и обеспечивают максимально высокий уровень безопасности хранения и использования закрытых ключей. Микросхема, которую использует этот класс устройств, обеспечивает безопасное хранение и использование ключей шифрования и ЭЦП, а также надёжное хранение цифровых сертификатов (рис. 2).

Рис. 1. Электронный идентификатор eToken

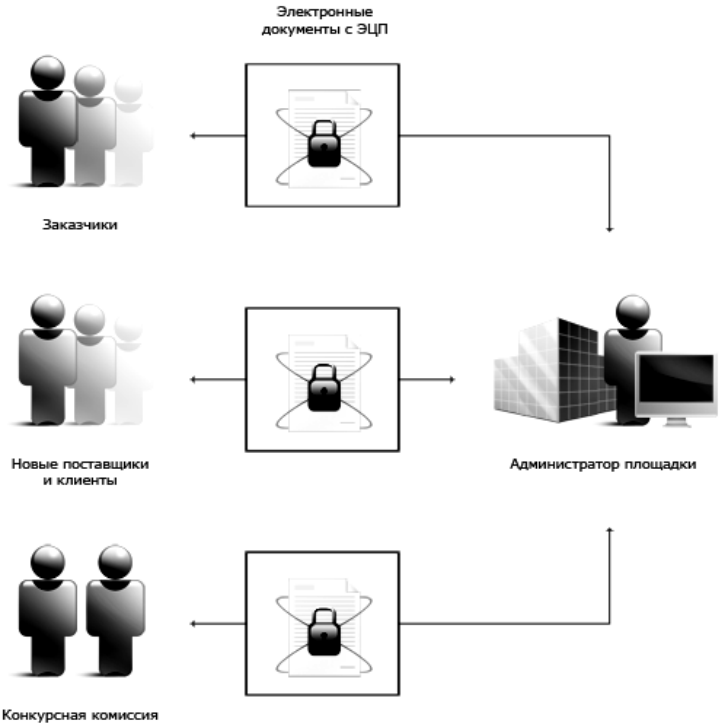


Рис. 2. Упрощенная схема применения ЭЦП в торгах

С момента приобретения центром статуса авторизованного удостоверяющего центра он начинает нести ответственность за ущерб любым третьим лицам в связи с неисполнением либо ненадлежащим исполнением своих обязательств по осуществлению деятельности удостоверяющего центра перед участниками размещения заказа на электронных площадках. Размер ответственности составляет до 7000000 руб. по каждому случаю нанесения ущерба третьим лицам, что в очередной раз доказывает необходимость высокого уровня информационной безопасности и специальных проверочных мероприятий при авторизации удостоверяющих центров. В Томске такой статус авторизованного удостоверяющего центра имеет структурное подразделение ТУСУРа – Удостоверяющий центр Сибири [5].

Для государственных учреждений выдачу сертификатов ключей подписи осуществляет Федеральное казначейство.

Так как в любой автоматизированной системе самым слабым звеном является человек из-за своей непредсказуемости, организационный элемент комплексной системы обеспечения информационной безопасности крайне важен [6]. Актуальным является вопрос обеспечения специалистов авторизованных удостоверяющих центров организационно-методической документацией, разработки соответствующих регламентов, должностных инструкций, форм журналов и отчетов. Для участников электронных торговых систем, которые являются пользователями СКЗИ, в свою очередь актуальной является разработка программы обучения, рекомендаций и инструкций по эксплуатации СКЗИ.

ЛИТЕРАТУРА

1. Федеральный закон от 21.07.2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» (в ред. от 01.01.2011 г.).

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

3. Приложение № 7 соглашения, заключенного между Федеральной антимонопольной службой, Минэкономразвития и пятью отобранными операторами для проведения торгов госзаказа, которым является «Регламент получения сертификатов ключей подписи и использования электронной цифровой подписи».

4. [Электронный ресурс]. Режим доступа: http://www.aladdin-rd.ru/catalog/etoken/

5. [Электронный ресурс]. Режим доступа: http://www.udcs.ru/

6. *Мещеряков Р.В., Шелупанов А.А.* Комплексное обеспечение информационной безопасности автоматизированных систем. Томск: В-Спектр, 2007. 278 с.

СОЗДАНИЕ ОБРАЗОВАТЕЛЬНОГО ПОРТАЛА КАФЕДРЫ

Р.В. Петриченко, В.А. Шаров, студенты
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, roman-vp@rambler.ru

Цель данного проекта – создание образовательного портала для обеспечения единого информационного пространства различных групп участников: преподавателей, студентов, родителей студентов, работодателей и др.

Для реализации поставленной задачи разумно использовать одну из свободно распространяемых CMS (content managment system – система управления веб-содержимым). Также применение наработок по различных модулям веб-сайтов позволит существенно сократить время создания интернет-ресурса с необходимым функционалом.

Наиболее распространёнными бесплатными CMS являются: wordpress, drupal и joomla. Первый не отвечает функциональным требованиям, т.к. является блого-ориентированной системой. И joomla и drupal смогут выполнить поставленные требования, но второй более социально ориентирован и имеет меньшие проблемы с безопасностью. Благодаря этим факторам выбор был сделан в пользу drupal.

Для дальнейшей реализации по требуемой структуре сайта был составлен список функциональных требований. Данные требования были реализованы посредством модулей, указанных в таблице.

Требуемые модули

Требуемый функционал	Необходимые модули
Проведение опросов	Poll
Категорирование материалов	Taxonomy
Анимация основного меню	dhtml_menu
Реализация блогов	Blog
Текстовый редактор	TinyMCE
Галерея	Image, Lightbox2
RSS	RSSAgregator

Но данных модулей недостаточно для задач, связанных с запросами к базе данных. В данных случаях будет использоваться php-код, исполняемый при помощи встроенного модуля php-filter. При должной настройке администраторы смогут размещать исполняемый код, осуществляющий выполнение требуемых операций. Стоит отметить, что в drupal существует программная прослойка между CMS и базой данных, позволяющая абстрагироваться от конкретной СУБД [1]. Данная возможность реализована для postgresql и mysql в шестой версии системы управления и для oracle и sqlite в седьмой [2]. Используя встроенные в drupal функции, мы можем не беспокоиться о работе сайта на поддерживаемых платформах.

Работа с оформлением сайта должна вестись комплексно в трёх направлениях: работа с css-стилями, с каркасом страниц и с ресурсами. Каркас страницы написан на php и html, он проверяет, активны ли элементы оформления, и помещает их в соответствующие блоки, как правило, разбит на несколько файлов. CSS-стили в основном отвечают за отображение текста. К ресурсам в данном случае относятся графические файлы и разделители.

В ходе работы не была затронута часть проекта, связанная с разграничением доступа. В системе реализована ролевая модель разграничения доступа. Она позволит назначить привилегии в соответствии со статусом пользователя, например: родитель, ученик, преподаватель, а также присваивать несколько ролей одному и тому же человеку. Это необходимо для решения специфических задач, например: выдача преподавателю права изменять раздел о стипендиях. Помимо этого, нужно реализовать возможность запрета доступа некоторых ролей к определенным страницам. На данном этапе такая функция работает только на страницах администрирования в рамках соответствующих модулей.

ЛИТЕРАТУРА

1. Drupal project Frequently Asked Questions (FAQ) // Drupal's online documentation 2011 URL: http://drupal.org/node/130533 (дата обращения: 18.02.2011).

2. *Рысевец М.В.* Drupal .BZ DRUPAL HAND BOOK [Электронный ресурс]. 2010. URL: http://drupal.bz (дата обращения: 23.12.2010).

ОПРЕДЕЛЕНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОМОЩИ МЕТОДОВ КОГНИТИВНОЙ ЛОГИКИ

П.В. Плетнев, аспирант, В.М. Белов, проф., д.т.н.
г. Новосибирск, СибГУТИ, pavel-pletnev@rambler.ru

В данной статье приводится описание процесса оценки угроз информационной безопасности (ИБ), а также рассматривается способ применения когнитивно-ориентированных моделей и схем вывода, в частности таких средств, как Сорит и семантические сети, для оценки угроз ИБ.

Основная идея предлагаемого подхода определения угроз ИБ состоит в следующем. На базе вопросников, заполняемых в ходе аудита, формируют унарные и бинарные высказывания, после чего строят Сорит, результатом которого являются факты, влекущие за собой угрозы ИБ [1]. Затем на основании исчисления предикатов строят модель ак-

туальных угроз, а именно угроз, влекущих утечку информации. Таким образом, используя данные процедуры, формируют семантическую сеть, с итогом использования на большом количестве предметных областей. Результатом построения такой сети является формирование базы знаний, позволяющей определять угрозы информационной сети, имея на входе лишь её формальное описание. Ниже приведём описание каждого этапа более подробно.

Для построения Сорита необходим ряд исходных унарных высказываний. В примере рассмотрим исходные высказывания, касающиеся использования на предприятии отчуждаемых носителей информации.

1) W0 – рассматриваемая организация;
2) W1 – организация, в которой используют гибкие магнитные диски (ГМД);
3) W2 – организация, имеющая уязвимое звено «отчуждаемые носители информации»;
4) W3 – организация, подверженная угрозе хищения носителей;
5) W4 – организация, подверженная угрозе уничтожения носителя;
6) W5 – организация, подверженная угрозе утери носителя.

На основе унарных высказываний сформируем бинарные высказывания, в которых задействованы традиционные для формальной логики кванторы:

A, W0, W1 – рассматриваемая организация есть организация, в которой используют гибкие магнитные диски (ГМД).

Данное бинарное высказывание строим, исходя из фактической ситуации на предприятии. Далее перечислены бинарные высказывания, справедливые для любой организации.

A, W1, W2 – всякая организация, в которой используют ГМД, есть организация, имеющая уязвимое звено «отчуждаемые носители информации».

A, W2, W3 – организация, имеющая уязвимое звено «отчуждаемые носители информации», есть организация, подверженная угрозе хищения носителей.

A, W2, W4 – организация, имеющая уязвимое звено «отчуждаемые носители информации», есть организация, подверженная угрозе уничтожения носителей.

A, W2, W5 – организация, имеющая уязвимое звено «отчуждаемые носители информации», есть организация, подверженная угрозе утери носителей.

Бинарные высказывания с точки зрения силлогистики Аристотеля, представляют собой одну из посылок силлогизма с соответствующим квантором A, E, I, O. Эти посылки могут сочетаться в различных комбинациях друг с другом, в результате чего будут получены новые

заключения. Заключения также можно сочетать между собой до тех пор, пока естественный переход от сильных модусов к слабым не остановит процесс порождения новых выводов [2].

Сорит, построенный на основе исходных посылок, представлен на рис. 1. В результате построения сорита получены следующие выводы:

1) A, W0, W3 – рассматриваемая организация есть организация, подверженная угрозе хищения носителей;

2) A, W0, W4 – рассматриваемая организация есть организация, подверженная угрозе уничтожения носителей;

3) A, W0, W5 – рассматриваемая организация есть организация, подверженная угрозе утери носителей.

Данный подход используется в ежедневной аудиторской деятельности предприятия ООО «Центр информационной безопасности»

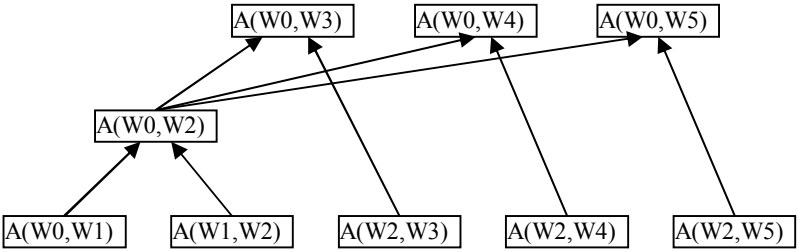


Рис. 1. Построенный сорит

ЛИТЕРАТУРА

1. *Козлов Л.А.* Когнитивное моделирование на ранних стадиях проектной деятельности. Барнаул: Изд-во АлтГТу, 2009.

2. *Поспелов Д.А.* Моделирование рассуждений. Опыт анализа мыслительных процессов. М.: Радио и связь, 1989.

СРАВНЕНИЕ МЕТОДОВ ПОВЫШЕНИЯ КАЧЕСТВА ИЗОБРАЖЕНИЯ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

А.А. Полетаев, магистрант

Научный руководитель Р.Т. Файзуллин, проф., д.т.н.

г. Омск, ОмГТУ, каф. ССИБ, poletaev.andrew@gmail.com

Понятие качества изображения неоднозначно, под ним может подразумеваться как более приятное для наблюдателя изображение (экспертная оценка), отсутствие искажений, так и некие количественные параметры. С целью исключения неоднозначности для сравнения методов использовалось эталонное изображение, подвергающееся ис-

кажению, с последующим применением различных методов повышения качества, что позволило использовать не только критерий визуального восприятия, но и численно оценить работу каждого метода. Далее в статье под «качеством» будем понимать только пространственное разрешение, а при работе с «синтетическими», искусственными данными – меру отклонения полученного изображения от исходного.

В однокадровых (single-frame) системах применяются наиболее простые в реализации и хорошо известные методы, такие как билинейная и бикубическая интерполяция, комбинации различных фильтров и т.д.

Многокадровые (multi-frame) системы являются наиболее перспективными, так как позволяют использовать главное преимущество систем видеонаблюдения: наличие множества кадров, содержащих информацию об объекте наблюдения [1, 2].

Однако существует фундаментальное ограничение, не позволяющее напрямую использовать данные методы: каждый кадр, как правило, отображает одновременное и неупорядоченное движение множества объектов. Для решения данной проблемы ранее было предложено использовать методику, состоящую в выделении из каждого кадра той его части, которая соответствует объекту [3].

Сверхразрешение

Под сверхразрешением (super-resolution) понимается подход к увеличению пространственного разрешения изображения, сходный с методами восстановления изображений. Необходимым условием является наличие точной информации о взаимном смещении в исходной последовательности изображений. В настоящее время существует множество методов, реализующих данный подход [4–6].

Далее по тексту под «сверхразрешением» будем понимать алгоритм, предложенный Michal Irani и Shmuel Peleg [7]. Реализация упрощённой версии данного алгоритма в виде программы на языке Python (не учитывалось влияние шума, так как использовалось искусственное изображения) была использована для сравнения с методами интерполяции.

Сравнение методов

Сначала исходное изображение, представленное на рис. 1, было уменьшено и подвергнуто небольшим сдвигам на несколько пикселей в произвольных направлениях. Следующим шагом к уменьшенным изображениям применялись следующие методы:

– билинейная интерполяция;
– бикубическая интерполяция;
– бикубическая интерполяция с применением фильтра «резкость»;
– сверхразрешение.

Результаты приведены на рис. 2.

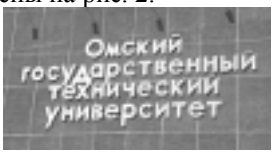
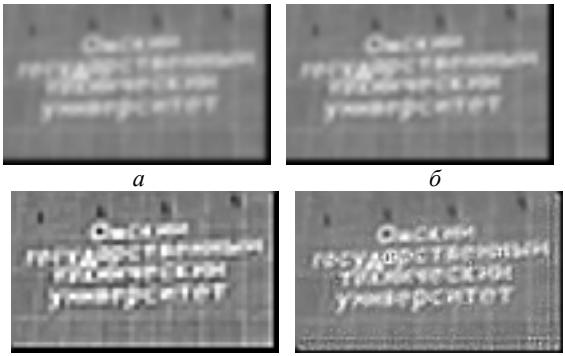


Рис. 1. Исходное изображение



а *б*

в *г*

Рис. 2. Результат применения методов повышения качества: *а* – билинейной интерполяции; *б* – бикубической интерполяции; *в* – бикубической интерполяции с применением фильтра «резкость»; *г* – сверхразрешения

Для оценки качества будем использовать критерий среднеквадратического отклонения (СКО) двух изображений. Выбор данного критерия имеет ряд преимуществ: его просто подсчитать и легко оценить. Кроме того, в случае использования искусственных данных имеется исходное изображение, которое искажается и с которым происходит сравнение полученного результата, то есть в нашем случае параметр имеет объективный характер. При использовании реальных данных эталонного изображения нет и использование данного критерия некорректно.

Для вычисления СКО двух изображений f_1 и f_2 размера $M \times N$ воспользуемся следующей формулой [8, 9]:

$$e_{CKO} = \left[\frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(f_1(i,j) - f_2(i,j) \right)^2 \right]^{1/2}. \qquad (1)$$

Анализ результата

Результат работы каждого из оцениваемых методов приведён на рис. 2. Количественные параметры, вычисленные в соответствии с формулой (1), приведены в таблице.

Полученные данные в общем согласуются с критерием визуального восприятия, за исключением неожиданно большой среднеквадратичной оценки результата, представленного на рис. 2, *в*: фильтр резкости усилил искажения, что привело к увеличению параметра, хотя визуально данный результат превосходит первые два.

Исходя из полученного результата, можно сделать вывод о превосходстве методов многокадровой обработки изображений и метода сверхразрешения в частности, над методами улучшения, использующими только одно изображение.

Величина ошибки

Оцениваемый метод	СКО
Билинейная	37,087
Бикубическая	38,071
Бикубическая с применением фильтра «резкость»	45,340
Сверхразрешение	27,014

ЛИТЕРАТУРА

1. *Frederick W. Wheeler, Xiaoming Liu, Peter H.Tu, Ralph T. Hoctor*. Multi-frame image restoration for face recognition // Proc. of IEEE Signal Processing Society: Workshop on Signal Processing Applications for Public Security and Forensics (SAFE).

2. *Aloysius K. Mok, Deji Chen*. A Multiframe Model for Real-Time Tasks // IEEE Transactions on Software Engineering. 1996. Vol. 23. P. 635–645.

3. *Полетаев А.А., Файзуллин Р.Т.* Применение сверхразрешения в задаче повышения качества видеоизображения объекта наблюдения // Научная сессия ТУСУР–2010. Томск: В-Спектр, 2010. Ч. 3. 280 с.

4. *Park S.C., Park M.K., Kang M.G.* Super-resolution image reconstruction: a technical overview // IEEE Signal Processing Magazine. 2003. Vol. 20, Issue 3. P. 21–36.

5. *Sroubek F., Cristobal G., Flusser J.* A Unified Approach to Superresolution and Multichannel Blind Deconvolution // IEEE Trans. Image Processing. 2007. Vol. 16. P. 2322–2332.

6. *Farsiu S., Robinson D., Elad M., and Milanfar P.* Fast and Robust Multi-frame Super-resolution // IEEE Transactions on Image Processing. 2004. Vol. 13, № 10. P. 1327–1344. October.

7. *Irani M., Peleg S.* Super Resolution From Image Sequences // ICPR. Vol. 2, 1990, June. P. 115–120.

8. *Bradski G., Kaehler A.* Learning OpenCV // O'Reilly Media, Inc, 2008. 526 p.

9. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. М.: Техносфера, 2005. 1072 с.

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННУЮ СИСТЕМУ

А.В. Поварницына
Научный руководитель В.В. Золотарев, зам. директора института информатики и телекоммуникаций, доцент, к.т.н.
г. Красноярск, Сибирский государственный университет им. М.Ф. Решетнева, vee2005@mail.ru

В настоящее время роль обеспечения информационной безопасности является одной из приоритетных задач. Управление информационной безопасностью – важный вид деятельности, целью которого является контроль процессов обеспечения информацией и предотвращение ее несанкционированного использования. Для решения проблемы обеспечения информационной безопасности необходим анализ угроз, рисков и их возможных последствий.

Целью данной работы является разработка методики оценки воздействия на информационную систему.

Можно выделить следующие задачи:

– разработка системы показателей для классификации факторов воздействия на информацию;

– определение параметров, от которых зависит функция воздействия;

– выбор контрольных точек исследуемой системы;

– получение зависимостей воздействия от параметров системы;

– аналитическое описание функции воздействия;

– анализ полученных результатов.

Информационная система представляется как ориентированный граф, вершинами которого будут являться элементы системы, а ребрами – связи (зависимости) между элементами. Элементы системы выбираются таким образом, чтобы наиболее точно описать систему.

Качественные характеристики системы, которые изменяются под влиянием воздействия, – конфиденциальность, целостность, доступность. Конфиденциальность предполагает комплексную оценку недоступности и нераскрываемости процесса обработки информации для неуполномоченных лиц. Целостность предполагает комплексную оценку нахождения процесса обработки информации в неискаженном, неизменном виде по отношению к некоторому определенному состоянию. Доступность предполагает комплексную оценку возможности получения и использования со стороны лица, принимающего решение, требуемых ему информационных ресурсов в рамках существующего процесса обработки информации. По изменению характеристик оценивается функция воздействия.

Каждая поставленная задача решается последовательно. Объединение классификаторов системы факторов воздействия позволяет выявить совокупность неблагоприятных факторов, связанных с множеством свойств системы. При классификации факторов, которые могут приводить к реализации информационных рисков, были использованы государственные стандарты в области информационной безопасности (ГОСТ Р 50922–2006, ГОСТ Р 512750–2006, ГОСТ Р ИСО/МЭК ТО 19791–2008 и др.), доктрина информационной безопасности и другие документы министерств и ведомств.

НЕЯВНЫЙ ДОСТУП К КОНФИДЕНЦИАЛЬНЫМ ДАННЫМ В КОМПЬЮТЕРНОЙ СЕТИ

И.И. Прокопов, доцент каф. ЦРТС
г. Челябинск, ЮУрГУ, ПСФ, prokopov_2009@74.ru

При доступе к конфиденциальным данным через компьютерную сеть по клиент-серверной схеме используются авторизованные рабочие станции. Можно рассматривать такую локальную сеть как открытую распределенную среду, в которой пользователи со своих рабочих станций должны иметь возможность доступа к услугам на серверах в сети [1]. К серверам должны получать доступ только зарегистрированные пользователи, и сервер должен иметь возможность аутентифицировать запросы к сервисам. Пользователи (операторы) используют на рабочем месте электронные ключи для шифрования данных. В совокупности это дает надежный авторизованный доступ к данным, не предполагающий утечку информации к другим лицам. Но в ряде случаев возможен неявный доступ в отсутствие владельца ключа.

Способы и причины неявного доступа к данным

Под неявным доступом понимается доступ к данным неавторизованным оператором (т.е. не имеющим на это право).

Способы неявного доступа:

1. Доступ к данным неавторизованным оператором с авторизованной рабочей станции с использованием ключей шифрования, хранящихся на съемном носителе этой рабочей станции.

2. Доступ к данным неавторизованным оператором с неавторизованной рабочей станции с использованием копий ключей шифрования, хранящихся на съемном носителе этой рабочей станции. При этом способе требуется подделка аппаратных характеристик другой рабочей станции для целей ее авторизации на сервере в качестве легальной. При этом требуются ключи шифрования (копии) с оригинальной рабочей станции, не имеющие привязки к оборудованию и носителю, либо

оригинальный носитель. Рабочая станция расположена в локальной сети сервера.

3. Вход на авторизованную рабочую станцию с другой ЭВМ посредством программ удаленного доступа (администрирования), в том числе из сети Интернет. Ключи шифрования должны быть в наличии на оригинальном носителе (в случае аппаратной привязки) и подключены к ЭВМ. Доступ осуществляется с легальной рабочей станции и с оригинальными ключами. Доступ возможен и в рабочее время при отсутствии оператора.

Рассмотрим причины и условия, приводящие к неявному доступу.

1. Наличие подключенных оригинальных носителей ключей включенной рабочей станции при отсутствии авторизованного оператора на рабочем месте. В этом случае возможен доступ как удаленным способом, так и с консоли.

2. Наличие питания 220 В на рабочей станции в нерабочее время. В связи с наличием в современных аппаратных платформах средств удаленного администрирования посредством программного обеспечения BIOS компьютер может быть включен удаленно через сеть. В ряде случаев компьютеры не выключаются вообще для целей их администрирования (архивирование данных, резервное копирование, установка обновлений и ПО и т.п.). Если в помещение нет физического доступа, компьютер может быть использован для доступа через удаленный рабочий стол или терминальную программу.

Разделим условно все общеупотребимые виды ключей на две категории:

а) С привязкой к носителю. Простое копирование файлов с такого носителя либо невозможно (смарт-карты), либо бессмысленно, т.к. при смене носителя требуется перегенерация ключей при наличии оригинального носителя.

б) «Плавающие» ключи. Требуется всего лишь наличие соответствующих файлов по пути, указанному в драйверах доступа. Наиболее удобный для злоумышленника тип, т.к. копирование возможно по сети.

В некоторых организациях, имеющих клиентские части от 5–10 банков, образуется смесь всех возможных типов ключей, каждый из которых имеет свой носитель, включая ключи категории «б».

Основное условие, определяющее возможность реализации всех способов доступа, – это наличие носителей закрытых ключей шифрования в соответствующих портах ЭВМ при отсутствии оператора, а также наличие у неавторизованного оператора кода для идентификации владельца ключа (PIN-код). Этот код можно получить с помощью аппаратных или программных кейлогеров [2].

Модель неявного доступа

Модель неявного доступа представлена в виде матрицы доступа (таблица). Операторы и рабочие станции разделены на два типа – авторизованные и неавторизованные. Символ «X» означает возможность доступа к данным, «0» – отсутствие доступа к данным (с консоли), «1» – доступ к данным при особых условиях (например, физическое отсутствие авторизованного оператора). Параметр «время» имеет значения «рабочее» и «нерабочее».

Модель неявного доступа

		Время		Тип оператора		Тип раб. станции	
		раб.	нераб.	авт.	неавт.	авт.	неавт.
Время	раб.	–	–	X	0	X	1
	нераб.	–	–	0	X	0	X
Тип оператора	авт.	X	0	–	–	X	0
	неавт.	0	X	–	–	1	X
Тип раб. станции	авт.	X	0	X	1	–	–
	неавт.	1	X	0	X	–	–

Способы противодействия подмене (маскарадингу) оператора

1. Применение «тонких» клиентов-терминалов для доступа к данным с целью исключения программных кейлогеров и удаленного администрирования, предполагая при этом надежность администратора сервера баз данных и сервера аутентификации [1].

2. Запрет администрирования рабочей станции через сеть (только локальное администрирование), в особенности через сеть Интернет.

3. Изоляция авторизованной рабочей станции от других узлов локальной сети программно-аппаратными средствами [3].

4. Контроль наличия съемных носителей (и параллельно аппаратных кейлогеров) при покидании рабочего места, выключении ЭВМ. Возможно использование радиометок (RFID) для носителей ключей (при привязке ключей к носителю).

ЛИТЕРАТУРА

1. *Столлингс В.* Криптография и защита сетей: принципы и практика. 2-е изд.: Пер. с англ. М.: Изд. дом «Вильямс», 2001. 672 с.

2. *Хорев А.А.* Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. 436 с.

3. *Брэгг Р.* Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг: Пер. с англ. М.: ЭКОМ, 2006. 912 с.

ИССЛЕДОВАНИЕ ПРОГРАММНО-ТЕХНИЧЕСКОГО ЭЛЕМЕНТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

А.А. Роговский, студент
г. Томск, ТУСУР, ФВС, script-05@mail.ru

Для режимных объектов в условиях роста и широкого распространения в современном обществе угроз утечки и нарушения конфиденциальности информации жизненно важное значение имеют эффективные системы комплексной безопасности (физической защиты) и их главная составная часть – рубежи защиты зоны [1].

Как известно, СЗИ физических и виртуальных объектов создаются по принципу последовательного построения рубежей защиты, которые препятствуют распространению угроз и обеспечивают их своевременное обнаружение.

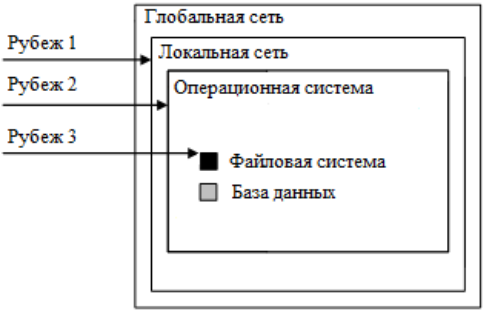


Рис. 1. Многоуровневый подход к защите зоны

В данной работе рассматриваются зоны для работы с информацией, ее хранения и передачи. Для каждой зоны существуют рубежи защиты (РЗ), отделяющие зоны друг от друга. Схема, по которой рассматривается каждый РЗ, приведена на рис. 2.

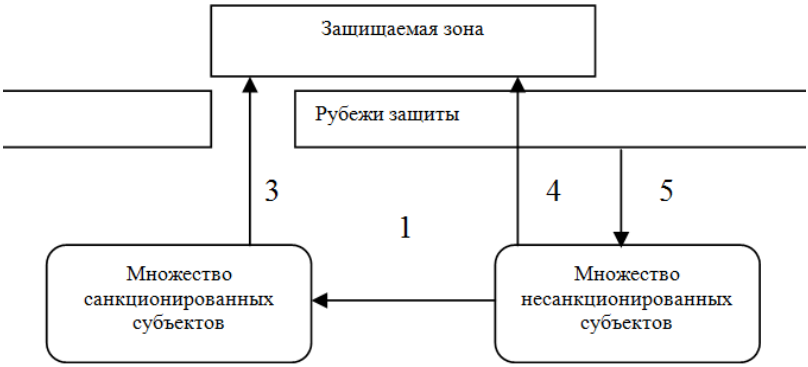


Рис. 2. Общая схема

1) Переход субъектов из несанкционированного множества в санкционированное.

Разграничение доступа. Пользователю выдаются соответствующие права доступа в защищаемую зону.

Во множестве субъектов действует контроль целостности, для исключения попыток нелегального изменения списка санкционированных субъектов

2) Возможность создания защищаемой зоны.

Определяется на стадии установки РЗ.

3) Санкционированное преодоление рубежей защиты.
4) Целостность рубежей защиты.
5) Конфиденциальность рубежей защиты.

ЛИТЕРАТУРА

1. / Рубежи защиты [Электронный ресурс]. Электрон. дан. Режим доступа: http://www.iz-news.ru/lect/464/

ЗАЩИЩЕННЫЕ ТЕРМИНАЛЬНЫЕ СИСТЕМЫ

С.А. Рожков, инженер, каф. ЦРТС
г. Челябинск, ГОУ ВПО «ЮУРГУ», conf@zserg.ru

Терминальная система, построенная по схеме сильный сервер – слабая рабочая станция, очень экономична и легко управляема. Однако она подвержена новым специфическим атакам на ее безопасность. Некоторые из этих атак и способы противодействия им изучены в данной статье. Исследования проводились на базе разработанной автором терминальной системы WTPRO. Предложена и реализована система взаимной аутентификации клиента и сервера WTPRO.

Терминальная система упрощает администрирование компьютерной сети и ее защиту. Вместе с тем такая система подвержена новым атакам, актуальным только для терминальных систем. Источником большинства проблем безопасности является то, что на терминале нет предустановленной ОС, а она загружается по сети. Используемые при этом протоколы разрабатывались в 80-х годах прошлого века [1, 2] и не обеспечивают необходимого сегодня уровня защищенности.

Обеспечить приемлемый уровень безопасности можно, установив сетевое оборудование, например корпорации CISCO, и правильно его сконфигурировав. Однако терминальные системы часто создаются на морально устаревшем оборудовании и используют недорогие серверы, следовательно, покупка сетевого оборудования, по цене сравнимая со стоимостью всей сети, не оправдана.

В 2005 г. на основе ядра Linux 2.6 был разработан дистрибутив Elinux [3], позволяющий проводить анализ сети, восстанавливать ОС, работать в качестве терминального сервера и рабочей станции. Достоинством дистрибутива был его небольшой размер (30 Мб). В 2006 г. был создан тонкий клиент ElinuxT (торговая марка WTPRO) [4; также 5, с. 447]. В настоящее время WTPRO – единственная, разрабатываемая в РФ терминальная система, в которую встроен модуль взаимной аутентификации.

Проблема аутентификации

Стандартные методы аутентификации, основанные на знании клиентом какой-либо уникальной информации о сервере и хранении этой информации на клиенте, не могут использоваться, т.к. тонкие клиенты загружаются по сети и не имеют локальных носителей информации.

В то же время решение проблемы аутентификации должно быть совместимым с существующими технологиями, простым и не дорогим.

Аутентификацию клиента можно осуществить, используя аппаратные ключи Etoken или RuToken, т.к. они не поддаются клонированию и выполняют криптографические операции на собственном процессоре. Аналогично, оснастив сервер аппаратным ключом, можно решить проблему аутентификации сервера.

Автором статьи разработаны расширения для виртуальных каналов RDP протокола, расширяющие функциональные возможности сервера терминалов, позволяющие производить идентификацию и аутентификацию клиента и сервера.

Алгоритм идентификации и аутентификации в виртуальных каналах

При создании новой терминальной сессии на сервере создается новый виртуальный канал, в дальнейшем все данные передаются через этот виртуальный канал.

Сервер получает запрос на доступ к сессии. Генерирует ЭЦП и случайную последовательность данных. Передает эти данные клиенту.

Клиент средствами аппаратной идентификации (ключ Etoken) проверяет данные сервера. В случае успеха добавляет к случайной последовательности данных свою случайную последовательность и генерирует собственную ЭЦП. Отправляет эти данные серверу.

Сервер, получив данные от клиента, проверяет их.

В случае успеха взаимной проверки клиента и сервера разрешается старт терминальной сессии. В противном случае сессия прерывается.

Периодическая взаимная аутентификация позволяет гарантировать подлинность клиента и сервера на протяжении всего сеанса работы.

На основе переданных от клиента к серверу и от сервера к клиенту случайных данных можно создать сессионный ключ шифрования и на его основе зашифровать передаваемые по виртуальному каналу данные.

Альтернативное решение – помещение в загрузчик сетевой карты открытого ключа сервера, при условии, что злоумышленнику блокирован физический доступ внутрь системного блока клиента. Алгоритм взаимной аутентификации аналогичен приведенному выше, за исключением того, что все ключи хранятся в bootrom и проверка ключей производится средствами центрального процессора, а не Etoken.

Рассмотрим аутентификацию сервера на базе протокола SSH средствами визуализации открытого ключа сервера. При подключении клиента к серверу на экране клиента появляется картинка – например, графический примитив дома или стула, изменяется ключ – изменяется картинка. Графические изображения можно сделать состоящими из большого количества элементов, в зависимости от длины ключа. Если длина ключа равна 256 бит, то часть бит задают цвет фона, часть – цвет элементов, количество элементов и т.д.

Один из возможных алгоритмов реализации этой идеи включен в программный продукт.

Также решением проблемы аутентификации является расширение протоколов DHCP и TFTP с сохранением совместимости путем добавления алгоритмов для аутентификации сервера и клиента, например, приведенных выше. Данное расширение протоколов будет включено в очередные версии терминала WTPRO.

Выводы

Терминальные системы в силу своей архитектуры защищены от многих угроз безопасности, которые актуальны для полноценных рабочих станций. В то же время они подвержены новым специфическим атакам. Поскольку тонкий клиент загружается по сети и не имеет локальных носителей информации, то очень важна аутентификация как клиента, так и сервера. В работе предложены три метода аутентификации терминальных серверов и клиентов: виртуальные каналы RDP протокола; расширение протокола DHCP; графическая аутентификация. Программно-аппаратные реализации этих методов включены в очередную версию терминального клиента WTPRO, разработанного и поддерживаемого автором.

ЛИТЕРАТУРА

1. *Джамса К., Коуп К.* Программирование для Internet в среде Windows. СПб.: Питер, 1996. 672 с.

2. RFC1533 http://www.faqs.org/rfcs/rfc1533.html

3. *Рожков С.А.* Дистрибутив Elinux // Матер. Всерос. науч.-практ. конф: «Безопасность информационного пространства». Екатеринбург: УГТУ–УПИ, 2005. С. 83–84.

4. *Рожков С.А.* Защищенная терминальная система WTPRO: Свидетельство о государственной регистрации программы для ЭВМ № 200961.

5. *Стахнов А.* Linux-сервер в Windows-окружении. СПб.: БХВ, 2007. 656 с.

ЗАДАЧИ МОДЕЛИРОВАНИЯ СЕТЕВОГО ТРАФИКА, ОТЯГОЩЕННОГО ПОМЕХАМИ

С.В. Русаков, аспирант каф. информационной безопасности

г. Тюмень, ТюмГУ, sergey_rus@bk.ru

Для решения ряда задач, связанных с обеспечением безопасности компьютерных сетей, в число которых можно включить такие задачи, как фильтрация трафика или сетевой мониторинг, необходимо построить математическую модель потоков, функционирующих в них. Одними из наиболее актуальных моделей потока пакетов данных в цифровых сетях передачи информации являются потоки, поведение которых определяется цепью Маркова (МС – Markov Chain). К ним относятся MAP (Markovian Arrival Process) и дважды стохастический поток событий с дискретными состояниями.

В настоящее время имеет место большое количество работ как по моделированию и исследованию свойств систем массового обслуживания (СМО) с такими потоками, так и по исследованию свойств самих потоков указанных типов.

При исследовании МС-потоков, как правило, решаются задачи следующих двух больших классов:

1) задача фильтрации интенсивности потока (или задача оценивания состояний потока событий) по наблюдениям за потоком (по наблюдениям за моментами наступления событий);

2) задача оценивания неизвестных параметров потока по наблюдениям за моментами наступления событий.

Эксперименты, проведенные рядом исследователей, показали достаточно точную аппроксимацию реальных потоков в информационных сетях различными моделями дважды стохастических потоков событий с дискретными состояниями [1–4].

Несмотря на то, что достаточно большое количество работ посвящено исследованию СМО с входящими МС-потоками, почти все они рассматривают идеальные варианты потоков однородных событий. Однако в реальных сетях связи события (информационные пакеты) неоднородны, а также часты случаи возникновения помех различ-

ной природы и свойства. Таким образом, представляется актуальным вопрос моделирования информационного потока, отягощенного помехами, существующими независимо от самого потока и накладывающимися на него.

Здесь и далее нормальным будем называть трафик без помех, и примем в качестве математической модели базового трафика дважды-стохастический поток событий в силу достаточно хорошего соответствия трафика информационной сети последнему.

Примеры моделей помехи и задач, связанных с ними

Для исследования свойств потока, отягощенного помехой, необходимо определить понятие и разновидности помехи и очертить круг задач, возникающих при наблюдении потока событий с помехой того или иного рода.

В качестве примера формализации помех можно предложить следующие:

а) на некотором интервале времени на нормальный трафик (базовый поток событий) начинает накладываться «паразитный», т.е. внедренный, чужеродный поток; в первом приближении внедренный поток можно принять как простейший с интенсивностью λ_P (рис. 1);

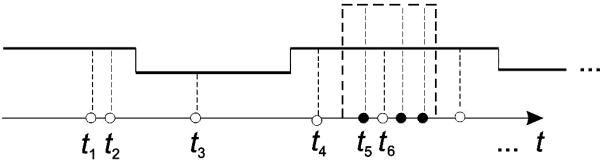


Рис. 1. Внедрение паразитного трафика в дважды-стохастический поток событий. Пунктирная линия – интенсивность паразитного трафика. Белые кружки – события потока. Черные кружки – события паразитного трафика

б) пакеты нормального трафика (события базового потока) исчезают с некоторой вероятностью $0 < p < 1$ (рис. 2).

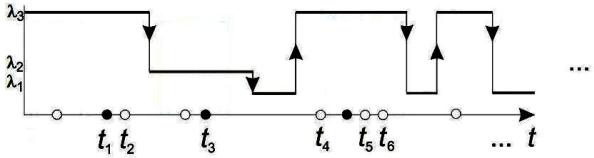


Рис. 2. Дважды-стохастический поток с помехой 2-го типа. Белые кружки – события потока. Черные кружки – потерянные (ненаблюдаемые) события потока

Для описанных помех можно предложить следующие задачи:

Для помехи типа «внедрение паразитного трафика»:

а) Известны τ_1, τ_2, …, τ_{n-1} – интервалы между соседними событиями в наблюдаемом базовом потоке, параметры которого известны. Определить, принадлежат ли следующие интервалы τ_n, τ_{n+1}, … потоку с помехой, т.е. началось ли наложение «паразитного» трафика на интервале τ_n?

б) Известны τ_1, τ_2, …, τ_{n-1} – интервалы между соседними событиями в наблюдаемом потоке событий с помехой. Определить, принадлежат ли следующие интервалы τ_n, τ_{n+1}, … базовому потоку с известными параметрами, т.е. закончилось ли наложение паразитного трафика на интервале τ_n?

в) Известны τ_1, τ_2, …, τ_{n-1} – интервалы между соседними событиями в наблюдаемом потоке событий с помехой. Определить интенсивность паразитного трафика λ_P и долю «паразитных» событий среди наблюдаемых. Определить апостериорную вероятность того, что наблюдаемое событие является событием паразитного трафика.

Для помехи типа «потеря событий»:

а) Известны t_1, t_2, …, t_{n-1} – моменты наступления событий в базовом потоке. Определить, началась ли помеха на интервале $[t_{n-1}, t_n]$.

б) Известны t_1, t_2, …, t_n – моменты наступления событий в потоке с помехой. Определить среднее ожидаемое количество исчезнувших событий; p – вероятность, с которой событие утрачивается. Оценить моменты, в которых произошла утрата событий.

Помимо рассмотренных задач, можно указать и другие задачи, требующие моделирования потока с помехой различного типа.

ЛИТЕРАТУРА

1. *Беккерман Е.Н., Катаев С.Г., Катаева С.С., Кузнецов Д.Ю.* Аппроксимация МС-потоком реального потока событий // Вестник ТГУ. 2005. №14. Прил. С. 248–253.

2. *Головко Н.И., Каретник В.О., Танин В.Е., Сафонюк И.И.* Исследование моделей систем массового обслуживания в информационных сетях // Сиб. журн. инд. матем. 2008. Т. XI. №2(34). С. 50–58.

3. *Царенков Г.В.* BMAP-потоки как модель трафика реальной сети // Матер. междунар. науч. конф. «Матем. методы повышения эффект. функционир. телекоммун. сетей». Минск: БГУ, 2005. С. 254–258.

4. *Ниссенбаум О.В., Пахомов И.Б.* Аппроксимация сетевого трафика моделью альтернирующего потока событий // Прикладная дискретная математика. 2009. Прил. №1. С. 78–79.

АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА «УЧЕТ ОЦЕНОК»

М.С. Саблин, Е.Ц. Чимитдоржиева,
Б.В. Шефф, студенты 4-го курса
Научный руководитель М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, каф. КИБЭВС, msvega@mail.ru

В современном мире компьютерные технологии плотно вошли в нашу жизнь. Компьютеры есть практически во всех сферах общества: в банках и офисах, на различных производствах и в медицинских учреждениях. Также они широко используются и в образовании: в каждой школе, в каждом университете или институте есть компьютерные классы, не говоря уже о машинах в кабинетах преподавателей и сотрудников. Информационные технологии эффективно применяются не только в процессе передачи знаний, но и в управлении образовательным процессом.

Управление образовательным процессом подразумевает работу с большим количеством однотипной информации (например, списки учащихся, оценки и т.д.) и сложными процессами по ее обработке. Примером таких сложных процессов являются контроль успеваемости студентов, процесс восстановления или перевода студентов с других специальностей или вузов. Данные проблемы вытекают из наличия разных учебных планов, по которым обучаются студенты, и необходимости их сравнения на соответствие прослушанных курсов, часов и способов оценивания по данному курсу. Процесс такого анализа и сравнения трудоемкий и времязатратный, требующий от специалиста большого внимания. Автоматизация подобных процессов положительно сказывается на качестве и скорости принятия решения. Средством для автоматизации подобных процессов являются клиент-серверные технологии с применением баз данных для хранения информации.

Для автоматизации данного процесса необходимо определить основные процессы и правила, по которым производится работа в данной предметной области. В основе учета успеваемости студентов лежат учебные планы по соответствующим направлениям и специальностям. Для того чтобы произвести учет успеваемости студентов факультета (курса, группы) за определенный учебный год, в системе должны быть заведены учебные планы, по которым учились студенты факультета (курса, группы) в данном учебном году.

На основе учебных планов курсов, специализаций, на определенный учебный год формируются индивидуальные учебные планы студентов. В индивидуальный учебный план студента входят:

• Учебные дисциплины, курсовые и научно-исследовательские работы, практики, итоговые госэкзамены, выпускные квалификационные работы, составляющие обязательную часть учебного плана курса.

• Дисциплины по выбору, включенные в учебный план курса.

• Факультативы, включенные в учебный план курса.

• Общевузовские факультативы, не входящие ни в один из учебных планов факультетов.

• Дисциплины из учебных планов других факультетов, курсов, специализаций, изучаемые студентом по его желанию.

При разработке автоматизированной системы планируется создать:

• Базу данных, содержащую полную информацию о студенте, относительно его успеваемости.

• Архив для хранения всех учебных планов как групповых, так и индивидуальных.

• Переводную карточку студента, которая отображает процесс перевода студента с одной специальности на другую или его восстановление на другой учебный план.

• Инструмент сравнения учебных планов.

• Инструмент создания отчетов по расчету средних показателей посещаемости и успеваемости студентов индивидуально, по группам или курсам для различных промежутков времени.

Использование баз данных для перечисленных направлений предоставляет очевидные преимущества (достаточно представить себе стопки бумаг, которые постоянно теряются, рвутся и не подлежат никаким изменениям). Вся интересующая информация хранится в аккуратных таблицах, связанных между собой, может быть в любое время просмотрена и изменена (естественно, при наличии соответственных прав).

В заключение стоит отметить, что создание в образовательном учреждении развитой информационной структуры, наполнение ее конкретным содержанием и организация свободного доступа к материалам на электронных носителях поможет всем участникам образовательного процесса решать не только управленческие, но и образовательные задачи.

ЛИТЕРАТУРА

1. [Электронный ресурс]. URL: http://www.edu.ru/modules.php?page_id=6&name=Web_Links&l_op=viewlinkinfo&lid=69481.

2. Статья «Научные базы данных в образовательном процессе» [Электронный ресурс]. URL: http://www.ict.edu.ru/vconf/files/10034.pdf.

3. Методические указания «Базы данных в образовательном процессе» [Электронный ресурс]. URL: http://iso.pippkro.ru/idnews.php?id=14.

РАЗРАБОТКА СТЕГАНОГРАФИЧЕСКОГО МЕТОДА ВСТРАИВАНИЯ ИНФОРМАЦИИ В ПРОСОДИЧЕСКИЕ ПАРАМЕТРЫ РЕЧИ

М.О. Салагай, аспирант каф. прикладной и экспериментальной лингвистики

Научный руководитель Р.К. Потапова, дир. Института прикладной и математической лингвистики Московского государственного лингвистического университета, проф., д.филол.н.

г. Москва, МГЛУ, ИПиМЛ, info@linguanet.ru

Широкое распространение мобильной связи, массовость и доступность сделали её наиболее привлекательной в качестве средства скрытой связи по открытым каналам с использованием стеганографии. Особый интерес для систем скрытой связи представляют подходы, в которых скрываемые данные внедряются в значения непрерывных несущих параметров – в фундаментальные характеристики, т.н. контейнеры речевого сигнала, не связанные непосредственно с их цифровым представлением. Одним из таких подходов является использование языковой просодии – совокупности таких фонетических признаков речи, как тон, громкость, темп и др. Значительная вариативность просодии, а также сложность формализации и анализа особенностей её индивидуальной и ситуационной изменчивости заключают в себе возможность её использования для внедрения скрытых данных в речь. Основой вариативности просодии является речевой инвариант, позволяющий вносить в него такие изменения, которые не выходят за пределы допустимого отклонения от нормы, а потому не заметны постороннему наблюдателю.

Концепция и содержание стеганографического метода

Концепция метода базируется на предположении о том, что если речевой сигнал на передающей стороне сегментировать на естественные однородные участки, то на этих участках можно выделить некоторые акустические параметры, преобразования которых в определенных пределах от нормы не различаются в канале связи ни на слух, ни с помощью инструментальных средств без сравнения с эталоном, которым владеет только передающая сторона.

В соответствии с основами традиционной фонетики [1, 2] материальными акустическими средствами языковой просодии являются частота основного тона (ЧОТ), контурность тона; интенсивность основного, второстепенного ударения; длительность и расположение пауз; уровень, длительность и интенсивность фразового акцента. Измерение и модификация некоторых параметров просодии – ЧОТ, интенсивно-

сти, длительности сегментов речи и длительности пауз путем обработки цифровых отсчетов сигнала не представляет алгоритмических трудностей [3].

Квантование речевого сигнала по времени и уровню является необходимым условием встраивания цифровых данных в просодические параметры речи. Квантование по времени – это сегментация речи на некоторые временные участки. На них измеряемый параметр (тон, интенсивность, длительность, расположение и др.) может быть описан простой функцией или правилом (звук–тишина, тональный–шумовой, подъем–спад, постоянство), а на границах этих участков происходят резкие изменения акустических характеристик.

Основой данного стеганографического метода встраивания информации является кодирование просодических параметров сегментов речи. Наиболее простым в реализации является метод кодирования по уровню с модуляцией индекса квантования (Quantization Index Modulation – QIM) [4]. Кодер QIM осуществляет линейное однородное квантование непрерывной или дискретной последовательности, подобное тому, какое используется при преобразовании аналогового сигнала в описывающую его последовательность чисел цифрового кода. Физически результат преобразования кодером, например, частоты основного тона на передающей стороне состоит в том, что из естественных, произвольных по частоте сегментов речи, поступающих на вход кодера, на выходе кодера формируется композитный сигнал – сегменты речи с нормированными частотами, соответствующими кодовой таблице внедряемых цифровых данных. На выходе кодера QIM необходимо иметь поточный криптографический преобразователь, который формирует из нормированных параметров новые, похожие на произвольные, естественные для человеческой речи, но зашифрованные параметры. В отличие от криптографических систем основной целью его является обеспечение неопределенности для нарушителя распределения скрываемого сообщения в контейнере.

Выводы

Разработанный стеганографический метод внедрения информации основан на квантовании речи по времени, для выделения однородных сегментов, и по уровню – для стеговнедрения скрываемых данных в сегменты. Для кодирования по уровню использован метод с модуляцией индекса квантования. Учет естественной сегментации речи и особенностей слухового восприятия человека позволил добиться высокой скрытности внедрения конфиденциальных данных. Для обеспечения неопределенности для нарушителя распределения скрываемого сообщения в контейнере используется криптографическое преобразование значений уровня несущих параметров.

Экспериментальные исследования в интересах выявления допустимых пределов модификации речи, скрытной пропускной способности, стойкости метода к помехам и преобразованиям в канале связи выполнены применительно к одному просодическому параметру – частоте основного тона речи. Эти исследования показали, что метод позволяет незаметно модифицировать данный параметр на 5–10% при пропускной способности стегоканала около 8–10 бит/с, обладает высокой стойкостью к воздействию передискретизации, сжатия с потерями, шумов и вокодерным преобразованиям, в связи с чем может быть использован в интересах скрытой связи.

ЛИТЕРАТУРА

1. *Потапова Р.К.* Речь: коммуникация, информация, кибернетика: учеб. пособие. 2-е изд. доп. М.: Эдиториал УРСС, 2001.

2. *Кодзасов С.В., Кривнова О.Ф.* Общая фонетика: Учеб. М.: Рос. гос. гуманит. ун-т, 2001.

3. *Neubaecker P., Gehle G., Kreutzkamp C., Granzow U.* Celemony Melodyne Studio v.3.2.2.2, [Computer program]. Copyriht 1999. 2008. by Celemony SoftwareGmBH, Valleystr. 25, 81371 Muenchen, Deutschland.

4. *Chen B., Wornel G.W.* System, method, and product for information embedding using an ensemble of non-intersecting embedding generators. U.S. patent pending. Licensing info.: MIT Technology Lic. Office. 1996.

СЕТИ НА ОСНОВЕ P2P-ТЕХНОЛОГИИ

Г.А. Шевчук, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, vampiric@sibmail.com

Можно ли современный интернет назвать свободным интернетом? Я считаю, что нельзя. Государство оказывает своё воздействие принимая новые законопроекты, вводя цензуру на размещаемый контент. Примерами могут служить события во Франции – Национальная ассамблея включает к рассмотрению анти-P2P закон, Google и цензура поисковых запросов Китая, цензура на Facebook, отключение интернета в Египте на 5 дней по приказу властей, запрет доступа к некоторым западным ресурсам, таким как YouTube, Twitter или Google, в ряде стран. Таких примеров очень много, и все они доказывают, что современный интернет испытывает жесткое влияние цензуры государства. Россию тоже не обошло стороной (пример: файлообменные сети и 4-я часть ГК РФ).

Каждый раз, размещая в сети информацию, неизбежно задумываешься о её безопасности и приватности. Кому принадлежит контроль над ней? Правительство, спецслужбы, Фэйсбук и др. располагают

большими объемами информации о нас. Это не означает, что нужно шифроваться и прятаться от них, ведь они зависят от нас не в меньшей мере. Злоупотребив закрытой информацией, они потеряют гораздо больше, чем приобретут, их репутация зависит от неприкосновенности личной информации.

Контроль доступа к «закрытой» информации весьма условен. Он зависит от кусочка кода где-нибудь на сервере. Желание взять всё под собственный контроль породило сообщество разработчиков, объединенных идеей о децентрализованной безопасной с точки зрения ограничения доступа к информации сети.

Очень перспективным является направление создания свободного интернета на основе p2p (peer-to-peer)-технологии. Весь контент в такой сети распределен между пользователями одноранговой сети, отправителем (сервером) является каждый участник, а вся информация собирается по кусочкам. Никто не знает, откуда и куда осуществляется пересылка.

P2P-сеть – это оверлейная компьютерная сеть, основанная на равноправии участников. В такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры.

P2P-сети позволяют использовать ресурсы множества компьютеров – участников этой сети, одновременно обеспечивая анонимность участников. Используя эти преимущества, успешно развиваются множество проектов, таких как Locker (проект децентрализованной социальной сети на P2P-протоколе Telehash), сервисы для организации p2p-трансляции видео, проекты распределенного интернета (Web-P2P-Web), распределенный p2p-хостинг.

Децентрализованные технологии перспективны и содержат очень много работы. Массовость и популярность можно получить, предложив нужные и понятные любому преимущества. В своей работе я хочу осветить вопросы касательно сетей на основе P2P, показать неоспоримое преимущество данной технологии, провести анализ существующих проектов и их решений и сравнить их с существующими аналогами, внести свой вклад в российское сообщество разработчиков.

ЛИТЕРАТУРА

1. Habrahabr [Электронный ресурс]. Режим доступа: http://habrahabr.ru/search/?q=p2p&target_type=posts

2. Гражданский кодекс Российской Федерации. От 18 декабря 2006 г. № 230-ФЗ. Ч. 4.

3. Лента.ру [Электронный ресурс]. Режим доступа: http://lenta.ru/

МОДЕЛИРОВАНИЕ ОЦЕНКИ ДОСТУПНОСТИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Е.К. Шипова, студентка 5-го курса радиотехнического факультет
г. Воронеж, Воронежский институт МВД России, iksjyndri@mail.ru

В настоящее время вопросы обеспечения информационной безопасности являются актуальными и весьма значимыми. Это обусловлено тем, что, с одной стороны, информация пронизывает все без исключения сферы человеческой деятельности и поэтому угрозы ее безопасности могут приводить к серьезным негативным последствиям, а с другой стороны, задача обеспечения полной безопасности информации на данный момент решения не имеет.

Под безопасностью информации в соответствии с [1] понимается состояние защищенности информации, при котором обеспечивается ее конфиденциальность, доступность и целостность, которые являются основными показателями эффективности информационной безопасности. Для оценок этих показателей используют методы математического моделирования, которые в настоящее время проработаны недостаточно. Это и определяет актуальность данной работы.

Оценка доступности информации при передаче с использованием телекоммуникационных систем. В соответствии с [1] доступность – это состояние информации, при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно. При этом понятие «беспрепятственно» не раскрывается, что затрудняет процесс оценки доступности. Поэтому для моделирования оценки доступности информации в телекоммуникационных системах (ТКС) первоначально следует конкретизировать это понятие. На наш взгляд, под беспрепятственностью следует понимать возможность субъекта за приемлемое время получить требуемую информацию. Таким образом, проверка доступности сводится к проверке выполнимости условия

$$T \le \hat{T}, \qquad (1)$$

где T – время получения информации, $\hat{T}$ – допустимое время для получения этой информации.

Согласно вышеизложенному предлагается под доступностью информации при передаче ее в ТКС понимать возможность адресата за приемлемое время получить в полном объеме требуемую информацию.

Рассмотрим способы получения оценок используемых в задаче параметров. Ограничение $\hat{T}$, как правило, может быть определено экспертами в зависимости от характера информации и субъекта, которому она предназначена. Поэтому решение вопроса оценки доступно-

сти информации в ТКС неотъемлемо связано с оценкой времени получения информации, которую можно определить следующим образом:

$$T = V / P, \qquad (2)$$

где V – объем передаваемой информации; P – пропускная способность ТКС при передаче данного объема информации.

Значение объема информации V, как правило, известно. Следовательно, для решения задачи оценки доступности информации необходимо разработать метод оценки пропускной способности ТКС P. Следует иметь в виду, что значение пропускной способности линий связи определяется в основном характеристиками ТКС, поэтому обратимся к разработке модели ТКС.

Модель телекоммуникационной системы. Для моделирования ТКС и процессов передачи информации в них удобно использовать методы теории графов [2]. Каждая ТКС включает узлы, соединенные линиями связи. Для каждой линии связи (ЛС) известна ее пропускная способность, т. е. объем передаваемой информации в единицу времени. Обозначим:

$U = \{u_1, u_2, ..., u_n\}$ – узлы телекоммуникационной системы;

$E = \{e_1, e_2, ..., e_m\}$ – ЛС между узлами;

$Q = \{q_1, q_2, ..., q_m\}$ – оценки величины пропускных способностей ЛС.

В таком случае моделью всей ТКС является ориентированный взвешенный связный граф $G = (U, E, Q)$.

Модель передачи информации в телекоммуникационной системе. Будем рассматривать процесс передачи данного объема информации от одного источника информации $v \in U$ к одному потребителю $w \in U$.

В каждом узле собирается информация, поступившая по всем входящим в него ЛС, и передается далее по исходящим из него ЛС. При этом выполняются следующие ограничения:

1) объем передаваемой информации в единицу времени r_j по ЛС e_j не превышает ее пропускной способности: $r_j \le q_j$, $j \in \{1,2,...,m\}$;

2) объем поступившей и переданной информации на каждом узле связи (кроме источника и стока), т. е. для всех $u \in \tilde{U} \setminus \{v, w\}$, совпадает: $\sum_{j \in E_u^+} r_j = \sum_{j \in E_u^-} r_j$, где E_u^+ – множество всех ЛС, входящих в узел связи u; E_u^- – множество всех ЛС, выходящих из узла связи u;

3) объем переданной из источника информации совпадает с объемом информации, полученной потребителем: $\sum_{j \in E_v^-} r_j = \sum_{j \in E_w^+} r_j$.

Выполнение указанных ограничений позволяет интерпретировать множество значений r_j, $j \in \{1,2,...,m\}$ как поток, протекающий от источника v к стоку w.

Оценка пропускной способности. Описанная выше модель позволяет под оценкой пропускной способности ТКС при передаче данного объема информации P считать величину максимального потока в графе $\tilde{G}$. Введем определения.

Разрезом графа называется множество его дуг, удаление которых увеличивает число компонент связности графа. Величиной разреза называется сумма весов входящих в него дуг.

В соответствии с теоремой Л.Р. Форда – Д.Р. Фалкерсона [3] величина максимального потока равна величине минимального разреза, такого, что сток и источник оказываются в различных компонентах связности. Таким образом, пропускную способностью ТКС можно оценивать величиной минимального разреза, т. е. суммой пропускных способностей всех дуг разреза.

Выводы. Разработанная модель позволяет получить значение пропускной способности ТКС при передаче данного объема информации P, а следовательно, оценку доступности информации по формулам (1)–(2). Полученную оценку можно рассматривать как приближенную оценку. Для ее уточнения следует учесть технические характеристики оборудования ТКС и, в частности, маршрутизаторов.

Данная модель может быть использована для оптимизации распределения средств на модернизацию ТКС, т. е. выбирать те ЛС, модернизация которых в наибольшей степени увеличивает пропускную способность ТКС.

ЛИТЕРАТУРА

1. Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056 – 2005. М.: Изд-во стандартов, 2005. 105 с.

2. *Зыков А.А.* Основы теории графов / А.А. Зыков. М.: Наука, 1987. 384 с.

3. *Форд Л.Р.* Потоки в сетях / Л.Р. Форд, Д.Р. Фалкерсон. М.: Мир, 1966. 276 с.

МЕТОД РЕЗОЛЮЦИЙ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ В МЕДИЦИНСКОЙ ЭКСПЕРТНОЙ СИСТЕМЕ

Е.Ф. Щипунов, аспирант
Научный руководитель Р.В. Мещеряков, проф., д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, sef@security.tomsk.ru

Начиная с момента формирования понятия «искусственный интеллект», человечество пытается запрограммировать процесс мышления, рассуждения и принятия решений. Задача довольно нетривиальна, однако её решение стоит затраченных усилий.

Искусственный интеллект в контексте программного обеспечения понимается как интеллектуальная программа, позволяющая анализировать и принимать решение подобно тому, как это делает человек. Преимуществ систем, использующих элементы искусственного интеллекта в качестве базового механизма принятия решений, очень много. В частности, такие системы более доступны пользователям, а значит, доступными становятся и экспертные знания, находящиеся в ней. Такие системы способны объяснять полученное решение, в отличие от эксперта, который может оказаться в затруднительном положении. Отсутствие эмоций, плохого самочувствия, открытость и надёжность – преимущества экспертных систем (ЭС), дополняющие этот список [1].

В данной статье рассматривается метод принятия решений на основе резолюций. Данный метод рассматривается в контексте экспертной системы для ранней диагностики сердечно-сосудистых заболеваний с упором на тромбоэмболию.

Систему поддержки принятия решений (СППР) следует создавать тогда и только тогда, когда решение задачи невозможно запрограммировать. Если для достижения цели можно составить алгоритм, то неэффективно применять аппарат искусственного интеллекта. Медицинская ЭС должна оперировать множеством весьма специфических данных. Это могут быть ранжированные переменные, числовые показатели, текстовая информация и т.п. Алгоритмизация принятия решения среди подобных пластов информации с минимальным уровнем ошибки – задача неразрешимая.

Процедура принятия решений – это доказательство обоснованности принятого решения. Для этих целей оптимальным представляется использование правил вывода, называемых резолюциями. Резолюция представляет собой общее правило вывода, на основании которого вычисляются искомые резольвенты. Идея данного метода заключается в том, что доказательство истинности или ложности выдвинутого утверждения выполняется методом от противного [2]. Например, выражение

$$\left(A_1 \wedge A_2 \wedge \ldots \wedge A_N\right) \rightarrow B$$

будет являться истинным, если взять противоположную гипотезу и попробовать доказать истинность выражения. Если в процессе доказательства получается пустая резольвента, то гипотеза истинна. В данном случае, согласно методу резолюций, выражение для доказательства примет вид

$$\neg\left(A_1 \wedge A_2 \wedge \ldots \wedge A_N\right) \rightarrow B$$

В общем виде, целью метода резолюций является получение резольвенты на основании родительских выражений. В связи с этим метод резолюций целесообразно использовать вместе с дедуктивной логикой. Такая связка позволит использовать особенности обоих методов – метода резолюции, позволяющего доказать ложность выражения, и дедукции, когда процесс мышления направлен от общей гипотезы к частным утверждениям.

Применительно к обсуждаемой СППР процесс принятия решения на основе дедуктивной логики с использованием метода резолюций носит характер обратного логического вывода. Схематически данный процесс представлен на рис. 1.

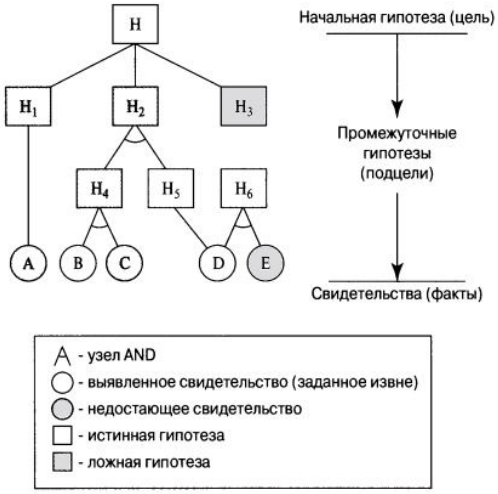


Рис. 1. Обратный логический вывод

Для того чтобы применить метод резолюции в ЭС, необходимо привести его к соответствующей форме. Для этого необходимо:

1. Удалить из высказывания все знаки условной операции с помощью эквивалентной её подстановки.

2. Устранить знаки отрицания, сведя область действия к атомарным значениям.

3. Устранить кванторы существования.

4. Преобразовать в конъюнктивную нормальную форму, в которой операции выполняются над парами дизъюнктов.

5. Убрать оставшиеся кванторы всеобщности.

6. Устранить все конъюнктивные знаки, записав высказывания как множество выражений.

В качестве примера принятия решения можно привести следующий. Рассмотрим предикаты A, B, C, D. Предикат A: «у пациента гиподинамия»; B: «пониженная СОЭ (скорость оседания эритроцитов)»; C: «повышенный уровень эритроцитов»; D: «риск развития тромбоэмболии». С помощью метода резолюций отыщем правильное решение относительно пациентов с гиподинамией. Для этого предположим, что пациенты с гиподинамией не обладают повышенным риском развития тромбоэмболии. Согласно вышеописанной схеме, необходимо преобразовать искомые выражения, т.е. $A \rightarrow D \equiv \sim A \vee D$. Методом от противного, получаем отрицание: $\sim(\sim A \vee D) \equiv A \wedge \sim D$. В данном высказывании отсутствуют кванторы всеобщности и существования, поэтому преобразование выражения с целью их устранения не требуется. Далее получаем конъюнктивную нормальную форму дизъюнктивных пар переменных: $(\sim A \vee B) \wedge (\sim B \vee C) \wedge (\sim C \vee D) \wedge A \wedge \sim D$.

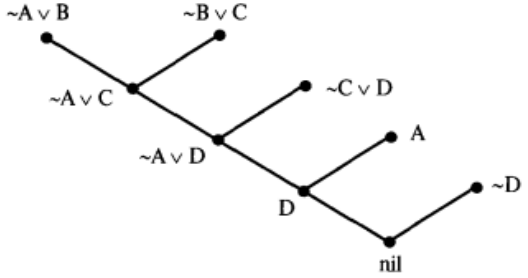


Диаграмма дерева опровержения резолюции изображена на рис. 2.

Рис. 2. Диаграмма дерева опровержения резолюции

Известно, что $D \wedge \sim D$ есть противоречие. Поэтому утверждение о том, что все пациенты с гиподинамией подвержены риску возникновения тромбоэмболии более остальных пациентов, вследствие пониженной СОЭ и повышенного числа эритроцитов, является справедливым. Таким образом, метод резолюции, применительно к задаче построения медицинской ЭС, представляет необходимые возможности для успешного решения данной задачи.

Если же в базе знаний ЭС имеется множество правил, составляющих общую совокупность знаний о тромбоэмболии, то работа системы будет в точности повторять схему, изображённую на рис. 1. Поскольку для получения диагноза необходимо сначала предоставить всю имеющуюся о пациенте информацию, а только потом, выдвинув гипотезу о возможном диагнозе, пытаться её либо доказать, либо опровергнуть.

ЛИТЕРАТУРА

1. *Джарратано Д., Райли Г.* Экспертные системы. Принципы разработки и программирования. М.: Вильямс, 2007. 1152 с.

2. *Artificial* Intelligence. [Электронный ресурс] Department of Computing, Imperial College, London. URL: http://www.doc.ic.ac.uk/~sgc/teaching/v231/

АНАЛИЗ ЗАЩИЩЕННОСТИ СЕТИ

С.С. Безносиков, Д.А. Деревянкин, Э.Р. Заитова, А.И. Покрышкин, М.А. Швецова, Е.Г. Шубникова, Т.Н. Шуклина, студенты

Научный руководитель Г.А. Праскурин, ст. преподаватель каф. КИБЭВС

г. Томск, ТУСУР, ФВС, каф. РЗИ, каф. КИБЭВС, error313@sibmail.com

В настоящее время не существует достаточно четких определений процедуры анализа защищенности вычислительной сети и методики ее выполнения, возможных на этапах проектирования и эксплуатации, что в значительной мере препятствует внедрению технологий анализа и аудита информационной безопасности ВС [1].

Такой анализ необходим при контроле и мониторинге защищенности компьютерных сетей, при аттестации автоматизированных систем (компьютерных сетей) и сертификации средств вычислительной техники по требованиям действующих нормативных документов и требует обработки большого объема данных в условиях дефицита времени.

Защищенность компьютерной сети определяется как степень адекватности реализованных в ней механизмов защиты информации (такие, как идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование) существующим в данной среде функционирования рискам, связанным с осуществлением угроз безопасности информации, т.е. способность механизмов защиты обеспечить конфиденциальность, целостность и доступность информации. Защищенность может оказывать и зачастую оказывает решающее влияние на показатели эффективности функционирования компьютерных сетей. Под угрозой понимается совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба функционированию компьютерной сети. Угрозы могут классифицироваться по различным признакам. В частности, по характеру происхождения угрозы делятся на две группы: умышленные и естественные. Основными умышленными угрозами считаются: подключение нарушителя к каналам связи, несанкционированный доступ, хищение носителей информации. К основным естественным угрозам

относятся: несчастные случаи (пожары, аварии, взрывы), стихийные бедствия (ураганы, наводнения, землетрясения) и ошибки в процессе обработки информации (сбои аппаратуры) [2]. При анализе защищенности компьютерных сетей во внимание следует принимать все разновидности угроз, однако наибольшее внимание должно быть уделено тем из них, которые связаны с действиями человека, злонамеренными или иными. Поэтому естественные угрозы в нашем исследовании не рассматриваются.

Необходимость анализа защищенности компьютерных сетей на этапах проектирования и эксплуатации диктуется низким уровнем эффективности существующих средств обеспечения информационной безопасности.

На основе вышеизложенного актуальной является разработка подхода, объединяющего множество моделей и методику для реализации детального анализа защищенности компьютерных сетей. Достижение данной цели остро необходимо, так как использование средств автоматизации детального анализа защищенности будет способствовать созданию и эксплуатации более безопасных компьютерных сетей.

Цель проекта: разработка методики анализа защищенности компьютерных сетей.

Для достижения данной цели необходимо решить следующие задачи:

1. Создание модели анализируемой компьютерной сети.
2. Разработка моделей компьютерных атак и нарушителя анализируемой компьютерной сети.
3. Анализ существующих методов и средств анализа защищенности.
4. Разработка методики анализа защищенности сети.

Методика анализа защищенности сети позволит проектировщику и/или системному администратору сети определять не только известные уязвимости в используемом программном и аппаратном обеспечении, но и определять последовательности выполняемых нарушителем атакующих действий, выявлять «узкие» места в безопасности компьютерной сети, моделировать поведение нарушителей, принимать обоснованные решения по составу используемых или планируемых к использованию средств обеспечения безопасности [3].

До настоящего момента нами была решена задача по созданию модели анализируемой сети, подразумевающей построение локальной сети.

Построение локальной сети условно можно разделить на следующие этапы:

- Виртуализация сети.
- Проектирование сети.

- Администрирование сети.
- Тестирование сети.
- Сканирование сети.

В результате проделанной работы были выполнены следующие задачи:

5. Изучение основ построения сетей на базе ОС Windows и ОС семейства Unix.
6. Создание сетей и виртуализация.
7. Тест созданных сетей на наличие уязвимостей.
8. Изучение методов устранения уязвимостей.

Тем самым была решена задача создания модели анализируемой компьютерной сети – первого этапа в разработке методики.

ЛИТЕРАТУРА

1. http://www.itsec.ru/articles2/Oborandteh/analiz_zaschischen_vy4is lit_seti_metodika_ego_proved

2. Доктрина информационной безопасности Российской Федерации.

3. *Котенко И.В., Степашкин М.В.* Интеллектуальная система анализа защищенности компьютерных сетей на различных этапах жизненного цикла // Тр. междунар. науч.-техн. конф. «Интеллектуальные системы (AIS-05)» и «Интеллектуальные САПР (CAD-2005)». М.: Физматлит, 2005.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МЕСТНОСТИ: СЕГМЕНТАЦИЯ ИЗОБРАЖЕНИЙ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ

А.А. Сметанин, магистрант каф. ВТ

Научный руководитель Е.Ф. Стукалина, доцент, к.т.н.

г. Ижевск, ИжГТУ, das-len@yandex.ru

В соответствии с [1, 2] под **информационной безопасностью объектов местности** (ИБ ОМ) в настоящей работе понимается состояние защищенности образов и параметров растительных покровов и грунтов, гидрографии, рельефа, инженерных сооружений, контурных и других объектов.

Естественная база ОМ – поверхность Земли. Современным представлением поверхности Земли и находящимися на ней ОМ является цифровая модель местности (ЦММ), одним из основных способов формирования которой в настоящее время является автоматизированное дешифрирование (профессиональный термин, практический аналог термину «дешифрование») материалов аэрокосмической съемки (МАКС).

Поставим задачу создания ЦММ по результатам дешифрирования МАКС.

Изображения дистанционного зондирования (ДЗ) – материалы аэрокосмической съемки, в настоящее время являются основным источником цифровой картографии, в общем случае – цифровой модели местности (ЦММ).

Представим ЦММ в виде множества контуров с описанием [2–4]:

$$M = \{L_i, S_i\},\ i = 1,...,I\ , \tag{1}$$

где L_i – множество метрических характеристик контура G_i; S_i – множество семантических характеристик G_i.

В свою очередь:

$$L_i = \{K_{i,j}, P_i\}, j = 1,...,J, i \neq j\ , \tag{2}$$

где $K_{i,j}$ – множество контурных сегментов, ограничивающих G_i и являющихся граничными между G_i и G_j; P_i – множество контурных признаков (периметр, изрезанность границ и т.п.).

Контурные сегменты определяются следующим образом:

$$K_{i,j} = \{V_{i,j}, c_i, c_j\}, \tag{3}$$

где $V_{i,j}$ – множество координат вершин ломаной, аппроксимирующей сегмент; c_i и c_j – коды G_i и G_j.

Задача выделения контуров – сегментация исследуется в различных областях обработки и распознавания изображений [3] и содержит основные технологические функции: утоньшение линий контуров; устранение разрывов. Термин «утоньшение» – наиболее общий термин для обозначения процесса преобразования линий, имеющих ширину в несколько пикселей, в линии единичной ширины. К операциям утоньшения предъявляются, как правило, следующие основные требования: после преобразования все контуры имеют единичную толщину; связность объектов изображения и фона должна быть сохранена; преобразование не нарушает топологию изображения, т.е. линиям и узлам исходного изображения соответствуют линии и узлы преобразованного изображения.

Для утоньшения контуров можно воспользоваться алгоритмом выделения средних линий на основе вписанных квадратов.

Рассмотрим алгоритм выделения средних линий на основе вписанных квадратов. На первом шаге выполняется сканирование объекта скелетизации. В процессе сканирования выделяются средние точки, каждому пикселю объекта присваивается индекс.

Индекс – это размер квадрата, нижний левый угол которого совпадает с текущим пикселем. Индекс вычисляется по формуле

$$d = \min(a,b,c) + 1, \tag{4}$$

где d – индекс текущего пикселя, a – индекс пикселя сверху, b – индекс пикселя слева сверху, c – индекс пикселя слева.

Если выполняется условие:

$$\begin{cases} b \geq a, \\ b \geq c, \\ b \geq d, \end{cases} \quad (5)$$

то квадрат является вписанным и заносится в матрицу размеров квадратов. На втором шаге устраняются разрывы в скелетных линиях. По градиенту в матрице размеров квадратов связываем найденные квадраты.

Переменные индексирования:

b	a
c	d

Алгоритм выделения средних линий на основе вписанных квадратов выполняется за гарантированное время $O(n)$, что быстрее известных алгоритмов триангуляции [7], которые решают эту задачу за гарантированное время $O(n \log n)$.

Выводы

1. Подтверждено определение информационной безопасности объектов местности.

2. Поставлена задача формирования цифровой модели местности и, в частности, контурной информации.

4. Рассмотренный алгоритм выделения средних линий на основе вписанных квадратов является усовершенствованием алгоритма на основе триангуляции.

5. Трудоемкость рассмотренного алгоритма выделения средних линий линейная.

ЛИТЕРАТУРА

1. *Белов Е.Б.* Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. М.: Горячая линия – Телеком, 2006. 544 с.

2. *Сметанин А.М.* Информационная безопасность объектов местности: автоматизированное дешифрирование материалов аэрокосмической съемки // Доклады Том. гос. ун-та систем управления и радиоэлектроники. Томск: Изд-во ТУСУР, 2008. № 2 (18), ч. 1. С. 18–19.

3. *Стукалина Е.Ф.* Программно-аппаратные средства анализа и распознавания изображений дистанционного зондирования. Дис. ... канд. техн. наук. Ижевск, 2002. 156 с.

4. *Сметанин А.М.* Природно-социальные системы: Прикладные проблемы распознавания образов // Интеллектуальные системы в производстве: Период. науч.-практ. журн. 2003. № 1 / Отв. за вып. В.А. Тененев. Ижевск: Изд-во ИжГТУ, 2003. С. 65–80.

СЕМЕЙСТВО КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ С НЕФИКСИРОВАННОЙ СТРУКТУРОЙ «BIMOT»

Е.А. Сопов, студент
Научный руководитель О.О. Евсютин, аспирант каф. КИБЭВС
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, sea-kg@ya.ru

Многие современные симметричные криптографические алгоритмы построены на основе сети Фейстеля (DES, ГОСТ 28147–89), изображенной на рис. 1, и структура каждого из алгоритмов известна [1].

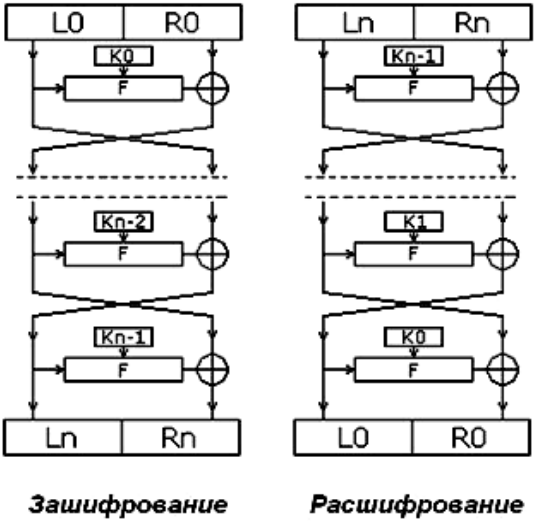


Рис. 1. Сеть Фейстеля

Такие алгоритмы используют ключ, равный 128, 256, 512 бит и выше, что в свою очередь дает возможность злоумышленнику распараллеливать перебор ключа [2, 3].

Возможны следующие изменения существующего подхода к конструированию симметричных шифров: отказ от фиксированной длины ключа и определение необходимых элементарных операций преобразования из ключевой информации.

Во второй версии «BIMOT» эти предложения были реализованы. Из ключевой информации формировались операции преобразования и операнды к ним, в таком случае ключевая информация могла быть любой длины. Схема работы данного алгоритма приведена на рис. 2.

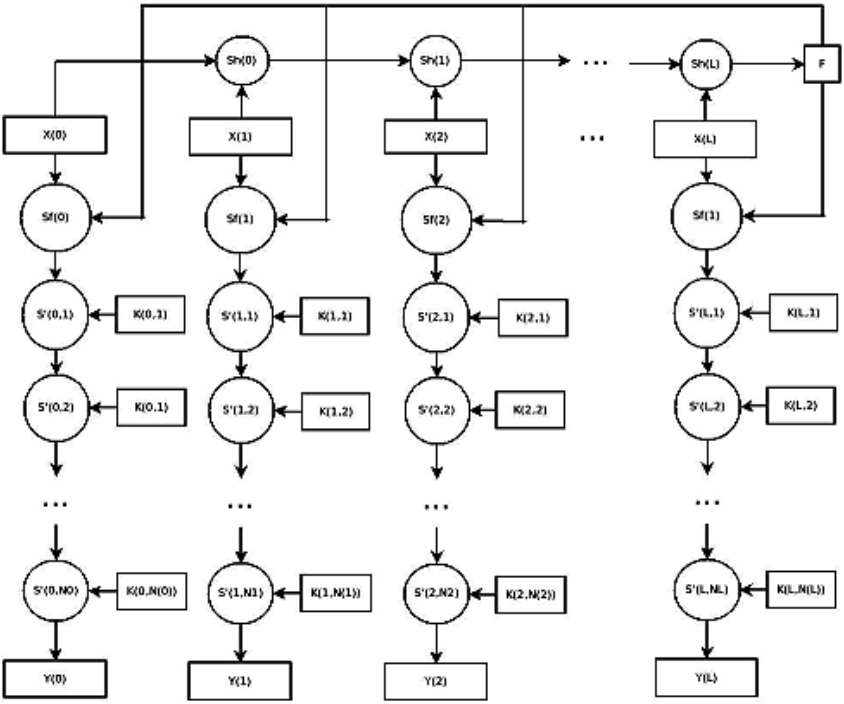


Рис. 2. Основной алгоритм шифрования «BIMOT»

Для проведения теста на скорость был реализован класс на языке программирования C++ [4]. Тестирование проводилось на машине с процессором Intel(R) Celeron(R) CPU 560 @ 2,13 GHz. Результаты приведены в таблице.

Скорость криптографических преобразований

Объем данных	Скорость зашифрования, Кбит/с	Скорость расшифрования, Кбит/с
256 Кб	17394,5	959,386
5 Мб	17679,1	960,595
10 Мб	17845,9	950,462

Во второй версии алгоритма были выявлены некоторые недостатки, поэтому была осуществлена разработка третьей версии, в которой используются 729 операций (для сравнения, в предыдущей версии использовалось только четыре операции), что значительно повысило криптостойкость алгоритма. Также была изменена процедура генерации ключевой последовательности из ключа.

В настоящее время продолжается работа над созданием и тестированием новой версии алгоритма шифрования «BIMOT».

ЛИТЕРАТУРА

5. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.

6. *Информационная* безопасность. Стандарты и алгоритмы шифрования [Электронный ресурс]. Режим доступа: http://naukoved.ru/content/view/826/35.

7. *О применяемых* алгоритмах шифрования [Электронный ресурс]. Режим доступа: http://www.familytree.ru/ru/cipher/cryptc.htm

8. *Язык* программирования C++. Специальное издание. СПб.: Бином, 2008. 1104 с.

ЗАЩИТА МОБИЛЬНОГО ТЕЛЕФОНА, РАБОТАЮЩЕГО НА ОСНОВЕ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

А.Ю. Сорокин, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, sasha15@bk.ru

Сотовый телефон предназначен для работы в сетях сотовой связи. В настоящее время сотовая связь – самая распространённая из всех видов мобильной связи. Суммарное количество проданных сотовых телефонов в 2010 г. превысило 1 млрд 300 млн экземпляров, рост продаж по сравнению с 2009 г. составил 18,5% [1].

Использование мобильного телефона обуславливает хранение небольшой личной, но порой действительно ценной информации.

Утеря подобных данных может быть критична для их владельца, т.к. они могут содержать как личную, так и конфиденциальную информацию, утрата или рассекречивание которых может негативно повлиять на владельца.

В связи с этим в настоящее время остро встает проблема обеспечения защиты данных в телефоне, ограничение доступа к различным установленным приложениям и невозможность получения доступа к хранимой информации несанкционированным лицом в случае утери или кражи мобильного телефона.

В ходе работы рассматривается рынок мобильных телефонов-смартфонов. Анализируются состояние рынка, доля определенных мобильных операционных систем на рынке.

Было выяснено, что самой перспективной и в то же время самой молодой является мобильная операционная система (ОС) Android.

Согласно исследованию Canalys estimates [2], на конец 4-го квартала 2010 г. было продано 33,3% сотовых телефонов с установленной

ОС Android, тем самым с первого места впервые за 10 лет была вытеснена операционная система Symbian. Рост поставок телефонов с установленной ОС Android с конца 2009 г. до начала 2011 г. составил 615,1%.

Сама операционная система является свободно распространяемой, исходный код открыт, потому производители мобильных телефонов могут сами модернизировать ОС под нужды своих моделей.

В свете данных обстоятельств очевидны актуальность и перспективность разработки приложений для платформы Android. Небольшой возраст системы обусловливает малое количество разработанных приложений, в том числе и направленных на обеспечение безопасности телефона.

Доступ к данным в ОС осуществляется с помощью приложений. Разработанная система защиты приложений позволит ограничить доступ к приложениям, установленным на телефоне, что позволит исключить их несанкционированный запуск и как следует ограничить доступ к данным, подлежащим защите. При этом разрабатываемая система обеспечивает защиту не на физическом уровне (т.е. доступ к носителю информации не контролируется), а на уровне операционной системы, когда пользователь телефона взаимодействует только с интерфейсом, предоставляемым ОС.

В ходе работы было разработано приложение для мобильного телефона, работающего на основе операционной системы Android. Данная разработка позволяет контролировать запуск установленных приложений, защищает их от несанкционированного использования.

Система защиты запускается в виде системного сервиса и отслеживает состояние системы, отлавливает событие запуска приложения. Если приложение находится в числе защищаемых, то сервис защиты блокирует его запуск и выводит окно, предлагающее ввести аутентификационные данные. В случае ввода неверной ключевой информации в доступе пользователю отказывается.

Разработанное приложение также позволяет указывать список разрешенных SIM-карт. В случае обнаружения неразрешенной SIM-карты телефон при загрузке операционной системы автоматически активирует систему защиты.

В будущем данный элемент системы защиты будет расширен – при обнаружении посторонней SIM-карты будет происходить не только автоматический запуск системы защиты, но также и уведомление об этом владельца телефона на заранее указанный им номер телефона или E-mail. Контроль SIM-карт является эффективным средством защиты сотовых телефонов при краже, позволяет выявить сотовый номер злоумышленника, его примерное местоположение, получить отчет о его действиях на телефоне.

Ещё один разрабатываемый элемент защиты – возможность удаленного доступа к мобильному телефону. Сотовый телефон, выступающий в роли клиента, подсоединяется к заранее указанному серверу, после чего сервер может как получать различную информацию от клиента, так и управлять им.

ЛИТЕРАТУРА

1. Mobile Phone Market Grows 17.9% in Fourth Quarter // IDC – Press Release [Электронный ресурс]. Электрон. журн., 2011. URL: http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22679411&sectionId=null&elementId=null&pageType=SYNOPSIS (дата обращения: 27.02.2011).

2. Android smart phone shipments grow 886% year-on-year in Q2 2010 // Expert Analysis for the high-tech industry [Электронный ресурс]. Электрон. журн., 2010. URL: http://www.canalys.com/pr/2010/r2010081.html (дата обращения: 24.02.2011).

ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ВУЗОВ НА ОСНОВЕ ФУНКЦИОНАЛЬНОЙ МОДЕЛИ

В.Ю. Степанов, студент 5-го курса, М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, stepashkin@mail.ru

Информационные технологии давно и прочно вошли в нашу жизнь. Но, пользуясь благами цивилизации, мы редко задумываемся о том, что, обращаясь и на сайт президента России, и в штатный ЖЭК, оставляем кому-то свои личные данные. Причем не имея никакого представления о том, как они используются, хранятся и кому в каких случаях передаются. До принятия 01.01.2007 г. Федерального закона «О персональных данных» данная сфера никак не контролировалась. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [1]. Правила обработки персональных данных россиян регламентированы Федеральным законом №152 «О персональных данных». Законом и определены уполномоченные органы по защите прав субъектов персональных данных и контролю над операторами, обрабатывающими эти данные, – служба Минсвязьнадзор, Роскомнадзором, ФСБ, ФСТЭК.

Использование персональных данных в отечественных организациях жестко регулируется законодательством с помощью вышеупомянутого Федерального закона «О персональных данных» и другими нормативно-правовыми актами. Эти документы являются основными в

данной сфере и, по сути, представляют собой перечень самых общих высокоуровневых требований к защите персональной информации. Вследствие этого данный закон остается лишь набором общих рекомендаций.

Обеспечение защиты персональных данных обрабатываемых в информационных системах современного вуза, является актуальной задачей. Это обусловлено тем, что нет конкретных рекомендаций о том каким образом любому университету применять регламентированные правила по работе с персональными данными, вследствие чего работниками вузов допускается большое количество ошибок (неправомерных действий) при обработке, хранении, передаче и т.д.

По данным публичного доклада Роскомнадзора 2009 г. наблюдаются проблемы, возникающие в связи с нарушениями операторами персональных данных требований ФЗ «О персональных данных». Причинами этого являются:

– отсутствие согласия на обработку персональных данных;

– незаконная передача персональных данных третьим лицам;

– несоблюдение условий конфиденциальности (опубликование в средствах массовой информации, размещение в общественных местах, на интернет-сайтах информации, содержащей персональные данные).

Для приведения ИСПДн к нормам российского законодательства необходимо разработать аппарат, при помощи которого можно адаптировать данные нормы к конкретной сфере деятельности, в частности системе высшего образования. Основой для разработки такого аппарата может являться функциональная модель организации.

Основой для построения функциональной модели могут служить документы Министерства образования и науки РФ о деятельности и функционировании высших учебных заведений и непосредственно анализ деятельности самих университетов. Для построения адекватной модели следует рассматривать университеты, доказавшие свою состоятельность в основных видах деятельности. На основании функциональной модели можно проследить информационные потоки и выделить те, в которых будут принимать участие персональные данные.

Любая организация должна заботиться о безопасности обрабатываемой ей персональных данных. К сожалению, на данный момент проблема незащищенности персональной информации вузов не теряет своей актуальности и по-прежнему требует к себе большого внимания со стороны уполномоченных органов по защите персональных данных и руководителей образовательных учреждений.

ЛИТЕРАТУРА

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

РАЗРАБОТКА ТЕХНОЛОГИИ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО ДИНАМИКЕ НАБОРА ПАРОЛЬНОЙ ФРАЗЫ

А.Е. Сулавко, аспирант каф. информационной безопасности
г. Омск, Сибирская государственная автомобильно-дорожная академия (*СибАДИ*), *sulavich@mail.ru*

Одной из самых опасных угроз информационной безопасности можно считать неавторизованный доступ. По данным Information Security Breaches Survey 2010 г. угроза неавторизованного доступа стоит на третьем месте в списке самых опасных и губительных для бизнеса угроз информационной безопасности. Для защиты от неавторизованного доступа разрабатываются различные продукты: биометрические системы идентификации и аутентификации, аппаратные идентификаторы, многофакторные системы разграничения доступа. Но несмотря на это, наибольшей популярностью до сих пор пользуются средства, основанные на аутентификации по паролю – наиболее старом методе борьбы с данной угрозой, что обусловлено удобством и простотой его использования и реализации, метод не требует никаких дополнительных устройств и усилий от пользователя. К сожалению, у данного метода есть существенный недостаток, обусловленный человеческим фактором. Пользователь может забыть или записать пароль на бумаге и оставить ее на самом видном месте, использовать «слабый» пароль или вовсе его не использовать, пароли могут храниться в открытом виде, пользователь даже может сам сказать свой пароль кому-либо или отправить его по электронной почте. Помимо этого, пароли воруют и взламывают. Учитывая этот недостаток, парольную защиту нельзя считать надежной.

Данная работа посвящена усовершенствованию парольного метода защиты, а именно разработке технологии биометрической идентификации пользователей по динамике набора парольной фразы.

Анализ клавиатурного почерка позволяет получить множество независимых признаков для идентификации, но основной проблемой систем идентификации на базе динамических биометрических признаков являются изменчивость самих признаков, их низкая информативность. В данной работе в качестве признаков для идентификации используются характеристики *n*-грамм символов (*n* символов, набираемых при помощи клавиатуры последовательно). В каждой *n*-грамме учитываются временные задержки между нажатиями клавиш и времена удержания каждой клавиши. На данный момент в результате проведенных исследований выявлено несколько информативных биграмм и триграмм, временные характеристики которых существенно отлича-

ются у различных пользователей при вводе парольной фразы и стабильны для каждого пользователя. При этом временные характеристики данных *n*-грамм практически не зависят от парольной фразы и ее длины. Приведенное выше справедливо для всех пользователей, принимавших участие в исследованиях. Было установлено, что все исследуемые признаки распределены по нормальному закону.

В качестве алгоритма для принятия решений используется специально разработанный адаптивный алгоритм, в основе которого лежит стратегия Байеса. Для распознавания «чужих» (пользователей, не зарегистрированных в системе) с помощью стратегии Байеса можно использовать пороговое значение апостериорных вероятностей. Под пороговым значением вероятности далее понимается минимальная разница между максимальной на каком-либо шаге апостериорной вероятностью гипотезы-лидера (самой вероятной гипотезы) и остальными апостериорными вероятностями других гипотез.

При использовании в задачах биометрической идентификации по динамическим биометрическим признакам стратегия Байеса дает сбои. Часто на очередном шаге вероятность какой-либо гипотезы становится близкой по значению к единице, а остальные в сумме дают число ≈ 0. Такая ситуация почти всегда ведет к ошибке идентификации. Помимо этого, в результате проведенных исследований были выявлены следующие зависимости:

– при увеличении количества признаков вероятность ошибки первого рода уменьшается, вероятность ошибки второго рода растет;

– при увеличении количества эталонов вероятность ошибки первого рода увеличивается, вероятность ошибки второго рода уменьшается;

– при увеличении количества эталонов динамика формирования вероятностей гипотез по Байесу становится менее агрессивной (приращения апостериорных вероятностей на всех шагах уменьшаются);

– пороговое значение вероятности влияет на величину ошибок 1-го и 2-го рода и их соотношения.

В целом при увеличении количества эталонов пользователей сумма ошибок первого и второго рода стремительно увеличивается и при наличии в базе более 50 эталонов принимает неприемлемые значения (более 0,1). Учитывая приведенные выше данные, было принято решение ограничить приращения вероятностей в соответствии с (1):

$$P'(H_i|A_j) = P'(H_i|A_{j-1}) + (P(H_i|A_j) - P'(H_i|A_{j-1}))*W_j, \quad (1)$$

где $P(H_i|A_j)$ – апостериорная вероятность, вычисленная по формуле Байеса для *i*-й гипотезы на *j*-м шаге, W_j – вес *j*-го шага принятия решений по Байесу.

Вес W_j вычисляется по специально разработанной формуле, учитывающей все приведенные выше зависимости.

На сегодняшний момент с применением описанного подхода были достигнуты следующие результаты: вероятность правильной идентификации по клавиатурному почерку при использовании парольной фразы из 50 символов составляет 0,996 (вероятность ошибки первого рода составляет 0,005, вероятность ошибки второго рода составляет 0,003) при наличии в базе 147 настоящих (полученных не при помощи моделирования) эталонов пользователей. Достоверность этого результата 0.90309.

На данный момент ведутся исследования с целью сокращения длины парольной фразы для идентификации, выявления новых информативных *n*-грамм и новых признаков. Также ведутся работы по увеличению количества эталонов пользователей в базе.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ САЙТОВ

Д.С. Гордин, студент

г. Томск, ТУСУР, ФВС, gor.dan@bk.ru

Информационная защита сайтов в наше время должна быть основополагающим критерием при проектировании сайта. Часто можно услышать тревожные сообщения в СМИ о том, что на днях хакерами был взломан интернет-ресурс крупной компании, и эта компания понесла большие убытки из-за взлома. Множество компаний каждый день все больше интегрируются в сеть Интернет, начиная от простого размещения информации о компании и заканчивая ведением всех стадий бизнеса, используя только Сеть. Сообщения о взломах сайтов появляются с завидной регулярностью, и со временем частота их появления растет. Это не говорит о том, что с каждым днем грамотность веб-программистов падает. Это говорит о том, что сложность проектируемых веб-систем с каждым годом, да что тут говорить – с каждым месяцем – растет. Из-за этого роста уследить за всеми потенциальными уязвимостями системы становится все сложнее.

Цель проекта – создать некое веб-приложение (сайт), которое в автоматическом режиме сможет показать информацию и возможные уязвимости другого интернет-ресурса. Эта информация сможет упростить дальнейшую оценку информационной безопасности этого сайта. Ниже приведен список данных, которые могут помочь в аудите информационной безопасности.

Информация о сервере:

– IP;

− OS (по возможности);
− версия веб-сервера;
− другая информация (версия СУБД, интерпретатора и т.д.) (по возможности).

Информация о домене:
− full whois (из нескольких источников).

Информация о сайте:
− файловая структура сайта;
− открытые пути;
− версия CMS;
− насколько возможно, точный порядковый номер версии CMS;
− установленные модули и плагины;
− список возможных паблик уязвимостей для данной версии и список возможных эксплоитов;
− уязвимые скрипты;
− sql-injection;
− xss;
− php-инклудинг.

В настоящий момент реализованы проверка информации о сервере, о домене и части информации о сайте, такой как определение версии CMS (как по официально определяющим ее признакам, там и по косвенным), и поиск уязвимых скриптов, очень упрощенный, но дающий свои результаты.

В результате это будет веб-система, то есть это будет полностью серверное приложение. Должен заметить, у этого веб-приложения будет база данных, содержащая информацию о способах проведения атак (sql-injection, xss, php-инклудинг) и информацию, позволяющую правильно идентифицировать установленную CMS и установленные плагины к этой CMS. Эффективность работы создаваемого приложения будет зависеть исключительно от актуальности этой базы.

Само же приложение, возможно, будет написано на нескольких серверных языках программирования (пока PHP). Все будет зависеть от простоты и возможности реализации и дальнейшей модернизации некоторых функций на определенном языке. У проектируемого мною веб-приложения есть аналоги, но они часто специализированы только на одной области, например ищут только sql-injection и xss. В большинстве это клиентские приложения, и результат работы этих приложений зачастую оставляет желать лучшего. Это можно понять, ведь объем работ, который нужно провести для автоматизации поиска уязвимостей, разновидности которых появляются чуть ли не каждый день, должен быть колоссальным.

Любая компания должна заботиться о безопасности своих сайтов. Ведь в первую очередь это престиж компании, который долго зарабатывается и легко теряется.

ЛИТЕРАТУРА

1. *Фленов М.Е.* PHP глазами хакера. СПб.: БВХ-Петербург, 2005. 304 с.

ПОДХОД К ОЦЕНКЕ ПРАВИЛЬНОСТИ ПРОИЗНОШЕНИЯ ЗВУКОВ ИНОСТРАННЫХ ЯЗЫКОВ

С.Д. Тиунов, аспирант

Научный руководитель Р.В. Мещеряков, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, t5d@ms.tusur.ru

Одним из применений речевых технологий является помощь в обучении иностранному языку [1]. Предполагается, что такая система должна воспринимать речь обучаемого и оценивать правильность его произношения. Исследователи выделяют два основных подхода к оценке произношения: оценка правильности отдельных звуков и общая оценка произношения. Наиболее интересным является оценка отдельных звуков, поскольку из множества оценок отдельных звуков можно составить и интегральную оценку качества произношения. С другой стороны, в интегральную оценку могут входить и супрасегментные показатели качества речи, то есть правильность просодии: ударения, тона, интонации. В данной статье остановимся на оценках отдельных звуков.

Оценки правильности отдельных звуков, как правило, делаются при помощи системы распознавания речи. Такая система принимает на вход речевой сигнал, а на выходе дает последовательность распознанных звуков с привязкой границ этих звуков ко времени. Использовать эту информацию для коррекции произношения можно, лишь обладая знанием о том, что на самом деле было сказано. При этом разработчики обучающих систем используют наиболее очевидный способ получения этого знания: студенту предлагается произнести конкретную фразу, и при обработке его речи предполагается, что он действительно произнес предложенную фразу. При этом распознаватель речи используется в так называемом режиме усиленного выравнивания (forced alignment), то есть выходная последовательность звуков заранее предопределена и задачей распознавателя является осуществление привязки ко времени, а также определение меры схожести произнесенного звука и соответствующего звука в выходной последовательности. Далее эти оценки схожести, как правило, используются обучающей системой как оценки качества произношения звуков [2–4].

Ярким примером такого подхода является работа [3]. На рис. 1 представлена общая схема работы системы оценивания. Параметры, выделенные для распознавания речи, используются в двух вариантах распознавания: обычном (цикл по фонемам, в котором фонема выбирается по наименьшей ошибке) и усиленном выравнивании (см. выше). Эти два результата распознавания сравниваются, и дается оценка качества произношения. Если оценка качества произношения выше предопределенного порога, то считается, что данная фонема произнесена правильно. В противном случае считается, что фонема произнесена неправильно.

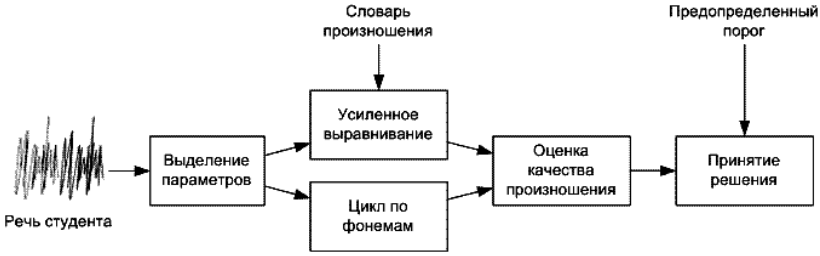


Рис. 1. Типовая система оценки качества произношения

Такой подход имеет, по крайней мере, следующие недостатки. Исследователи выдвигают к обучающим системам требования наличия корректирующей обратной связи: система должна сообщать студенту не только о том, какие звуки он произнес плохо, но и о том, как скорректировать данные звуки. При использовании такого подхода (получении одномерной оценки «схожести») возможно дать лишь общие рекомендации по правильному произнесению данного звука, а не предлагают способ коррекции допущенной ошибки. Объяснение этому достаточно простое: пространство звуков не может быть сжато до одномерного с сохранением метрики схожести каждой пары звуков. Например, пространство гласных звуков как минимум двумерное, поскольку однозначное определение гласного проходит по его подъему и ряду, что соответствует положению первой и второй формант соответственно.

Таким образом, более правильно в данном случае использовать для оценки схожести и формирования корректирующей обратной связи не одномерные оценки распознавателей речи, а набор значений параметров, которые используются для расчета таких оценок. Например, была произнесена гласная /i/, более задняя, чем языковой эталон. Обучающая система, измерив параметры речевого сигнала, соответствующие положениям первой и второй форманты, определит, что вторая

форманта имеет низкое значение, поэтому сообщит студенту, что при произнесении гласной /i/ необходимо сильнее прижимать язык к зубам.

ЛИТЕРАТУРА

1. *Eskenazi M.* An overview of spoken language technology for education / M. Eskenazi // Speech Communication. 2009. Vol. 51, № 10. P. 832–844.

2. *Eskenazi M.* The Fluency pronunciation trainer: Update and user issues / M. Eskenazi, Y. Ke, J. Albornoz, K. Probst // In Proceedings INSTiL2000. 2000. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.10.3295.

3. *Witt S.* Use of Speech Recognition in Computer-assisted Language Learning: Ph.D. thesis / University of Cambridge. 1999. http://mi.eng.cam.ac.uk/reports/svr-ftp/auto-pdf/witt_thesis.pdf.

4. Automatic detection of phone-level mispronunciation for language learning / H. Franco, L. Neumeyer, M. Ramos, H. Bratt // Learning, Proc. of Eurospeech 99. 1999. P. 851–854. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.50.1634.

ПОСТРОЕНИЕ МОДЕЛИ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Ю. Ткачев, студент 5-го курса

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, renoz@mail.ru

Исследования проблемы обеспечения безопасности компьютерных систем ведутся в направлении раскрытия природы явлений, заключающихся в нарушении целостности и конфиденциальности информации, дезорганизации работы компьютерных систем. Серьезно изучается статистика нарушений, вызывающие их причины, личности нарушителей, суть применяемых нарушителями приемов и средств, используемые при этом недостатки систем и средств их защиты, обстоятельства, при которых было выявлено нарушение, и другие вопросы, которые могут быть использованы при построении моделей потенциальных нарушителей.

Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно, если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлении.

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений [1].

Среди всех существующих моделей описания нарушителя ИБ на сегодняшний день самой общей является модель общих критериев.

Основываясь на этой модели описания нарушителя можно составить основные параметры нарушителя ИБ, на которых будет строиться новая модель описания нарушителя ИБ:

– Средства поиска уязвимостей.

Наличие (0/1)/ качество (>0).

– Средства использования уязвимостей.

Наличие (0/1)/ качество (>0).

– Навыки/умения работы со средствами обработки информации.

Наличие (0/1)/качество (>0).

– Нужность информации.

Наличие (0/1) / качество (>0) (усердность добывания).

– Знание рубежей защиты.

0 – отсутствие знаний, (>0) относительно каждого рубежа.

– Количество рубежей защиты, которые осталось преодолеть.

0 – санкционированный пользователь, (>0) – несанкционированный.

– Преднамеренность совершения нарушения.

0 – случайное, 1 – преднамеренное.

– Возможность использования несанкц. средств обработки информации.

0 – полная защита от сторонних средств, 1 – есть возможность использования сторонних средств.

Угрозы от нарушителя видовой информации.

Каналом будем считать зону разрешенной видимости.

1) Устройство вывода (монитор) -> Человек.
   1. Н/с человек, санкц. Канал.
   2. Н/с человек, Н/с канал.
   3. Н/с устройство вывода.
   4. Санкц. человек, н/с канал (несанкц. помещение).

2) Устройство вывода (принтер) -> Документ.
   1. Н/с человек, санкц. канал.
   2. Н/с человек, н/с канал.
   3. Н/с устройство вывода.
   4. Санкц. человек, н/с канал (несанкц. помещение).

3) Документ -> Человек.
   1. Н/с человек, санкц. канал.
   2. Н/с человек, н/с канал.
   3. Санкц. человек, Н/с канал (несанкц. помещение).

В ходе данной работы были рассмотрены возможные угрозы видовой информации и на их базе составлена модель нарушителя видовой информации, основанная на разработанных параметрах нарушителя информационной безопасности, и описана каждая из возможных рассмотренных угроз, относительно каждой из этих угроз был произведен анализ и описаны параметры нарушителя.

ЛИТЕРАТУРА

1. Журнал «Системы безопасности». 2007. №4.

ВЕРОЯТНОСТНАЯ МОДЕЛЬ РАСПРОСТРАНЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.В. Толстых, адъюнкт каф. высшей математики

г. Воронеж, Воронежский институт МВД России, tov48@mail.ru

Введение. На современном этапе информатизации органов внутренних дел (ОВД) происходит интенсивное техническое совершенствование объектов информатизации и телекоммуникационных систем, обеспечивающих их информационное взаимодействие, что обеспечивает повышение эффективности решения служебных задач сотрудниками ОВД.

Объекты информатизации [1] ОВД связаны с отдельными организационно выделенными подразделениями ОВД. Эти подразделения при осуществлении своей служебной деятельности могут использовать информацию, поступающую из нескольких информационных систем (ЕИТКС, Internet и др.). В каждой из этих информационных систем реализуется собственная политика безопасности. Вопросы согласования этих политик безопасности до сих пор не рассматривались.

Для решения этой задачи необходимо использование единого подхода к оценке эффективности информационной безопасности (ИБ) на всех объектах информатизации. В процессе решения этой задачи необходимо исследовать возможность распространения угроз ИБ на отдельном объекте информатизации ОВД. Для оценки вероятности реализации угроз ИБ необходимо разработать описательную модель распространения угроз на объекте информатизации.

Описание процесса распространения угроз информационной безопасности на объекте информатизации. Угрозы ИБ в значительной степени влияют на временные характеристики информационных систем, так как результатом их воздействия являются значительные временные потери, связанные с восстановлением информационных процессов.

Структурные подразделения ОВД в процессе своей деятельности могут использовать информацию, размещенную в нескольких информационных системах (ИС). Совокупность всех информационных ресурсов, средств и систем обработки информации подразделения является информационно-технической системой объекта информатизации.

Обеспечение информационной безопасности объектов информатизации ОВД направлено на предупреждение и нейтрализацию внешних и внутренних угроз, которые сводятся к несанкционированным действиям, влияющими на показатели безопасности информации [2]. Обеспечение информационной безопасности вызывает необходимость решения задачи учета оценки распределения возможности возникновения угроз информационной безопасности на элементах объекта информатизации ОВД.

Решение задачи защиты от угроз ИБ обеспечивается использованием на объекте информатизации системы защиты информации. В связи с тем, что информационное системы, размещенные на объекте информатизации, являются распределенными, система защиты информации также должна быть распределена.

Для решения указанной задачи необходимо разработать математическую модель распространения угроз ИБ на объектах информатизации.

Формализация процесса распространения угроз ИБ на объекте информатизации. Каждую информационно-техническую систему объекта информатизации O будем задавать множеством элементов его ИС: $O=\{o_1,o_2,...,o_n\}$, которые подвергаются множеству угроз. $U=\{u_1,u_2,...,u_m\}$ – множество всех типов угроз ИБ. В связи с тем, что ИС в составе информационно-технической системы объекта информатизации являются распределенными, СЗИ также должна быть распределена.

Обратимся к формализации процесса распространения угроз ИБ и разработке вероятностной дискретной модели. Будем считать, что вероятности появления угроз ИБ в силу названных причин изменяются в дискретные моменты времени.

Вероятности возникновения угроз ИБ на элементах информационно-технической системы объекта информатизации можно описать матрицей $V^t=(v_{i,j}{}^t)$, $i=1,...,m\ j=1,...,n$, где $v^t{}_{ij}$ – вероятность возникновения угрозы типа u_i на элементе o_j в момент времени t.

Устранение угроз ИБ в результате функционирования СЗИ может быть описано матрицей $Q=(q_{ij}),i=1,...,m\ j=1,...,n$, где q_{ij} – вероятность устранения средствами СЗИ угроз типа u_i на элементе o_j.

После устранения угроз ИБ вероятности их возникновения описываются матрицей $W^t = \left(w_{i,j}^t\right)$, $i = 1,...,m$ $j = 1,...,n$, где $w_{ij}^t = v_{ij}^t\left(1 - q_{ij}\right)$. Возможность передачи угрозы ИБ зависит от типа угрозы. Обозначим R_i – бинарное отношение на множестве O, определяющееся возможностью распространения угрозы u_i. Тогда возможность распространения этой угрозы описывается графом отношения R_i, т.е. графом $G_i = \left(O, R_i\right)$; возможность распространения всех типов угроз описывается графом $G = \bigcup_{i=1}^{p} G_i(O,R)$, где $R = \bigcup_{i=1}^{p} R_i$.

После реализации возможностей распространения угроз по элементам объекта информатизации эта матрица преобразуется в матрицу $V^{t+1} = \left(v_{ij}^{t+1}\right)$. Зададим вероятности возможности распространения угроз информационной безопасности между элементами объекта информатизации: P_{jk}^i – вероятность распространения угрозы u_i с элемента o_j на элемент o_k. В таком случае $v_{ik}^{t+1} = 1 - \prod_{j=1}^{n}\left(1 - w_{ij}^t \cdot P_{jk}^i\right)$.

Действительно, появление угрозы u_i на элементе o_j и возможности ее перехода с элемента o_j на элемент o_k являются независимыми событиями. Поэтому вероятность одновременного появления этих событий – $w_{i,j}^t \cdot P_{jk}^i$, а их непоявления – $1 - w_{i,j}^t \cdot P_{jk}^i$. Вероятность неперехода угрозы типа u_i на элемент o_k ни с одного элемента – $\prod_{j=1}^{n}\left(1 - w_{i,j}^t \cdot P_{jk}^i\right)$, а перехода этой угрозы – $1 - \prod_{j=1}^{n}\left(1 - w_{i,j}^t \cdot P_{jk}^i\right)$.

Выводы. Разработанная вероятностная дискретная модель позволяет оценивать наличие угроз информационной безопасности на элементах информационно-технической системы объекта информатизации с учетом возможности их распространения. Данная модель является основой имитационной модели, описывающей динамику распространения и устранения угроз на элементах информационно-технической системы объекта информатизации.

Имитационная модель может быть использована для оценки эффективности и оптимизации выбора варианта системы защиты информации на объекте информатизации.

ЛИТЕРАТУРА

1. *Техническая* защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056. 2005. М.: Изд-во стандартов, 2005. 105 с.

2. *Толстых О.В.* Обеспечение информационной безопасности объектов информатизации органов внутренних дел // Молодежный научный бюллетень. Воронеж: Воронежский институт МВД России, 2009.С. 164–167.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ВУЗЕ

Д.А. Третьяков, студент 5-го курса

Научный руководитель М.А. Сопов, ассистент каф. КИБЭВС,
г. Томск, ТУСУР, каф. КИБЭВС, webdizy@gmail.com

В соответствии с Конвенцией Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (ETS №108, 1981 г.), которую Россия ратифицировала в 2005 г., 26 июля 2006 г. был принят Закон №152 «О персональных данных». Согласно данному закону все организации, обрабатывающие сведения, относящиеся к категории персональных данных, должны защитить свои информационные системы по обработке персональных данных, а также получить документы, которые подтверждают их соответствие требованиям закона, не позднее 1 января 2010 г.

В соответствии с Федеральным законом ФЗ-152 «О персональных данных» любой вуз является оператором персональных данных, поскольку он организует и осуществляет обработку персональных данных, а также определяет в соответствии с законодательством об образовании цели и содержание обработки персональных данных. Таким образом, его деятельность в этой части регулируется данным законом.

Можно выделить три вида субъектов, чьи данные обрабатываются, по признаку цели обработки:

– работник;

– абитуриент;

– студент.

Соответственно характер и объем обрабатываемых данных для каждого вида будут значительно отличаться. Также будут отличаться и правовые основания для обработки.

Данные о работниках обрабатываются в соответствии и на основании Трудового кодекса, Налогового кодекса, другого законодательства и трудового договора.

Обработка персональных данных абитуриентов и студентов осуществляется на основании Федеральных законов №3266-1 «Об образо-

вании» и №125 «О высшем и послевузовском профессиональном образовании», а также лицензии на право ведения образовательной деятельности.

Ниже представлены необходимые меры для приведения информационных систем персональных данных университета к требованиям Закона №152:

– получение письменного согласия субъектов на обработку (с указанием, какая информация, с какой целью, в какие сроки обрабатывается и кому передается);

– пересмотр договоров с субъектами (работники, партнеры, клиенты);

– формирование документов по порядку обработки персональных данных;

– формирование списка допущенных лиц, ознакомление под подпись с указанием, к какой информации допущен и в какой срок;

– формирование списка лиц, ответственных за защиту персональных данных и их обучение;

– формирование модели угроз;

– классификация информационных систем персональных данных. Если есть подсистемы – по наибольшей категории;

– уведомление уполномоченного органа (Роскомнадзор) о намерении обрабатывать персональные данные;

– получение лицензии ФСТЭК на осуществление деятельности по технической защите конфиденциальной информации (для ИС ПДн 1-го и 2-го классов);

– приведение защиты персональных данных в соответствии с требованиями Федерального закона №152 от 2006 г.;

– проведение аттестации/декларирование соответствия СЗИ ИС ПДн (аттестация обязательна для ИС ПДн 1-го и 2-го классов);

– организация эксплуатации ИС ПДн и контроля безопасности.

Для достижения поставленной цели, приведения ИСПДн высших учебных заведений необходимо разработать и формализовать структурную модель университета, на основании которой можно провести анализ и оценку информационных потоков вуза на наличие в них персональных данных. Данная модель позволит адаптировать нормативно-правовые акты под отрасль высшего образования, что значительно упростит для сотрудников всех университетов России исполнения норм и требований законодательства в области персональных данных.

ЛИТЕРАТУРА

1. *Травкин Ю.И.* Персональные данные: М.: Амалданик, 2007. 432 с.

2. *Кухаренко Т.А.* Персональные данные: Кто, что и зачем должен о нас знать: М.: Эскмо, 2010. 224 с.

3. *Петров М.* Постатейный комментарий к Федеральному закону «О персональных данных». М.: Изд. дом «Юстицинформ» 2007. 160 с.

4. *Байкамова И.А., Новиков А.В., Рогачев А.И., Хыдыров А.Х.* Обеспечение защиты персональных данных: метод. пособие: М.: 1С-Паблишинг, 2010. 214 с.

АНАЛИЗ ЗАЩИЩЕННОСТИ СЕТИ

Е.Р. Тухбатуллин, студент 4-го курса

Научный руководитель Г.А. Праскурин, ст. преподаватель

г. Томск, ТУСУР, каф. КИБЭВС, pancher86@mail.ru

В настоящее время с развитием информационных систем широко применяются и развиваются компьютерные сети. Компьютерная сеть – это система связи компьютеров и/или компьютерного оборудования (серверы, маршрутизаторы и другое оборудование). С развитием компьютерных сетей растет и число их уязвимостей. Для обеспечения безопасности компьютерной сети необходимо проводить анализ защищенности сети.

В области защиты вычислительных сетей не существует достаточно четких определений процедуры анализа защищенности и методики ее выполнения, что значительно затрудняет внедрение технологий анализа и аудита информационной безопасности вычислительной сети. Работа нашей группы направлена на изучение и последующее исследование возможных уязвимостей и угроз безопасности компьютерных сетей и разработку методики проведения анализа защищенности сети с целью обеспечения необходимой безопасности сети.

Защищенность вычислительной сети – совокупность состояний, в которых обеспечивается безопасность ее информационных активов, то есть их конфиденциальность, целостность и доступность. Процедура анализа защищенности вычислительной сети предполагает проверку злоумышленником возможности нарушения этих состояний доступными ему способами. Выполнение этой процедуры требует решения следующих задач: сбор информации о компонентах и активах вычислительной сети, средствах ее защиты и их недостатках; обработка этой информации и построение приемлемой модели вычислительной сети на основе полученных результатов для дальнейшего ее использования при первичной оценке рисков вычислительной сети или при проведении аудита информационной безопасности вычислительной сети.

Анализ защищенности сети может выполняться как путем внешнего сканирования периметра и/или проникновения (из интернета), так и с помощью сканирования узлов и/или проникновения из внутренней сети.

В процессе сетевого аудита могут выполняться следующие виды аудита:

– сканирование сети (пассивный мониторинг);

– тест на проникновение (активный аудит);

– анализ архитектуры сети с точки зрения информационной безопасности (комплексный аудит сети).

Такой вид аудита как пассивный мониторинг, является наиболее простым в осуществлении. В ходе сканирования сети осуществляются поиск и исследование уязвимостей в отдельных узлах сети и формирование рекомендаций с предложениями по устранению выявленных недостатков. Использование полученных рекомендаций позволяет устранить опасные уязвимости и повысить уровень защищенности информационной системы при минимальных затратах на информационную безопасность. Однако при существенной ценности информации и высокой степени информационных рисков только пассивный мониторинг не позволяет обеспечить достаточно высокую степень оценки.

Активный аудит условно можно разделить на два вида: «внешний» (моделирование действий внешнего злоумышленника) и «внутренний» (моделирование действий внутреннего злоумышленника). При проведении активного аудита проводится анализ корректности настроек, потенциальных уязвимостей операционных систем, систем управления базами данных, почтовых, Web-серверов и другого программного обеспечения, которое используется в информационной системе.

Комплексный аудит сети включает как пассивный мониторинг, так и тест на проникновение и позволяет обеспечить наиболее высокую степень экспертной оценки уровня защищенности сети. При проведении данных работ специалисты не ограничиваются только поиском уязвимостей в отдельных узлах сети, а выполняют анализ всей сетевой инфраструктуры и формируют рекомендации по ее оптимизации с точки зрения обеспечения информационной безопасности. Результатом комплексного аудита может быть проект оптимизированной архитектуры сети либо рекомендации по доработкам существующей архитектуры с учетом текущих требований.

ЛИТЕРАТУРА

1. *Таненбаум Э.* Компьютерные сети. СПб.: Питер, 2007. 992 с.

2. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2007. 960 с.

3. *Астахов А.* Методика анализа защищенности сети // Открытые системы. 2002. № 7–8.

4. *Бакиров Т., Валеев С.* Методика анализа защищенности сети // Information Security (Информационная безопасность). 2008. №1.

АНАЛИЗ ДАННЫХ В ЗАДАЧАХ КЛАССИФИКАЦИИ ТЕКСТОВЫХ ДАННЫХ ДЛЯ ОПРЕДЕЛЕНИЯ ТЕКСТОВЫХ МАТЕРИАЛОВ СОДЕРЖАЩИХ ПРИЗНАКИ ЭКСТРЕМИЗМА

Д.Н. Великоцкий, инженер
г. Томск, ТУСУР, mrv@security.tomsk.ru

В 2002 г. вступил в силу Федеральный закон «О противодействии экстремистской деятельности», который определяет правовые и организационные основы противодействия указанной деятельности и устанавливает ответственность за ее осуществление.

Одной из разновидностей экстремистской деятельности является массовое распространение экстремистских материалов. В соответствии с Федеральным законом приоритетным направлением противодействия является разработка мер, направленных на предупреждение экстремистской деятельности.

Тенденции развития сети Интернет показывают, что данная среда стала одним из основных средств распространения экстремистских материалов. Использование Всемирной сети в экстремистских целях вызвано в первую очередь фактическим отсутствием существенных затрат на производство, хранение и распространение указанных материалов. Кроме того, процедура установления конкретных лиц, пропагандирующих экстремистские идеи, нетривиальна, что связано как с отсутствием «государственных границ» в сети Интернет, так и возможностью сокрытия своих истинных данных со стороны злоумышленников.

Свободный доступ к экстремистским материалам особенно опасен для лиц с формирующимся мировоззрением, т.е. категории пользователей Всемирной сети среднего и старшего школьного возраста, учащихся среднеспециальных образовательных учреждений, а также студентов вузов. Указанная категория пользователей активно использует сеть для общения, поиска материалов для учебного процесса, а также в развлекательных целях. Перед проведением исследования следует уточнить, что материалы, содержащие признаки экстремизма, могут появляться быстрее, чем может следовать реакция по предотвращению их распространения. Необходимо также признать факт их постоянного наличия в объективной действительности (в нашем случае – в сети Интернет).

Таким образом, область исследования является актуальной. Будем считать, что текст t_i из множества всех текстов T принадлежит к множеству всех экстремистских текстов T_e. Очевидно, что в данном случае необходимо оценивать не только ошибки первого и второго рода для классификации текста, но и их степень вредоностности, а также автор-

ство и принадлежность к определенной категории материалов. Целью создания такой автоматизированной (в идеале автоматической) системы считается не тотальное запрещение распространения материалов, «похожих» на экстремистские, а **затруднение беспрепятственного доступа** к явно сомнительным материалам большей части пользователей сети Интернет в обычном режиме.

Затруднение беспрепятственного доступа может быть осуществлено следующими способами:

1. Разработка механизма создания «черного списка» сайтов с экстремистским содержимым, обновляемого за счет жалоб пользователей сети Интернет и модераторов информационных ресурсов. Указанный список может быть подобен «черному списку» серверов, с которых осуществляется рассылка нежелательных электронных писем, т.е. список сайтов, содержащих сомнительный контент.

2. Учет поисковыми системами факта нахождения в индексируемом контенте ссылок на сайты из «черного списка» при ранжировании результатов поиска.

3. Организация для пользователей сети Интернет услуги ограничения доступа к «сайтам с возможным экстремистским содержимым» в системах администрирования, используемых провайдерами с возможностью пользователю самому добавлять в свои «черные списки» сомнительные ресурсы с указанием причины их внесения.

4. Учет поисковыми системами факта нахождения в индексируемом контенте сомнительных материалов, содержащих признаки экстремизма, при ранжировании результатов поиска.

5. Включение категории «Сайты с возможным экстремистским содержимым» в системы так называемого родительского контроля.

Целью настоящего исследования фактически являются не информационные материалы из федерального списка экстремистских материалов (предотвращение их распространения также может стать предметом исследования как более узкая, профильная задача), а информационные материалы сомнительного содержания, содержащие признаки экстремизма. Это данные, которые с высокой долей вероятности могут быть признаны экстремистскими в случае проведения лингвистического исследования и принадлежащие той предметной области, которая находится под законодательным запретом (например, материалы экстремистских организаций, деятельность которых запрещена на территории РФ).

РАЗРАБОТКА МОДЕЛИ ПОЛИТИКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ

О.А. Волков, СТиБ
Научный руководитель А.М. Сметанин, проф.
г. Ижевск, ИжГТУ, volkov-rus@yandex.ru

Использование сетевых технологий имеет ряд недостатков, к которым относится возможность несанкционированного доступа (НСД) к информации. Компьютерная сеть (КС) представляет собой комплекс программных и аппаратных средств, каждое из которых имеет уязвимости, дающие злоумышленнику возможность НСД. Любая организация, решившая использовать КС в своей деятельности, должна осознавать возможность реализации угроз НСД и предпринять ряд мер для их нейтрализации. Одной из таких мер станет разработка политики безопасности (ПБ). Предлагаемая в данной работе модель политики безопасности позволит оптимизировать систему защиты КС.

Серверное оборудование является привлекательным объектом для злоумышленников, обладая мощными вычислительными ресурсами, оно позволяет получить доступ к большим массивам обрабатываемой информации. Однако и защите такого оборудования обычно уделяется повышенное внимание. Персональные компьютеры (ПК) сотрудников имеют гораздо больше уязвимостей. Целью атаки на них может быть как непосредственный доступ к ресурсам ПК, так и завладение узлом, посредством которого могут быть атакованы остальные части сети. Во многих организациях использование периферийного оборудования не связывают с вопросами информационной безопасности. Хотя сданный в ремонт ксерокс, хранящий в памяти последние распечатанные документы, или потерянная «флэшка» могут стать причиной НСД к конфиденциальной информации, что подтверждено опубликованными в общедоступных источниках инцидентами. Каналы связи состоят из линий связи и узлов коммутации, в которых находится сетевое оборудование. В отличие от остальных узлов сети, каналы связи часто подвержены несанкционированному воздействию (НСВ), не связанному с действиями злоумышленников. Деструктивные силы природного характера часто приводят к повреждению линий связи и выходу из строя коммутационного оборудования.

Выделение нескольких узлов КС в группу позволит установить правила поведения внутри группы и правила для взаимодействия с объектами вне группы. Группы могут взаимодействовать на равных как, например, несколько локальных групп пользователей, или входить одна в другую как локальная сеть, входящая в состав распределенной сети. В первом случае ПБ будут отличаться количественными пара-

метрами (объем общего дискового пространства, время нахождения в сети), во втором случае – качественными (приоритет одной ПБ перед другой).

Такой элемент сети, как персональный компьютер, не включает в себя других узлов, и в связи с этим его ЗП носит характер начального, базового уровня. Наличие подключения рабочей станции к сети Internet значительно повышает шансы злоумышленника на успешную атаку. При подключении появляется риск получения злоумышленником несанкционированного удаленного доступа к ПК.

Переносные накопители информации приобретают все меньшие габариты, но все больший объем. Появляется возможность незаметно внести или вынести большой объем информации. В связи с этим становится необходимым аппаратными и программными средствами, ограничивать любое несанкционированное подключение устройств, способствующих хищению конфиденциальной информации.

Внутренняя угроза, исходящая от одного из сотрудников или группы лиц, направленная на хищение конфиденциальной информации, наиболее реальна и способна нанести огромный урон, так как может затронуть любую область информационных потоков организации.

Выявлять установки несанкционированного оборудования, может DLP (Data Loss Prevention) – система предотвращения потерь. Кроме того, она может вести наблюдение и протоколировать события, касающиеся передачи данных, для последующей обработки при расследовании инцидентов, а также обнаруживать явные нарушения, например, попытку документа с грифом «секретно» покинуть пределы КС организации.

Выделение нескольких ПК в отдельную группу на основании схожих функциональных параметров (принадлежность к одному подразделению, обработка данных одного уровня конфиденциальности), позволяет назначить им ПБ отличную от базовой. Она отвечает за взаимодействие ПК, внутри данного сегмента и нескольких сегментов сети между собой.

Создание ПБ, на базовом и сегментном уровне позволит контролировать информационные потоки внутри КС. Информационный обмен с внешней средой должен быть регламентирован отдельной ПБ. Исходящие или входящие данные пересекают границу КС. Граничный уровень защиты наиболее подвержен риску, так как именно этот уровень напрямую связан с внешней средой. Защита внешнего периметра носит двунаправленный характер: отражение внешних атак и контроль за информацией, покидающей пределы организации.

Данные ПБ находятся в иерархической зависимости друг от друга. При перемещении данных через несколько уровней в первую очередь

они будут подчинены ПБ более высокого уровня. Например, передача данных от ПК одной группы на ПК другой будет в первую очередь ограничена ПБ сегментного уровня, а после этого ПБ базового уровня.

Исходя из изложенного, становится понятно, что степень защищенности различных узлов системы не может быть одинаковой. А значит и данные, обрабатываемые в этих узлах, будут подвержены разной степени риска несанкционированного воздействия. Разделив информацию по степени важности на несколько категорий можно оптимизировать модель системы защиты любой организации. Цель оптимизации состоит в том, чтобы усилить защиту узлов, обрабатывающих более важную информацию, в связи с тем, что ее потеря нанесет большой урон предприятию. Наиболее действенным будет разделить данные на две группы: критические (данные, НСД к которым приведет к существенным потерям) и некритические. Дальнейшее дробление этих групп зависит от конкретных информационных потоков.

При передаче информации между различными участками КС возникают ситуации, требующие определить, какая из политик безопасности должна быть применена. ПБ исходящего и входящего узлов должны иметь удельный вес, позволяющий при сравнении установить, какая из политик имеет приоритетное значение. Факторами, определяющими удельный вес ПБ, являются: уровень на котором действует политика; степень важности информации, которую обрабатывает узел, попадающий под действие данной политики. Сумма удельного веса (УВ) этих факторов определяет удельный вес ПБ (таблица).

Диапазон УВ степени конфиденциальности может быть расширен в зависимости от требования конкретной организации. При совпадении весов должны быть соблюдены требования обеих ПБ.

Определение удельного веса политики безопасности

Уровень ПБ (УВ) Степень конфиденциальности информации (УВ)	Базовый (1)	Сегментный (2)	Граничный (3)
Некритичная (1)	2	3	4
Критичная (2)	3	4	5

Выводы. Система защиты КС организации представляет собой совокупность мер по детектированию и своевременному реагированию на возможные угрозы. Для повышения эффективности защиты информации следует разделить политику безопасности КС на несколько ПБ. Предлагается выделить три основных группы ПБ: базовая, сегментная и граничная. При анализе информационных потоков данные, потеря

которых приведет к значительному ущербу для организации, необходимо выделять в отдельную группу, защите которой стоит уделить особое внимание. При передаче информации между узлами, регулируемыми разными ПБ, соблюдаются требования ПБ с большим удельным весом.

МОДЕЛЬ СОКРЫТИЯ ИНДИВИДУАЛЬНЫХ ОСОБЕННОСТЕЙ ДИКТОРА (НОРМАЛИЗАЦИЯ И ИСКАЖЕНИЕ ГОЛОСА)

А.С. Яценко, студент 5-го курса

Научный руководитель Р.В. Мещеряков, доцент, к.т.н.

г. Томск, ТУСУР, каф КИБЭВС, y_a_s@sibmail.com

В настоящее время уже никого не удивишь системами голосовой идентификации и верификации. Тем более, что разработки в этой области ведутся постоянно [1]. Это очень удобно, ведь это не ключ, который можно потерять, или пластиковая карта, которую можно забыть дома. Поэтому внедрение систем верификации и идентификации дикторов по голосу не встречает особых трудностей, тем более, что и затрат особых оно не требует.

Но бывают случаи, когда совсем не хочется, чтобы голос был узнан по той или иной причине, причем не человеком, не системой идентификации, например:

– при даче показаний в суде;

– при необходимости провести разговор, не выдав себя;

– при желании не быть идентифицированным автоматической системой распознавания говорящих;

– разыграть коллег и т.п.

Естественно, находясь на близком расстоянии, приходится самостоятельно искажать свой голос, напрягая связки или меняя манеру разговора, но как только появляется возможность использовать для разговора средства коммуникации, будь то сотовый телефон или IP-телефония, то можно воспользоваться техническим или программным средством для маскировки своего голоса. Тем более, что использование такого средства будет значительно эффективнее искажений, создаваемых собственным голосом, а главное, не потребует никаких усилий со стороны использующего, ну разве что включение в активное состояние.

Для того что ы качественно и эффективно противодействовать не только стандартному звуковому анализатору, человеческому слуху, но и специальным методикам и системам, предназначенным для идентификации и верификации дикторов, необходимо изучить, на чем стро-

ится методика идентификации, т.е. на каких параметрах речи и голоса, и как это проходит.

Наиболее полной и показательной методикой, как и полагается пользуются эксперты-криминалисты [1–3]. Их методика идентификации состоит из нескольких типов анализа, а именно:

– описание и предварительное исследование материалов;

– аудитивный анализ;

– лингвистический анализ;

– инструментальный анализ.

Описание и предварительное исследование материалов включает в себя шумоочистку, выделение объекта исследования и сегментацию.

То есть препятствовать этому анализу смысла нет, поскольку шумоочистку всё равно проводят, а если сделать шум более громким, чтобы он по уровню был одинаков с голосовой составляющей, то наше сообщение попросту никто не сможет разобрать, особенно если шумовая помеха будет лежать в том же спектре, что и голос человека.

Следующий в этой методике – аудитивный анализ. В этом анализе эксперт на слух определяет анатомо-физиологические особенности речеобразующего аппарата диктора, индивидуальные особенности артикуляции и речевых навыков, особенности эмоционально-психологического состояния, психологических и социокультурных характеристик дикторов, а также схожесть голосов на слух.

Препятствовать этому анализу уже есть смысл, можно смягчить интонации, убрать волнение и прочие перепады, нормализовав звук по времени и по амплитуде, сделать тембр голоса повыше или пониже. Или же, наоборот, добавить перепадов, чтобы голос казался более эмоциональным.

Осуществляя лингвистический анализ, эксперт или группа экспертов сравнивают дикторов на основе индивидуального произношения речевых единиц, лексикона и словесных оборотов.

Инструментальный анализ включает в себя исследование спектральных составляющих, статических и мелодических характеристик голоса. В рамках статистического спектрально-формантного анализа фонограмма разбивают на небольшие отрезки и из них выделяют форматную структуру, тем самым набирают статистические данные, по которым и сравнивают дикторов.

Инструментальному анализу тоже есть смысл сопротивляться, меняя те или иные спектральные составляющие голоса или сдвигая частоту основных формант.

На основании всех вышеупомянутых анализов эксперт и выносит решение о том, идентифицирован диктор или нет.

Проанализировав описанную методику и еще некоторые реализации [4], был составлен список параметров голоса (речи) и моделей их оценки, на которых данные методики базируются:

– форманты F1-F4 и их соотношение;
– коэффициенты линейного предсказания;
– статистические модели Гаусса;
– частота основного тона и его интенсивность;
– спектр речевого сигнала;
– кепстральные коэфициенты.

Исходя из всего вышесказанного, модели сокрытия индивидуальных особенностей, диктор будет работать по схеме, показанной на рис. 1.

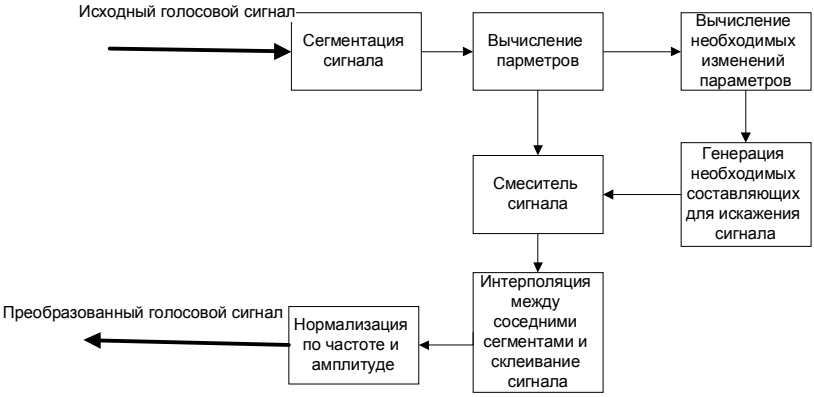


Рис. 1. Схема работы модели сокрытия индивидуальных голосовых особенностей диктора

Поступающий голосовой сигнал будет разбиваться на сегменты, для каждого из полученных сегментов вычисляются обозначенные выше параметры. Далее, исходя из вычисленных параметров, будут вычислены значения, на которые необходимо изменить текущее значение вычисленных параметров сигнала, после чего будет происходить генерация и представление в нужной форме искажающих составляющих. Следующим шагом будет «смешение» исходного сигнала и искажающей составляющей. После этого происходит линейная интерполяция между соседними сегментами и склеивание сегментов и нормализация преобразованного голосового сигнала по частоте и амплитуде.

Модель, построенная на вышеописанных параметрах и алгоритму, должна значительно затруднить процесс идентификации диктора.

ЛИТЕРАТУРА

1. *Коваль С.Л., Лабутин П.В., Пеховский Т.С. и др.* Методика идентификации дикторов по голосу и речи на основе комплексного анализа фонограмм (ООО «Центр речевых технологий», Россия, Санкт-Петербург) [Электронный ресурс]. Режим доступа: http://www.dialog-21.ru/dialog2007/materials/html/39.htm (дата обращения: 20.02.2011).

2. *Каганов А.Ш.* Криминалистическая экспертиза звукозаписей. М.: Юрлитинформ, 2005. 272 с.

3. *Галяшина И.Е.* Основы судебного речеведения. М., Стэнси, 2003. 236 с.

4. *Рамишвили Г.С.* Автоматическое опознавание говорящего по голосу. М.: Радио и связь, 1981. 224 с.

О РЕЗУЛЬТАТАХ РАЗРАБОТКИ ПРОГРАММНОГО КОМПЛЕКСА ГЕНЕРАЦИИ РЕКОМЕНДАЦИЙ ПО УСТРАНЕНИЮ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННОЙ СЕТИ

А.Р. Зайникаев, аспирант, каф. алгебры и дискретной математики

Научный руководитель Н.И. Синадский, доцент, к.т.н.

г. Екатеринбург, Уральский государственный университет им. А.М. Горького, archlich@e1.ru

В последнее десятилетие разработано немало средств для автоматизации анализа защищенности локальных сетей, позволяющих обнаруживать уязвимости. На данный момент известно такое количество уязвимостей в различных приложениях, что устранение каждой из них потребует значительных трудозатрат системных администраторов и администраторов безопасности. Для оптимизации усилий необходимо установить, какие из уязвимостей нужно устранить в кратчайшие сроки, какие злоумышленник в условиях данной структуры сети не может использовать, а какие требуют для использования предварительного проникновения в информационную систему, которое можно осуществить, задействовав иные уязвимости. Несмотря на важность указанной задачи, пока не создано программного обеспечения, позволяющего оценить степень важности устранения каждой из обнаруженных уязвимостей с учетом топологии защищаемой сети и установленных правил фильтрации трафика.

Для решения указанной задачи был выбран теоретико-графовый подход, в рамках которого было реализовано построение графа возможных атак на узлы (*node-predictive graph*). Вершинами такого графа являются наборы равнозначных с точки зрения уязвимости узлов, объединенных в группы, а ребрами – наборы уязвимостей, позволяющие провести атаку на каждый узел, соединяемый с исходной вершиной. Сохраняя информацию об объединенных в одной вершине узлах, мы

получаем возможность при необходимости вернуться к анализу интересующих нас узлов и уязвимостей на них в отдельности. Этот прием позволяет многократно уменьшить размер исследуемого графа, не снижая ценности получаемых рекомендаций, особенно в сетях с большим количеством однообразных сетевых узлов.

Генерация графа начинается с вершины злоумышленника, выявляются узлы, которые могут быть непосредственно атакованы из этой вершины. Происходит динамическое связывание обнаруженных уязвимых сетевых узлов. После этого узлы из группы добавляются в конец очереди и алгоритм продолжается. Общая сложность алгоритма не превосходит $O(N^3)$, где N – число узлов. Полученный граф проверяется на наличие мостов; уязвимости, соответствующие мостам будут рекомендованы к немедленному устранению, поскольку способствуют развитию атаки вглубь исследуемой информационной сети. Полная вычислительная сложность поиска мостов составляет $O(N_G^2)$, где N_G – число вершин графа.

При дальнейшей выработке рекомендаций происходит перестроение графа с учетом устранения уязвимостей в мостах, после чего проводится оценка защищенности сети на основе информации о возможном ущербе от реализации доступных атак. Для каждой уязвимости граф перестраивается, как при ее устранении, оценка защищенности пересчитывается. Перед оценкой отдельных уязвимостей проводится выбор атак, осуществимых только с одного узла. Все прочие атаки не оказывают влияния на безопасность сети при блокировании уязвимостей на атакующем узле, поскольку аналогичные атаки могут быть проведены с других машин в сети. В случае когда на рассматриваемом узле сети отсутствуют такие уникальные атаки, величина предотвращенного благодаря нейтрализации уязвимости ущерба сведется к его собственной ценности. Уязвимости упорядочиваются по эффекту от их устранения и в таком порядке предъявляются к устранению. Вычислительная сложность этого алгоритма зависит от соотношения среднего числа уязвимостей на узле и числа вершин графа и не превосходит сложностей $O(N_G M_G)$ и $O(M_G Vh_G^2)$, где N_G – число вершин графа, M_G – число ребер графа, Vh_G – число уязвимостей сети.

Результатом работы стал прототип программного комплекса, предлагающий обоснованные рекомендации по порядку устранения уязвимостей по полученным данным, представленным в виде файлов конфигурации от администратора или сгенерированных иными комплексами. Разработанный прототип позволяет выполнять следующие действия: загружать карты топологии информационной сети в формате программы LANsurveyor, описания хостов и уязвимостей информационной сети предприятия в собственном формате программы; прово-

дить комплексный анализ полученных данных с генерацией графа возможных атак на узлы, анализом полученного графа на наличие мостов, оценкой эффекта от устранения каждой уязвимости на всех машинах в информационной сети предприятия, в том числе с учетом устранения уязвимостей, узлов и их групп; отображать построенный для информационной сети граф возможных атак на узлы, скрывать на отображаемом графе и исключать из анализа вершины и ребра графа, отдельные узлы, атаки и уязвимости, устанавливать оценку ущерба при реализации атак различных типов, корректировать в данных по каждой уязвимости используемый протокол и порт, эффект от ее применения, необходимые для этого права на атакующем узле, возможность задействовать уязвимость локально или удаленно.

Дальнейшим развитием работы является совершенствование визуального интерфейса программы. Важными направлениями также представляются реализация получения данных от межсетевых экранов и маршрутизаторов, формирование на их основе списков доступа, учет полученной информации в анализе защищенности сети. Предполагается расширение списка поддерживаемых форматов данных о структуре информационной сети, наличии уязвимостей на хостах, условиях и эффектах применения уязвимостей.

ЛИТЕРАТУРА

1. *Степашкин М.В.* Интеллектуальная система анализа защищенности компьютерных сетей / М.В. Степашкин, И.В. Котенко, В.С. Богданов // КИИ-2006. X национ. конф. по искусственному интеллекту с международным участием: Тр. конф. Т. 1. М.: Физматлит, 2006.

2. *Sheyner O. et al.* Automated Generation and Analysis of Attack Graphs // 2002. IEEE Symposium on Security and Privacy, Oakland, CA, 2002.

3. *Lippmann R.P.* Evaluating and Strengthening Enterprise Network Security Using Attack Graphs / R.P. Lippmann, K.W. Ingols, C. Scott, K. Piwowarski, K.J. Kratkiewicz, M. Artz, R.K. Cunningham. N.Y., 2005.

ДЕТЕКТИРОВАНИЕ ВРЕДОНОСНОГО КОДА С ИСПОЛЬЗОВАНИЕМ ФУНКЦИОНАЛЬНЫХ СИГНАТУР

П.В. Збицкий, преподаватель каф. ЦРТС

Научный руководитель А.В. Рожков, проф., д.ф.-м.н.

ГОУ ВПО «Южно-Уральский государственный университет», pavel.zbitskiy@gmail.com

В работе рассмотрены проблемы детектирования сложных полиморфных и метаморфных компьютерных вирусов. Предложен и детально рассмотрен метод построения функциональной сигнатуры вируса на основе последовательности системных вызовов.

В последние годы развивается идея функциональных сигнатур компьютерных вирусов. В работе [6] рассмотрен подход так называемой кодовой нормализации – применение методов деобфускации / оптимизации для выделения минимальной функционально эквивалентной формы последовательности инструкций. Основным недостатком предложенного метода является предположение о корректной дизассемблируемости нормализируемого кода, сделанное на основании того, что вирус при построении новой копии должен сам себя дизассемблировать. В работах [3, 4] рассмотрены примеры метаморфных вирусов, которым не требуется производить самодизассемблирование при распространении и генерации новых копий.

Автором предлагается новый подход к выявлению функциональных сигнатур, основанный на анализе последовательностей системных вызовов процесса.

Назовем ***функциональной сигнатурой*** последовательность системных вызовов, производимую процессом во время выполнения и однозначно идентифицирующую некоторую программу.

Элементом сигнатуры (аналог байта классической сигнатуры) является унифицированный номер системного вызова для семейства операционных систем. В случае червей или троянцев сигнатурой может выступать запротоколированная последовательность вызовов за определенный промежуток времени. В случае же файловых вирусов, когда вирусные вызовы перемешаны с вызовами зараженной программы, или в случае вируса/червя/троянца, использующего технику перемешивания функциональных блоков в графе выполнения, встает проблема выделения подпоследовательности вирусных вызовов. Обычно это можно сделать сравнением последовательностей чистой программы и зараженной, предварительно применив алгоритм сворачивания повторяющихся подпоследовательностей (циклов).

Процесс составления сигнатур состоит из следующих этапов:

1. Получение последовательностей системных вызовов для нескольких запусков программы.
2. Поиск и сворачивание повторяющихся подпоследовательностей вызовов в каждой полученной последовательности.
3. Объединение последовательностей системных вызовов в сигнатуру.
4. Верификация сигнатуры.

В основе процедуры детектирования лежат автоматы-детекторы, свои для каждого процесса. Автоматный метод поиска совпадений является оптимальным решением как с точки зрения производительности, так и простоты реализации. Другими словами, при каждом новом вызове соответствующий автомат (автоматы) выполняет один шаг –

изменение текущего состояния согласно таблице переходов, это всего 8 машинных инструкций. Решение о детектировании принимается при достижении заключительного состояния.

При совпадении сигнатуры (перехода автомата в заключительное состояние) происходит определение имени процесса по PID и добавление в список обнаруженных угроз нового узла: номер сигнатуры, PID процесса, полный путь до исполняемого файла процесса. В зависимости от предустановленного флага блокирования программ процесс, вызвавший совпадение сигнатуры, может быть принудительно завершен.

Однако метод сигнатур на основе последовательностей системных вызовов (трасс выполнения) подвержен достаточно простой атаке – вставке мусорных системных вызовов. По аналогии с классическими сигнатурами и вставкой мусорных инструкций напрашивается решение – разряженные сигнатуры. Следовательно, опять возникает проблема многократных сравнений трасс выполнения, чтобы отсеять мусор. Это не всегда можно сделать в автоматическом режиме.

Таким образом, функциональная сигнатура на основе последовательности системных вызовов (трасс выполнения) может быть использована для детектирования сложных полиморфных и метаморфных вирусов, для которых построение классической сигнатуры затруднено или невозможно.

ЛИТЕРАТУРА

1. *Белов Е.Б.* Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. М.: Горячая линия – Телеком, 2006. 544 с.

2. *Гайдамакин Н.А.* Разграничение доступа к информации в компьютерных системах // Н.А. Гайдамакин. Екатеринбург: Изд-во УрГУ, 2003. 328 с.

3. *Filiol E.* Metamorphism, Formal Grammars and Undecidable Code Mutation / E. Filiol // PWASET / World Academy of Science, Engineering and Technology. 2007. Vol. 20. P. 1–7.

4. *Zbitskiy P.V.* Code mutation techniques by means of formal grammars and automatons / P.V. Zbitskiy // Journal in Computer Virology / Springer Paris, 2009. Vol. 5, № 2. P. 88–99.

5. *Варновский Н.П.* О применении методов деобфускации программ для обнаружения сложных компьютерных вирусов / Н.П. Варновский и др.// Информационное противодействие угрозам терроризма. М.: ФГПУ НТЦ, 2006. С. 107–126.

6. *Bruschi D.* Using Code Normalization for Fighting Self-Mutating Malware / D. Bruschi., L. Martignoni, M. Monga. Technical Report. Milan: University, 2006. 14 p.

7. *Збицкий П.В.* Функциональная сигнатура компьютерных вирусов / П.В. Збицкий // Доклады ТУСУРа. Томск, 2009. №1 (19), ч. 2. С. 75–76.

УНИВЕРСАЛЬНАЯ ЭЛЕКТРОННАЯ КАРТА

С.Е. Журавлев, студент, М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, Bublik526-3@sibmail.com

Возможности микропроцессорных технологий эффективно применяются в самых различных информационных системах – идентификационных, медицинских, транспортных, телекоммуникационных, банковских и прочих, что способствует быстрому темпу развития государства.

На протяжении последних пяти лет в нашей стране преобладает период «карточного» бума. Абсолютные цифры, характеризующие отечественный сектор обслуживания пластиковых карточек, пока малы по сравнению с аналогичными показателями для западных стран, однако динамика его роста весьма высока.

Не так давно основные средства массовой информации освещали очередное событие государственной важности – инновационный проект, призванный, по заверениям создателей и реализаторов, сделать более прозрачным взаимодействие гражданина с органами власти, сократить количество очередей в соответствующих учреждениях, а также упростить контроль государства за использованием бюджетных средств на местах.

Именно в связи с этим на основании Федерального закона от 27 июля 2010 г. №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» уже с 1 января 2012 г. начнется выдача гражданам России универсальных электронных карт для обеспечения им доступа к государственным, муниципальным и иным услугам, а также возможности оплаты указанных услуг.

Согласно этому закону универсальная электронная карта будет являться документом, удостоверяющим личность гражданина, которая необходима для быстрой идентификации гражданина, обратившегося в орган власти.

Карта будет действительно универсальной: помимо анкетных данных гражданина, она будет содержать информацию о его трудовой деятельности, учебе, уплате налогов, кредитной истории, получаемых социальных пособиях и даже о его здоровье. УЭК заменит водительское удостоверение, банковскую карту, медицинский полис и карту, проездной билет. Скорее всего, она будет содержать и биометрические данные, став, таким образом, основным средством идентификации человека, так что по карточке можно будет даже голосовать на выборах. Но основное ее назначение все же в другом – с ее помощью люди смогут обращаться во все инстанции за «государственными услугами».

На первых порах для совершения действий с УЭК нужен будет компьютер, терминал или банкомат (причем, по всей видимости, любой). Со временем действия с картой можно будет осуществлять и через мобильник: поверх сим-карты нужно будет вставить еще одну карточку, которая и активирует УЭК. Впрочем, насколько это технически возможно, пока не ясно. Создателем и оператором УЭК станет специально учрежденная «Сбербанком» ОАО «Универсальная электронная карта» (его совладельцами являются банки «Уралсиб» и «Ак барс»).

Конфиденциальность информации, содержащейся на карте, окажется под угрозой. С безопасностью УЭК вообще большие проблемы. Необходимо предпринять усилия по защите личной информации от возможного распространения и нецелевого использования. Эффективных способов защиты этой информации государством пока не найдено.

Тем не менее появление УЭК ставит проблему защиты персональной информации на совершенно ином уровне. Ведь, получив доступ к содержимому этой карты, мошенники смогут узнать о человеке все: какой собственностью и доходами он располагает, какими болезнями болеет, где и когда находился; доступ к УЭК позволяет снять деньги со счета, взять кредит. Трудно даже представить, какие последствия для человека может иметь «взлом» пин-кода его УЭК. Не говоря уже о том, что действия мошенников или банальный компьютерный сбой сделают гражданина на какое-то время фактически недееспособным: потеряв свою «виртуальную» личность, он не сможет совершать никаких правовых или финансовых действий.

Но, пожалуй, самым неприятным последствием введения УЭК станет тотальный контроль над человеком со стороны государства. Можно будет с легкостью отследить действия, перемещения и официальные контакты гражданина, сделав на основании этого выводы о его законопослушности и благонадежности. И общаться с «виртуальными» гражданами госорганам будет гораздо легче: если что, УЭК ведь можно и заблокировать.

ЛИТЕРАТУРА

1. Официальный сайт УЭК [Электронный ресурс]. Режим доступа: http://www.uecard.ru

2. [Электронный ресурс]. Режим доступа: http://terrao.livejournal.com/2710697.html#cutid1

3. Информационный портал государственных услуг Санкт-Петербурга [Электронный ресурс]. Режим доступа: http://pgu.spb.ru/priem/ID-karta.php

4. Российская газета [Электронный ресурс]. Режим доступа: http://www.rg.ru/2010/06/23/card.html

РАЗРАБОТКА МЕТОДИКИ СОВМЕСТНОГО ВЫБОРА КЛЮЧА И ТАБЛИЦЫ ЗАМЕН ДЛЯ АЛГОРИТМА ГОСТ 28147–89

В.Ю. Золотухин, студент 5-го курса, каф. БИТ,
Т.А. Чалкин, аспирант МБ СибГАУ
Научный руководитель Т.А.Чалкин, аспирант СибГАУ
г. Краноярск, СибГАУ им. М.Ф. Решетнева, zslavyan@rambler.ru

В настоящее время наиболее эффективными и хорошо изученными методами криптоанализа являются линейный и дифференциальный криптоанализы.

Количественными характеристиками, отражающими устойчивость шифрования к линейному и дифференциальному методам криптоанализа, являются нелинейность и динамическое расстояние [1].

При рассмотрении раунда шифрования алгоритма ГОСТ 28147–89 видно, что нелинейность и лавинный эффект обеспечиваются операциями сложения полублока данных с подключом раунда и замены бит по таблице. Таким образом, определяющим фактором надежности шифрования по ГОСТ 28147–89 является надлежащим образом выбранная ключевая информация (ключ и таблица замен) [1].

Так как криптостойкость обеспечивается, в том числе, и характеристиками ключа, то возникает задача нахождения оценки влияния выбранного ключа на нелинейность преобразования бит в ходе раунда шифрования. В ходе исследований нелинейности операции сложения с ключом шифрования были получены результаты при длине ключа от 4 до 9 бит. Графическое выражение зависимости значения нелинейности преобразования сложения с ключом раунда представлено на рис. 1.

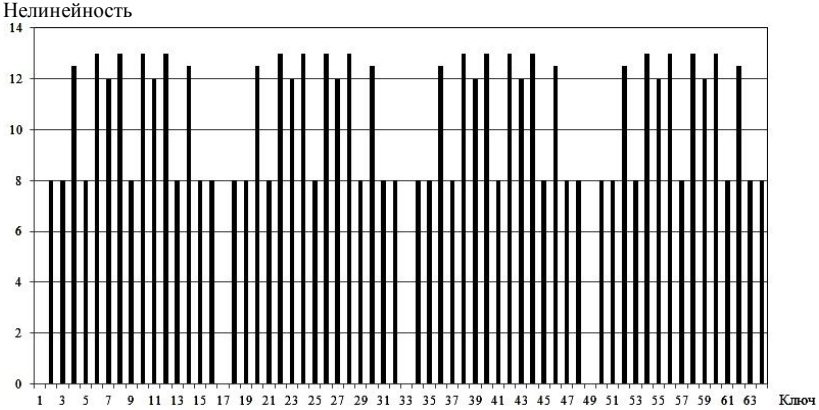


Рис. 1. Гистограмма значений нелинейности операции сложения по модулю 2^n при $n = 6$

Таким образом, при малых значениях числа переменных (n) можно выделить значения ключа, нелинейность операции сложения с которым будет иметь высокие показатели. Однако в алгоритме ГОСТ 28147–89 длина подключа раунда составляет 32 бита, а вычисление нелинейности от такого количества переменных – ресурсоемкая задача.

Если анализировать раунд шифрования в целом, то нелинейность раунда определяется нелинейностью композиции преобразований сложения с подключом раунда и замены бит по таблице.

Пусть характеристикой композиции преобразования будет двойка значений нелинейности (блок, композиция). При исследовании композиции преобразований сложения с подключом раунда и замены бит пространство исследования в рамках упрощенного варианта ГОСТ (таблица замен состоит из одного узла и ключ шифрования – 16 бит) составляет 16^{17}. В связи с этим исследования проводились с каждым возможным значением ключа (16 различных значений) и случайно сгенерированными узлами замен по 1 млн штук на одно значение ключа. Так как значение нелинейности операции сложения с подключом в классическом смысле равно нулю, то зададим характеристику композиции как двойку (нелинейность узла замен, нелинейность композиции). Результаты исследований представлены на рис. 2.

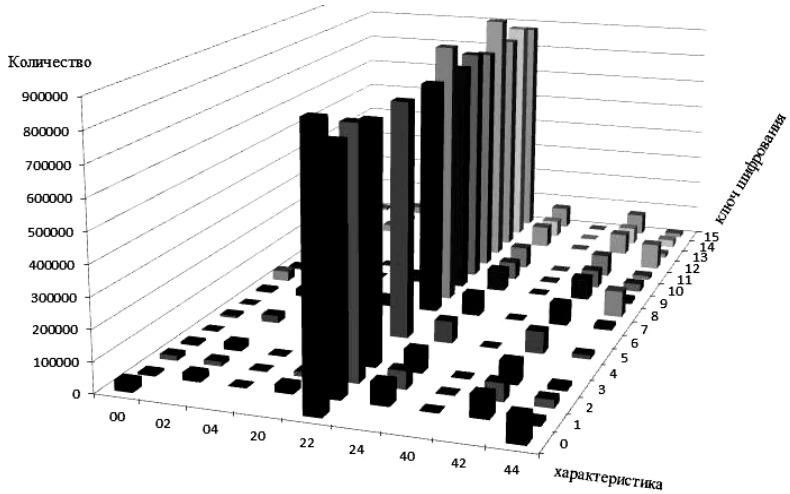


Рис. 2. Гистограмма распределения значений нелинейности при упрощенном варианте шифра ГОСТ 28147–89

В ходе анализа вышеприведенных данных были сделаны выводы о том, что для конкретного узла замен существуют такие значения

ключа, которые могут увеличить (характеристики (0,2), (0,4), (2,4)), уменьшить (характеристики (2,0), (4,0), (4,2)) или оставить без изменений (характеристики (0,0), (2,2), (4,4)) значение параметра нелинейности. Это означает, что выбор качественного ключа или таблицы замен в отдельности в общем случае не обеспечивает высоких значений нелинейности, поскольку существует взаимное влияние элементов ключевой информации.

Алгоритм генерации криптостойких узлов замен, приведенный в работе [2], позволяет создать 2 набора оптимальных с точки зрения параметров нелинейности и динамического расстояния узлов замен. Общее количество таких узлов составило порядка 10 млн штук.

В ходе исследований данных узлов замен на выборке, составляющей порядка 30% от всего множества перебора, оказалось, что для любого узла не существует такого значения ключа, которое ухудшает его нелинейность. На основании этого была выдвинута гипотеза о том, что, используя узлы замен, построенные с помощью данного алгоритма, можно выбирать любое значение ключа, и такой показатель криптостойкости, как нелинейность, останется на высоком уровне.

ЛИТЕРАТУРА

1. *Золотухин В.Ю.* Разработка методики оценки зависимости криптостойкости шифрования по алгоритму ГОСТ 28147–89 от выбранной ключевой информации / В.Ю. Золотухин, Т.А. Чалкин // Научная сессия ТУСУР–2010: матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых, Томск, 4–7 мая 2010 г. Томск: В-Спектр, 2010. С. 246–249.

2. *Чалкин Т.А.* Алгоритм построения узлов замен алгоритма шифрования ГОСТ 28147–89 / Т.А. Чалкин, К.М. Волощук // Вестник Сиб. гос. аэрокосмического ун-та им. академика М.Ф. Решетнева. Вып. 1 (22): В 2 ч. Ч. 2 / Под общ. ред. Г.П. Белякова. Красноярск: Сиб. гос. аэрокосмич. ун-т, 2009. С. 46–50.

ИСПОЛЬЗОВАНИЕ ЛОВУШЕК В ЛОКАЛЬНОЙ СЕТИ КАМПУСА УНИВЕРСИТЕТА

М.О. Золотых, аспирант каф. теоретических основ радиотехники
г. Екатеринбург, ФГАОУ ВПО УрФУ им. первого Президента России Б.Н. Ельцина, zolotih@isnet.ru

В настоящее время одной из самых распространённых технологий построения компьютерных сетей является Ethernet. Стандарт Ethernet в совокупности со стеком TCP/IP обладает целым рядом серьёзных уязвимостей (возможность подделки IP адреса, arp-спуффинг и т.д.). Недостатки протоколов обмена данными компенсируются функциями

безопасности, встраиваемыми в современное коммутационное оборудование. Однако в больших сетях (несколько тысяч абонентов) «разом» заменить всё оборудование невозможно. Наиболее проблемными являются участки сети, построенные с применением «неуправляемых» коммутаторов (т.е. коммутаторов, не имеющих настраиваемых функций). При использовании «неуправляемых» коммутаторов обеспечивать безопасность сети достаточно сложно: нельзя получить данные о трафике между абонентами одного широковещательного сегмента, в случае атаки затруднительно обнаружить источник и нельзя управлять доступом одного отдельно взятого узла к среде передачи данных. Соответственно, в таких сетях не могут нормально работать средства обнаружения и предотвращения атак, необходимость которых в крупных сетях сомнения не вызывает. Для противодействия угрозам безопасности в подобных сетях могут применяться ловушки.

Ловушка – ресурс автоматизированной системы, представляющий собой приманку для нарушителя и не участвующий в основном процессе обработки информации в системе. В англоязычной литературе для обозначения ловушек применяется термин «Honey pot» – горшочек с мёдом. Ловушки не позволяют непосредственно предотвратить проведение атаки, но при этом решают три основных задачи:

- задержка злоумышленника и отвлечение его от реальных объектов атаки;
- сбор доказательной базы;
- исследование способов взлома (сбор статистики).

При защите информации следует помнить, что ловушки не могут выступать основным средством защиты: всегда существует риск того, что злоумышленник не поверит приманке (либо будет знать о её существовании заранее). Поэтому наряду с ловушками всегда должны применяться «классические» средства защиты: межсетевые экраны, уже упомянутые средства обнаружения атак, антивирусные системы и т.п. В то же время не всегда есть возможность развернуть необходимые системы безопасности в достаточном объеме.

В качестве примера рассмотрим сети студенческого городка УрФУ. Локальная сеть УрФУ насчитывает не менее 10 тысяч узлов и поэтому требует особого подхода к обеспечению безопасности: невозможно (слишком дорого) единовременно проводить модернизацию всего оборудования и программного обеспечения. Анализируя опыт работы отдела развития и эксплуатации компьютерной сети УрФУ, можно отметить, что правонарушения в области информационной безопасности (кража паролей, распространение вредоносных программ) чаще всего встречаются именно в сегменте сети студенческого

городка. В последнее время наблюдается устойчивое снижение преступной активности, связанное с отказом от лимитированных тарифов доступа к сети Интернет, что, очевидно, не свидетельствует о повышении качества защиты информации, так как исчезает причина, но не возможность осуществления атак. Не секрет, что студенты являются одной из самых социально активных частей населения, и в их среде распространены наиболее популярные мотивы взлома информационных систем: желание получить выгоду, стремление к самоутверждению, вандализм, месть. Помимо этого, распространение технических новинок и овладение новыми знаниями в молодёжной среде всегда происходят очень активно. Размещение ловушек в сетях кампусов позволит изучить поведение внутренних нарушителей: большое количество участников информационной системы позволяет накопить достаточную статистику. Располагая ловушки в различных сегментах сети (например, в сетях общежития радиотехнического или строительного факультетов), можно получить различные модели нарушителя с различным уровнем профессиональной подготовки (опасности).

Планируемая модернизация компьютерных сетей и, как следствие, существенное повышение уровня защиты займут как минимум несколько лет и потребует значительных финансовых вложений. Внедрение ловушек позволило бы повысить защиту абонентов в ближайшей перспективе (путём отвлечения злоумышленника) и наработать статистику, которая в дальнейшем обеспечила бы более эффективное внедрение системы предотвращения атак. Сети, подобные сети студенческого кампуса, с наличием большого числа неуправляемых коммутируемых сегментов, достаточно распространены, в частности встречаются на крупных предприятиях, поэтому приобретенный опыт по применению ловушек для снижения числа инцидентов может быть трансформирован по мере необходимости.

ИССЛЕДОВАНИЕ ПРИЧИН ВОЗНИКНОВЕНИЯ И ХАРАКТЕРА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ КЛАВИАТУРЫ ПЭВМ

С.Д. Беспалов, студент каф. информационной безопасности
Научный руководитель А.А. Хорев, зав. каф. информационной безопасности, проф., д.т.н.
г. Москва, МИЭТ, bespalov-sd@rambler.ru

Одним из наиболее опасных технических каналов утечки информации при ее обработке СВТ является канал утечки, возникающий за счет побочных электромагнитных излучений (ПЭМИ) клавиатуры,

поскольку именно с ее использованием в компьютер вводятся различные пароли и текстовые документы.

Проведенный анализ показал, что в открытой отечественной и зарубежной литературе практически отсутствуют публикации, посвященные исследованию ПЭМИ, возникающих при вводе данных с клавиатуры.

Целями проведенных автором исследований являлись:

− на основе анализа принципов работы клавиатуры определение причин возникновения ПЭМИ и их характера;

− экспериментальные исследования структуры информативных сигналов, передаваемых по тракту клавиатуры;

− разработка рекомендаций по выбору тестового режима работы клавиатуры, обеспечивающего максимизацию отношения сигнал/шум на фоне собственных шумов измерительного приемника при измерении ПЭМИ клавиатуры.

В результате проведенных исследований установлено:

Обмен данными между клавиатурой PS/2 и контроллером клавиатуры в компьютере осуществляется асинхронно по последовательному протоколу. Суть асинхронной передачи состоит в том, что данные передаются только тогда, когда есть что передавать – нажата/отпущена клавиша на клавиатуре и нужно выдать соответствующий скан-код или контроллеру нужно выдать команду клавиатуре. Для обмена данными в клавиатуре PS/2 служат две линии – данных и синхронизации.

Частота следования импульсов линии синхронизации для различных клавиатур может колебаться в диапазоне 6 кГц. Амплитуда импульсов для клавиатур PS/2 составляет 5 В и практически не зависит от типа выбранной клавиатуры. Длительность импульса, передаваемого в линию сигнала, составляет 80 мкс [1, 2].

Данные передаются в следующем порядке: один стартовый бит – «0»; восемь бит данных; бит четности (сумма всех разрядов +1); один стоповый бит – «1». Например, при передаче «скэн-кода» клавиши «=» в линию поступит последовательность бит – 01010101011 (рис. 1).

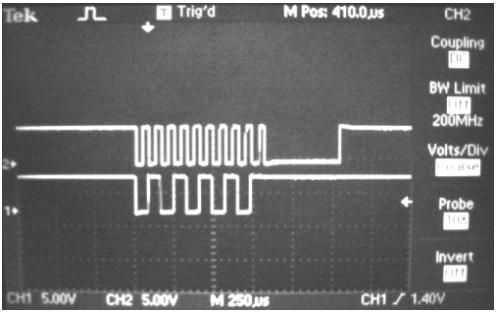
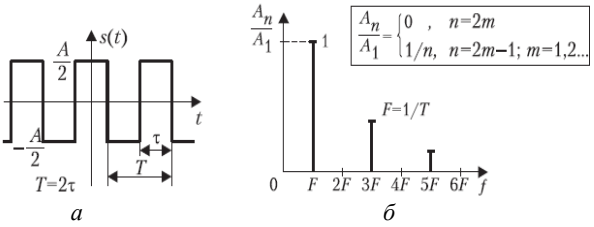


Рис. 1. Осциллограмма передачи клавиши «=»

Вид спектрограммы сигнала во многом зависит от длительности импульсов τ и периода колебаний T. На рис. 2 показана осциллограмма периодического прямоугольного сигнала со скважностью $Q = 2$ и его спектрограмма [3].



а *б*

Рис. 2. Осциллограмма сигнала со скважностью $Q = 2$ (*а*) и его спектрограмма (*б*)

Побочное электромагнитное излучение клавиатуры возникает при прохождении импульсного сигнала от клавиатуры к системному блоку по соединительному кабелю.

Спектр ПЭМИ определяется видом импульсного сигнала. Энергия периодического сигнала распределена между гармониками на определенных частотах, а энергия непериодического сигнала – по всему спектру частот.

Поскольку спектральная характеристика непериодического сигнала как функция частоты представляет собой хаотический процесс, поиск информативного сигнала средством перехвата должен осуществляться по всему диапазону частот, в котором возможно появление спектральных составляющих сигнала. Частоты излучения спектральных составляющих периодического сигнала являются фиксированными и зависят от периода колебания T и длительности импульсов τ.

Таким образом, в качестве тестового режима работы клавиатуры при оценке ее защищенности СВТ от утечки информации за счет ПЭМИ целесообразно использовать режим, при котором в компьютер передается периодический сигнал со скважностью $Q = 2$, что позволяет максимизировать отношение сигнал/шум на выходе измерительного приемника за счет некогерентного накопления импульсов и значительно упростить процесс измерения ПЭМИ.

Проведенные исследования показали, что последовательности импульсов, близкие к периодической последовательности и имеющие значение скважности $Q = 2$, поступают в линию при передаче сканкода от клавиши «=» (01010101011), клавиши «Pp» (01100110011) и клавиши «BackSpace» (00110011010). Разница в спектрах сигналов, полученных от нажатия перечисленных клавиш, будет наблюдаться из-за разницы в длительности импульса сигнала и периоде колебаний.

Так для сигнала, полученного от нажатия клавиши «=», длительность импульса составит 80 мкс, а период колебаний будет равен 160 мкс, для клавиш «Pp» и «BackSpace» длительность импульса составит 160 мкс, а период колебаний будет равен 320 мкс. Следовательно, тактовая частота излучаемого сигнала для клавиши «=» будет равна F = 6,25 кГц, а для клавиш «Pp» и «BackSpace» – F = 3,125 кГц.

Следовательно, при использовании предлагаемого тестового режима работы клавиатуры измерение ПЭМИ клавиатуры может осуществляться на фиксированных частотах, что повышает вероятность обнаружения информативного сигнала и значительно упрощает процесс измерений.

ЛИТЕРАТУРА

1. *Имитируем* работу клавиатуры [Электронный ресурс]. Режим доступа: http://kazus.ru/articles/18.html

2. *Мембранная* клавиатура [Электронный ресурс]. Режим доступа: http://electronic.vladbazar.com/index.php?do=search&story=%CA%EB%E0%E2%E8%E0%F2%F3%F0%E0&subaction=search.

3. Новиков Ю.Н., Фадеев А.О. Частотные спектры электрических колебаний [Электронный ресурс]. Режим доступа: http://www.cee.spbstu.ru/doc_popov/otez/lab20_z.pdf.

ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ

С.О. Бургашвили, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС

Беспроводные сети применяются в большинстве компаний любого масштаба благодаря своей низкой стоимости и простоте развёртывания. Для получения максимальных преимуществ беспроводных сетей необходима их защита. Незащищенные беспроводные сети открывают практически неограниченный доступ к корпоративной сети для хакеров и других злоумышленников, которые нередко стремятся лишь получить бесплатный доступ в Internet. В крупных учреждениях могут существовать несанкционированные беспроводные сети – члены рабочих групп или конечные пользователи подчас игнорируют корпоративную политику и устанавливают точки доступа (Access Points, AP), и это таит в себе большую опасность для предприятия. Владельцы незащищенных сетей должны быть готовы и к снижению пропускной способности Internet-соединения, и к проникновению вирусов и червей, и даже к несению уголовной или гражданской ответственности за использование незащищенных сетей для осуществления атак против третьих лиц.

Тема безопасности беспроводных сетей всегда была и остаётся актуальной на данный момент. Существуют достаточно надёжные стандартные средства защиты таких сетей. Базовым средством защиты является **технология WPA** (Wi-Fi Protected Access). Большинство существующего на данный момент Wi-Fi-оборудования имеет поддержку данной технологии. Главной особенностью этого стандарта является технология динамической генерации ключей шифрования данных, построенная на базе протокола TKIP (Temporal Key Integrity Protocol), представляющего собой дальнейшее развитие алгоритма шифрования RC4. По протоколу TKIP сетевые устройства работают с 48-битным вектором инициализации (в отличие от 24-битного вектора WEP) и реализуют правила изменения последовательности его битов, что исключает повторное использование ключей. В протоколе TKIP предусмотрена генерация нового 128-битного ключа для каждого передаваемого пакета. Кроме того, контрольные криптографические суммы в WPA рассчитываются по новому методу, носящему название MIC (Message Integrity Code). В каждый кадр здесь помещается специальный восьмибайтный код целостности сообщения, проверка которого позволяет отражать атаки с применением подложных пакетов. В итоге получается, что каждый передаваемый по сети пакет данных имеет собственный уникальный ключ, а каждое устройство беспроводной сети наделяется динамически изменяемым ключом.

Кроме того, протокол WPA поддерживает шифрование по стандарту AES (Advanced Encryption Standard), т.е. по усовершенствованному стандарту шифрования, который отличается более стойким криптоалгоритмом по сравнению с протоколами WEP и TKIP. При развертывании беспроводных сетей в домашних условиях или в небольших офисах обычно используется вариант протокола безопасности WPA на основе общих ключей – WPA-PSK (Pre Shared Key). Базовый вариант протокола WPA ориентирован в основном на корпоративные сети, так как авторизация пользователей при выборе этого протокола производится на отдельном RADIUS-сервере. При применении WPA-PSK в настройках точки доступа и профилях беспроводного соединения клиентов указывается пароль длиной от 8 до 63 символов.

Дополнительными мерами для надёжной защиты беспроводной сети являются фильтрация физических адресов (MAC-адресов) и режим скрытой идентификации сети SSID.

Фильтрация MAC-адресов. Эта функция поддерживается всеми современными точками доступа и беспроводными маршрутизаторами, хотя и не является составной частью стандарта 802.11. Считается, что данная мера позволяет повысить уровень безопасности беспроводной сети. Для реализации данной функции в настройках точки доступа

создается таблица MAC-адресов беспроводных адаптеров клиентов, авторизованных для работы в данной сети.

Режим скрытой идентификации сети SSID. Это еще одна мера предосторожности, которую часто используют в беспроводных сетях. Каждой беспроводной сети назначается свой уникальный идентификатор (SSID), который представляет собой название сети. Когда пользователь пытается войти в сеть, драйвер беспроводного адаптера прежде всего сканирует эфир на предмет наличия в ней беспроводных сетей. При применении режима скрытого идентификатора (как правило, этот режим называется Hide SSID) сеть не отображается в списке доступных и подключиться к ней можно только в том случае, если, во-первых, точно известен ее SSID, а во-вторых, заранее создан профиль подключения к этой сети.

Используя протокол WPA в совокупности с методом фильтрации физических адресов и режимом скрытой идентификации сети, можно обеспечить вполне надёжную защиту беспроводной сети. Более высокого уровня защиты возможно достичь при использовании дополнительных средств защиты на каждом узле беспроводной сети. К таким средством относятся межсетевые экраны, антивирусы, системы обнаружения вторжений, средства шифрования трафика (компоненты технологии VPN).

СОЗДАНИЕ ВЕБ-САЙТА ФИЛИАЛА ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ В г. СУРГУТЕ

Д.В. Гаврилов, студент
г. Томск, ТУСУР, ФВС, rs24@yandex.ru

Чтобы облегчить доступ для абитуриентов и студентов, было решено создать веб-сайт филиала Томского государственного университета систем управления и радиоэлектроники в г. Сургуте.

На сайте есть необходимые материалы для абитуриентов, такие как правила приема в университет, контакты филиала и т.д. Также есть необходимая информация для студентов: новости филиала, фотогалерея и другая информация.

Существует еще одна немаловажная проблема. На протяжении сессии деканатом выдается большое количество экзаменационных листов студентам. При этом существует вероятность ошибки при выдаче и обработке экзаменационных листов.

Проблема заключается в том, чтобы быстро и правильно выдать экзаменационные листы, а также быстро и без ошибок обработать их.

Подсчитаем время, затрачиваемое на выписку и обработку экзаменационных листов.

В день, во время сессии, деканат выписывает примерно 40 экзаменационных листов, соответственно за рабочую неделю деканат выпишет около 240 экзаменационных листов. На каждый экзаменационный лист тратится около 5 мин, учитывая, что его необходимо пронумеровать и зафиксировать в журнале. Итого получаем 1200 мин, в рабочую неделю выходит около 20 ч, и эти часы деканат по сути тратит впустую.

Чтобы избежать траты времени на выписку и обработку экзаменационного листа, было решено создать автоматизированную систему выдачи и регистрации экзаменационных листов.

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 сети университета для определения изменений в материале, что не всегда удобно. Эта проблема особенно существенна для студентов заочной формы обучения, которым приходится специально посещать университет.

Чтобы решить данную проблему, было решено на веб-сайте филиала создать систему обновления литературы, в которой преподаватель мог бы загружать информацию и литературу непосредственно на сайт и уведомлять об этом студентов.

Еще одна проблема – это уведомление студентов о предстоящих событиях, таких как экзамены, зачеты, сдача долгов и пр. Так как возможны изменения в расписании предметов, в расписании сдачи долгов, то необходимо своевременно предупредить студентов об этом изменении. Так как есть студенты, которые пропускают занятия, то их сложно уведомить об этом. В данный момент используется способ звонка преподавателя старостам, но это не всегда удобно и практично.

Чтобы решить данную проблему, было решено создать на сайте систему уведомлений, в которой преподаватель может написать необходимое объявление и разослать всем студентам или группам студентов. Все объявления должны отправляться на E-mail студентам.

Чтобы решить данные проблемы, был создан веб-сайт филиала.

Во-первых, веб-сайт будет доступен из любой точки России, во-вторых, веб-сайт – это современное и практичное средство представления и обработки информации.

Благодаря этому, студенту не составит проблем зайти на веб-сайт филиала и получить необходимую информацию и выполнить необходимые действия, а именно – выписать экзаменационный лист, скачать задания по предмету, задать вопрос преподавателю и т.д.

Также на сайте будет выложен весь необходимый информационный материал для студентов и абитуриентов.

Особенно важно не только решить эти проблемы, но и обеспечить безопасность сайта и пользовательских данных на нем.

Для этого разработана система защиты сайта от возможных уязвимостей и атак, таких как SQL injection, XSS атаки и брутфорс атаки.

ЛИТЕРАТУРА

1. *Колисниченко Д.Н.* Самоучитель PHP-5. СПб.: Наука и техника, 2004. 576 с.
2. *Паутов А.В.* Самоучитель MySQL. М.: НТ Пресс, 2005. 376 с.

СИСТЕМА ТЕСТИРОВАНИЯ ЗНАНИЙ СТУДЕНТОВ

К.А. Козловский, В.Б. Егоров, Н.В. Чижов, А.Н. Сусиков, студенты
г. Томск, ТУСУР, ФВС, каф. КИБЭВС

Разрабатываемая система предназначена для проведения тестирования знаний студентов по различным направлениям обучения.

Цель работы – повышение качества обучения.

На данный момент в Министерстве образования и науки Российской Федерации ведется внедрение федеральных государственных образовательных стандартов третьего поколения (далее ФГОС). В ФГОС 3-го поколения при разработке учебного плана используется компетентностный подход. Происходит переход от дидактических единиц и тем к компетенциям, дидактические единицы и темы подразумевают тесты, в которых нужно было выбирать правильные варианты ответов и т.п. Компетенции же будут оценивать практические навыки студента. Студент должен уметь применять свои навыки на практике. Тем самым компетентностный подход предполагает перестройку контрольно-оценочной составляющей образовательного процесса. Сущность перестройки состоит в переходе от оценки знаний к оценке компетенций как результатов образования. Разрабатываемая система строится с учетом современных методик проведения тестирования и компетентностного подхода при разработке тестовых заданий и оценке компетенций.

Мерой трудоемкости при компетентностном подходе ООП ВПО, является зачетная единица (36 ч). Одной зачетной единице соответствует один кредит ECTS (Европейская система переноса и накопления кредитов – EuropeanCreditTransferSystem). Трудоемкость каждой дисциплины будет оцениваться не в часах, а в зачетных единицах. Между академическими часами, отводимыми на изучение отдельных элементов образовательной программы, и зачетными единицами существует определенная зависимость, но не всегда прямо пропорциональная. При оценивании результатов тестирования необходимо учитывать такие показатели дисциплины, как важность и сложность.

Поскольку требуется перестройка оценочной составляющей учетного процесса, кроме традиционных оценок, в системах предполагается определять рейтинг студента. Рейтинг должен учитывать не только традиционную оценку знания, но и активность студента в плане научной работы, дисциплинированность и др.

Был проведен анализ систем тестирования, результат анализа двух из них приведен ниже:

Система SchoolhouseTest:

1) программа для создания тестов на бумаге. Не создает тесты в электронном виде;

2) предусмотрена возможность смены цветовой схемы интерфейса (в целом интерфейс очень похож на интерфейс программ серии MicrosoftOffice);

3) программа полностью на английском языке;

4) программное обеспечение платное:

– Single User License – USD $59;

– Small Site License (less than 250 students) – USD $149;

– Medium Site License (250 to 600 students) – USD $224;

– X-Large Site License (more than 1000 students) – USD $374;

5) возможность включения проверки правописания;

6) по ходу работы выскакивает автонапоминание с сохранением;

7) в программе имеется полное руководство, но на английском языке;

8) добавление вопросов по шаблону (9 типов вопросов);

9)возможность добавления комментариев к вопросу и инструкций;

10) при вводе вопросов в форму можно одновременно просматривать результат, который получится на бумаге;

11) расширенные возможности для создания вопросов (добавление рисунка, таблица символов, диаграмм, графиков, шрифт и др.).

Система тестирования FEPO:

1) программное обеспечение для тестирования знаний студентов;

2) создание тестов происходит вручную;

3) каждый тест содержит в себе несколько дидактических единиц (ДЕ), каждая из которых содержит в себе несколько тем;

4) информацию по темам можно посмотреть на сайте www.fepo.ru;

5) студента оценивают по следующей системе: если в каждой ДЕ, выполнено правильно больше половины тем, то тест пройден, иначе если хотя бы одна ДЕ не зачтена, то тест провален;

6) вопросы пяти типов;

7) руководство по созданию своего теста занимает не менее 40 листов;

8) свой тест создается с помощью специальных тегов в текстовом документе, всю информацию о создании теста можно узнать из руководства;

9) после выполнения теста можно оставить отзыв;

10) вопросы хранятся в зашифрованной базе данных;

11) ответы хранятся у разработчиков;

12) после прохождения теста формируется файл статистики и отправляется разработчикам, они сверяют ответы с правильными и выносят решение;

13) база готовых тестов огромна;

14) тестирование можно пройти онлайн прямо на сайте.

Результаты анализа показали, что каждая из систем имеет свои недостатки и использовать их в нашем проекте нельзя, следовательно, нужно создавать своё программное обеспечение.

На основании результатов, полученных при проведении ЕГЭ и FEPO, можно сказать, что у преподавателей сложилось отрицательное отношение к тестированию. В наших планах – реализовать систему, в которой будут учтены достоинства и недостатки других систем, которая будет объективно оценивать знания студента и учитывать изменения, заложенные ФГОС 3-го поколения.

В результате работы на данном этапе был проведен анализ аналогов. Была разработана концепция системы, разработана структура БД, определены функции и интерфейс.

Работы выполнены в рамках программы ГПО КИБЭВС-1006 – «Мехатронные системы».

О ПРИМЕНЕНИИ ПРИБОРОВ «ИСКУССТВЕННОЕ УХО» ДЛЯ ПРОВЕРКИ АУДИОМЕТРОВ ПО КОСТНОЙ ПРОВОДИМОСТИ

С.Ю. Кравец, студент

Научный руководитель Р.В. Мещеряков, доцент, к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, tstoz@mail.ru

Применение приборов «Искусственное ухо» с параметрами, приближенными к параметрам человеческого уха, для проверки аудиометров и слуховых аппаратов, а также их калибровки позволит повы-

сить качество и точность при определении количественной оценки слуха человека.

В работе был проделан обзор аудиометров отечественных и зарубежных производителей, способов их применения для изучения костной проводимости и для снятия характеристик остроты слуха человека.

Обзор устройств для проверки аудиометров и подбор функциональных схем, датчиков и прочих решений был крайне затруднен из-за отсутствия информации. Это наводит на мысль о том, что этих устройств крайне мало и они очень востребованы, что подтверждает то, что они редко встречаются в научной литературе и каталогах электроники. Причем из всех наименований приборов типа «Искусственное ухо» фигурировали российские разработки, что позволяет сделать предварительные выводы о том, что зарубежных аналогов нет, хотя в работе была приведена статья с публикацией изобретения для калибровки слуховых аппаратов и аудиометров со ссылкой на аналог в одном зарубежном источнике 1990 г. [1–5].

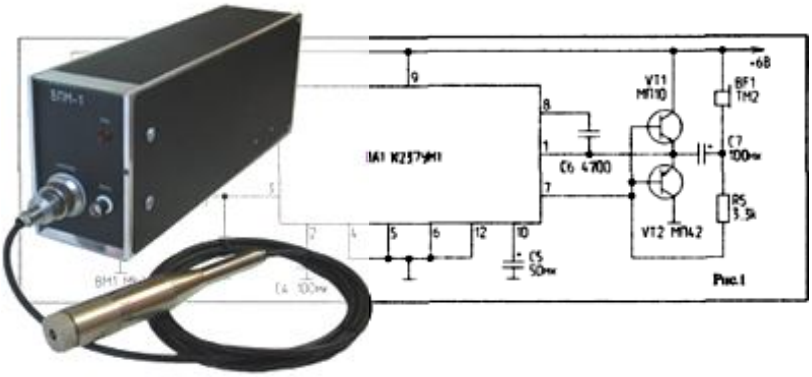


Рис. 1

Опираясь на изученный материал по аудиометрам и приборам для их проверки и калибровки, можно сделать вывод, что это очень сложный и трудоемкий процесс, а потому такой прибор, как «Искусственное ухо», который по своим техническим характеристикам приближен к параметрам человеческого уха, должен существенно упростить задачу.

В процессе поиска электрических схем, сборочных чертежей и другого материала по приборам «Искусственное ухо» в связи с отсутствием таковой информации неожиданно было найдено интересное и, возможно, удачное решение – использование электрической и принципиальной схемы прибора – регистратора слабослышимых акустических сигналов [6, 7]. Он используется для диагностики неисправностей

двигателей внутреннего сгорания; поиска мест утечек/натекания газа или воды из поврежденных газопроводных и водопроводных сетей; диагностики патологии внутренних органов; организации акустической связи. Это высокочувствительное устройство для регистрации слабых акустических сигналов вполне может выступать в качестве устройства для проверки аудиометров.

Таким образом, задача работы заключается в проектировании устройства типа «Искусственное ухо» для проверки аудиометров на основе анализа полученной информации.

ЛИТЕРАТУРА

1. Каталог слуховых аппаратов и аудиометров из Швейцарии магазина ALFATON. http://surdology.ru/professionals/equipment/audiometers.html ;

2. Каталог слуховых аппаратов и аудиометров ООО «Прибор» http://www.td-pribor.ru/print/13280.htm

3. Каталог поставки контрольно-измерительных приборов «Метра-Телеком» http://www.metrarus.ru/kip/element.php-ID=40593.htm

4. Аппараты телефонные цифровые – стандарт отрасли http://projekt.org.ru

5. *Шмальченко В.П., Усанов В.А.* Описание изобретения к патенту Российской Федерации. Научная публикация от 20.06.1996 г.

6. *Эфрусси М.М.* Слуховые аппараты и аудиометры // Массовая радиобиблиотека. Вып. 901. М., Энергия. 1975.

7. Схемки.ру http://shemki.ru/readarticle.php?article_id=369 «Электронное ухо как регистратор слабослышимых акустических сигналов».

СИСТЕМА ИЗМЕРЕНИЯ, СБОРА, АНАЛИЗА, ПРЕДСТАВЛЕНИЯ И ИНТЕРПРЕТАЦИИ ИНФОРМАЦИИ О ПОСЕТИТЕЛЯХ ВЕБ-САЙТОВ «WEB ANALYTICS»

В.А. Легасов, студент, Р.В. Мещеряков, доцент, к.т.н.
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, vilotiv@gmail.com

Анализ веб-сайта – это сложный и трудоемкий процесс. Каждый отдельно рассматриваемый сайт уникален, на его деятельность влияет много субъективных и объективных факторов. Вследствие этого перед началом анализа сайта нужно подобрать необходимый набор инструментов и разработать оптимальную стратегию. Задача значительно упрощается, если используются автоматизированные системы веб-аналитики («Web Analytics»), которые предоставляют данные о действиях посетителей на сайтах.

Выход веб-сайта в топ-позиции поисковых систем и увеличение его посещаемости не решают проблему его эффективности. Посетители, которым нравится сайт, приходят на него снова и снова. Таким об-

разом, они превращаются в целевую аудиторию веб-сайта. У сайта, владельцы которого занимаются только его раскруткой, может быть и 5 тыс. посетителей в сутки, но они будут приходить и уходить. Веб-сайт, оптимизированный с учетом анализа поведения его посетителей, может иметь и втрое меньше посетителей, но это устойчивая целевая аудитория, а значит, потенциальные клиенты.

Анализ посещаемости веб-страниц позволяет устранить проблемы в процессе взаимодействия посетителей с веб-сайтом и повысить уровень его эргономичности.

Необходимо проанализировать, что конкретно посетителям нравится и не нравится на сайте. Система веб-аналитики может помочь решить данную задачу. Благодаря «Web Analitics» можно наглядно представить, какие затруднения посетители испытывают при взаимодействии с веб-сайтом. Если убрать или видоизменить проблемные зоны, то впечатления посетителей от сайта изменятся в лучшую сторону.

Для того чтобы понять уникальные особенности взаимодействия посетителя с веб-сайтом, нужно проанализировать ряд важных измерений. Например, по каким ключевым словам или фразам посетитель пришел на сайт, какую поисковую систему он использовал, страна, регион и город его проживания и т.д. Все это в той или иной мере влияет на его дальнейшее поведение на веб-сайте.

Многие пользователи ассоциируют веб-аналитику со статистикой посещаемости сайта или с оценкой юзабилити сайта. Однако веб-аналитика – это не только статистика посещаемости сайта и анализ его юзабилити, но и ряд других аспектов, относящихся к деятельности веб-сайта:

- анализ эффективности рекламных кампаний;
- отслеживание мошеннических действий на веб-сайте;
- анализ контента веб-сайта и его проблемных (отвлекающих) элементов;
- анализ процесса заполнения веб-форм.

При анализе посещаемости веб-сайта в первую очередь стоит обратить внимание на страницы входа (рис. 1) и выхода, потому что страница входа создает первое впечатление о сайте, а на странице выхода прерывается взаимодействие посетителя с веб-сайтом.

С помощью данного отчета необходимо определить, какие страницы сайта наиболее популярны, и проанализировать процесс взаимодействия с ними посетителей. Целью данного анализа является минимизация количества отказов (уходов с этой страницы).

На данный момент автоматизированная система статистики «Web Analytics» собирает данные с сайтов http://isib.su/ и http://kibevs.tusur.ru/drop/. Краткая сводка полученных данных представлена на рис. 2.

URL страницы	Входы ▾	Bounces	Доля пользователей, ушедших после просмотра одной страницы
⊖ **drop**	**495**	**261**	**53%**
/index	339	152	45%
⊖ **?q=node**	**146**	**102**	**70%**
/130	53	38	72%
/125	32	28	88%
/127	13	11	85%

Рис. 1. Страницы входа

Сайт ▲	Посещений	Просмотры страниц	Уникальных посетителей	Развитие Посещений	
ISIB	101	527	49	-4.72 %	
KIBEVS	39	62	28	8.33 %	
Kibevs/DROP	516	1579	231	9.09 %	

Рис. 2. Сводная статистика всех сайтов

С помощью автоматизированной системы веб-аналитики возможно получение исчерпывающей информации по посетителям веб-сайта. Дружественный интерфейс системы делает ее удобной и понятной для пользователей, не имеющих специальных навыков в продвижении, поскольку каждый инструмент системы снабжен подробными пояснениями и комментариями.

С помощью системы статистики можно отслеживать:

− посещаемость сайта;
− географическое положение посетителей сайта;
− источники посетителей (поисковый трафик);
− какие страницы являются наиболее востребованными;
− позиции сайта в поисковых системах;
− ключевые поисковые фразы и слова;
− пути посетителей по сайту (откуда пришел посетитель, сколько времени провел на сайте, какие и сколько страниц посмотрел, куда ушел);
− точки входа/выхода;
− возвраты на сайт;
− постоянную аудиторию и многое другое.

ЛИТЕРАТУРА

1. *Клифтон Брайан.* Google Analytics: профессиональный анализ посещаемости веб-сайтов: Пер. с англ. М.: ИД Вильямс, 2009. 400 с.

2. Сбор статистики на PHP. [Электронный ресурс]. Режим доступа: http://www.citforum.ru/internet/php/stat_on_php/.

3. *Дари К., Бринзаре Б., Черчез-Тоза Ф., Бусика М.* AJAX и PHP. Разработка динамических веб-приложений. М.: Символ-Плюс, 2006. 333 с.

4. *Гутманс Э., Баккен С., Ретанс Д.* PHP-5. Профессиональное программирование. М.: Символ-Плюс, 2006. 703 с.

5. Определение географического положения пользователей сайта по IP своими руками [Электронный ресурс]. Режим доступа: http://www.5w.ru/site1.html

6. Определение местоположения пользователя по его IP [Электронный ресурс]. Режим доступа: http://js-php.ru/web-development/php-development/get-geo-info-by-ip/

СИСТЕМА АУТЕНТИФИКАЦИИ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ ЛИЦА

Д.А. Немятовских, студент, Г.А. Праскурин, ст. преподаватель

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, abc_xyz@sibmail.com

Подсистема аутентификации пользователей – важнейший компонент корпоративной системы информационной безопасности, и ее значение трудно переоценить. Подсистема аутентификации подтверждает личность пользователя информационной системы и поэтому должна быть надежной и адекватной, то есть исключать все ошибки в предоставлении доступа. Существующие методы аутентификации различны по степени надежности, и, как правило, с усилением защиты резко возрастает цена систем, что требует при выборе средств аутентификации анализа рисков и оценки экономической целесообразности применения тех или иных мер защиты.

В настоящее время всё более широкое распространение получают биометрические системы идентификации человека. Традиционные системы идентификации требуют знания пароля, наличия ключа, идентификационной карточки либо иного идентифицирующего документа, который можно забыть, потерять или подделать. В отличие от них биометрические системы основываются на уникальных биологических характеристиках человека, которые трудно подделать и которые однозначно определяют конкретного человека. К таким характеристикам относятся отпечатки пальцев, форма ладони, узор радужной оболочки, изображение сетчатки глаза. Лицо, голос и запах каждого человека также индивидуальны.

Распознавание человека по изображению лица выделяется среди биометрических систем тем, что, во-первых, не требует специального дорогостоящего оборудования. Для большинства приложений достаточно персонального компьютера и обычной видеокамеры. Во-вторых,

отсутствует физический контакт человека с устройствами. Не надо ни к чему прикасаться или специально останавливаться и ждать срабатывания системы. В большинстве случаев достаточно просто пройти мимо или задержаться перед камерой на несколько секунд.

К недостаткам распознавания человека по изображению лица следует отнести то, что сама по себе такая система не обеспечивает 100% надёжности идентификации. Там, где требуется высокая надёжность, применяют комбинирование нескольких биометрических методов.

На данный момент проблеме распознавания человека по изображению лица посвящено множество работ, однако в целом она ещё далека от разрешения. Основные трудности состоят в том, чтобы распознать человека по изображению лица независимо от изменения ракурса и условий освещённости при съёмке, а также при различных изменениях, связанных с возрастом, причёской и т.д.

ЛИТЕРАТУРА

1. *Волченков М.П.* Об автоматическом распознавании лиц [Электронный ресурс] / М.П. Волченков, И.Ю. Самоненко. Электрон. дан. Систем. требования: Acrobat Reader 5.0. Режим доступа: http://intsys.msu.ru/magazine/archive/v9(1-4)/volchenkov-135-156.pdf, свободный. Загл. с экрана.

СИСТЕМА ШИФРОВАНИЯ НА ОСНОВЕ НЕКОММУТАТИВНЫХ АЛГЕБР КЛИФФОРДА

А.С. Петухов, А.С. Шувалов, аспиранты МарГТУ,
А.Н. Леухин, д.ф.-м.н., и.о. зав. каф. ИБ МарГТУ

В работе рассмотрен новый подход в области криптографической защиты информации, основанный на использовании некоммутативных конечных групп, индуцированных алгеброй Клиффорда. Метод позволяет при меньших значениях ключа достигать большей криптостойкости шифруемого сообщения. Алгеброй Клиффорда в алгоритме задаются правила генерирования элементов группы, а также выполнения групповой операции умножения. Требуемая криптостойкость достигается благодаря сложности подбора правильных значений секретного ключа X, используемого в операции шифрования $X \circ M^e \circ X^{-1}$ при соответствующем выборе группы Г и ее элементов X и M, а использование ключа меньшей длины в некоторой степени достигается благодаря нелинейному увеличению мощности группы Г.

В настоящее время в области информационных технологий нашли широкое распространение системы криптографической зашиты ин-

формации, системы электронно-цифровых подписей (ЭЦП) и другие системы, предназначенные для качественного и безопасного владения информации и ее использования. Все эти системы реализуются по тем или иным алгоритмам. Так, например, известны и широко применяются алгоритмы симметричного шифрования: AES, DES, IDEA, ГОСТ 28147-89; шифрования с открытым ключом: RSA, DSA, DSS; а также алгоритмы ЭЦП, такие как схема Эль-Гамаля, RSA-PPS, DSA, ECDSA. С ростом вычислительных мощностей подобные алгоритмы должны оперировать все большими значениями и постоянно увеличивать длину используемого ключа, а подбор подходящих значений злоумышленником становится вопросом времени и использующейся вычислительной мощности. Особенно остро данная проблема возникает в последние несколько лет. Вследствие этого становится возможным поиск новых решений, иных подходов в данной области.

Предлагается существенно новый подход в области криптографии, основанный на использовании некоммутативных конечных групп и свойствах алгебры Клиффорда. Использование некоммутативных групп позволяет усилить криптостойкость разрабатываемого алгоритма, а также использовать ключи шифрования значительно меньших размеров без снижения эффективности защиты информации. Подбор подходящих значений ключа злоумышленником методом перебора всех возможных значений исключается либо существенно затрудняется, поскольку вместо использования простых целочисленных решений, в отличие от существующих распространенных аналогов алгоритмов, для реализации криптосистемы применяются элементы конечных групп. Данный метод был рассмотрен Н.А. Молдовяном в работе [1], где описывается общий метод построения алгоритмов шифрования и алгоритмов цифровой подписи с использованием конечных некоммутативных групп.

Отметим некоторые общие положения, касающиеся данного подхода. Как известно, некоммутативные группы образуются из элементов, обладающих свойствами ассоциативности, при условии, что для каждого элемента группы имеется обратный элемент, умножение на который дает нейтральный элемент группы и, главное, выполняется свойство некоммутативности, т.е. $X \circ Y \neq Y \circ X$, где «$\circ$» – знак групповой операции.

Всеми указанными свойствами обладают элементы алгебры Клиффорда, например общеизвестные кватернионы вида $q = e_0 + ie_1 + je_2 + ke_3$, с умножением в качестве групповой операции. Кватернионы будут рассматриваться в качестве примера реализации метода шифрования, но вместо них могут использоваться любые дру-

гие элементы из этой алгебры. Алгебра Клиффорда позволяет задавать в качестве элементов группы гиперкомлексные числа любых размерностей, равных степеням с основанием 2 (т.е. размерности 4, 8, 16, 32, и т.д.), путем формирования правила выполнения умножения гиперкомплексных чисел. Очевидно, что для каждой новой размерности элемента группы правило выполнения групповой операции будет отличаться от всех предыдущих и будет уникальным. Данный факт позволяет также усложнить подбор ключей злоумышленником за счет увеличения мощности группы и, следовательно, возможных вариантов ключей.

Рассмотрим общий метод построения алгоритма шифрования. Он заключается в применении некоммутативных конечных групп, построенных по правилам алгебры Клиффорда и имеющих элементы, значения которых не превышают некоторого простого многоразрядного числа p. В общем виде алгоритм шифрования частично похож на алгоритм RSA, но выполняя все действия в рамках некоммутативных групп:

1) выбирают модуль выполнения операций в виде простого числа p;

2) формируют секретный ключ шифрования в виде экспоненты e и элемента X группы Г;

3) формируют исходное сообщение M;

4) возводят сообщение M в степень e, дополнительно выполнив групповые операции с частью секретного ключа в виде элемента X и обратного ему элемента X^{-1}, результатом данных действий будет промежуточный шифротекст Y;

5) формируют конечный шифротекст C на основе секретного ключа.

Благодаря свойствам некоммутативности в общем случае результат выполнения групповой операции зависит от порядка расположения элементов группы, над которыми выполняется групповая операция. Вследствие этого уравнения вида $Y = X \circ M^e \circ X^{-1}$ с неизвестным значением X являются трудно решаемыми при соответствующем выборе группы Г и ее элементов X и M, что является решающим фактором в пользу криптостойкости алгоритма. Это позволяет использовать значение X в качестве секретного ключа шифрования и выполнять само шифрование, предварительно формируя сообщение в виде элемента M группы Г по формуле $Y = X \circ M^e \circ X^{-1}$, где e – многоразрядное число. Для получения шифротекста C с целью увеличения криптостойкости получаемого шифра применяется y-кратное выполнение аналогичной групповой операции, в которой на каждом i шаге вместо значений X и

X^1 принимаются элементы X^i и X^{-i} группы Г, а в качестве элемента M группы Г принимается результат предыдущего шага, т.е.

$$Y_y = X^{y-1} \circ Y_{y-1}^e \circ X^{-y-1}.$$

На начальном этапе реализации метода следует сгенерировать 2 некоммутативные конечные подгруппы: Γ_1 для выбора из нее элемента секретного ключа X и Γ_2 для формирования на основе ее элементов исходного сообщения M. Данные подгруппы формируются по одному из правил алгебры Клиффорда с условием, что порядок подгрупп будет максимально возможным для выбранного способа построения, а значения элементов не превосходят выбранного многоразрядного простого числа p. Для генерации элемента секретного ключа X следует выбрать любой элемент подгруппы Γ_1, не являющийся единичным элементом группы. Также генерируются дополнительные ключи шифрования в виде многоразрядных чисел e и y. При такой реализации заявленного способа шифрования формула шифрования примет вид

$$C = X^y \circ Y_y^e \circ X^{-y},$$

где $Y_y = X^{y-1} \circ Y_{y-1}^e \circ X^{-y-1}$,..., а $Y_1 = X \circ M^e \circ X^{-1}$.

Формула расшифровки сообщения в этом случае примет вид

$$M = X^{-1} \circ Y_1^d \circ X,$$

где $Y_1 = X^{-2} \circ Y_2^d \circ X^2$,..., а $Y_y = X^{-y} \circ C^d \circ X^y$, d – дополнительный секретный ключ дешифрования, который легко вычисляется из дополнительного секретного ключа шифрования как МДМ, обратное e по модулю, равному максимальному значению p порядка элементов группы.

Как уже говорилось, правило задания конечной некоммутативной группы основывается на выполнении групповой операции по правилам алгебры Клиффорда. Это позволяет конкретизировать генерацию конечной группы и, более того, увеличить мощность шифрования, поскольку с каждым новым выбранным правилом выполнения групповой операции меняется порядок элементов конечной группы. Так, например, для известного множества векторов алгебры Клиффорда, названных кватернионами, правило выполнения групповой операции над векторами вида $(1, ie_1, je_2, ke_3)$ при построении таблицы умножения базисных векторов имеет диагональ вида (1, –1, –1, –1), другими словами, $e_1^2 = e_2^2 = e_3^2 = -1$. Ниже приведены некоторые примеры таблиц умножения базисных векторов (табл. 1, 2).

Аналогичным способом задается любое правило выполнения групповых операций. Также правила алгебры Клиффорда позволяют

генерировать конечные некоммутативные группы с n-мерными элементами. Так, известными примерами реализации правил n-мерной алгебры Клиффорда являются 4-мерные кватернионы, 8-мерные элементы, 16-мерные седенионы и т.д. Следовательно, само правило задания формирования группы также может быть дополнительным параметром шифрования и войти в состав закрытого ключа.

Таблица 1

Таблица умножения базисных векторов с диагональю (1, –1, –1, –1)

·	**1**	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$
1	1	e_1	e_2	e_3
$\mathbf{e_1}$	e_1	–1	$e_1 \circ e_2$	$e_1 \circ e_3$
$\mathbf{e_2}$	e_2	$-e_1 \circ e_2$	–1	$e_2 \circ e_3$
$\mathbf{e_3}$	e_3	$-e_1 \circ e_3$	$-e_2 \circ e_3$	–1

Таблица 2

Таблица умножения базисных векторов с диагональю (1, –1, –1, –1)

·	**1**	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$
1	1	e_1	e_2	e_3
$\mathbf{e_1}$	e_1	1	$e_1 \circ e_2$	$e_1 \circ e_3$
$\mathbf{e_2}$	e_2	$-e_1 \circ e_2$	1	$e_2 \circ e_3$
$\mathbf{e_3}$	e_3	$-e_1 \circ e_3$	$-e_2 \circ e_3$	1

Рассмотрим пример реализации заявленного способа шифрования.

Пример.

Реализация способа шифрования сообщения с последующей его расшифровкой. Для формирования группы используется наиболее распространенное правило умножения элементов алгебры Клиффорда, формирующее множество кватернионов.

1. Генерируют простое число $p = 67$.

2. Генерируют две подгруппы Γ_1 и Γ_2.

3. Генерируют элемент секретного ключа X из подгруппы Γ_1, а также дополнительные ключи шифрования – произвольное простое число e и произвольное число y. Также из группы M_2 выберем произвольный элемент M в качестве исходного сообщения.

$X = (13, 40, 29, 54)$, $e = 13$, $y = 7$.

4. Формируют исходное сообщение в виде элемента M подгруппы Γ_2.

$M = (40, 13, 57, 59)$.

5. Генерируют криптограмму C

$$Y_1 = X \bullet M^{13} \bullet X^{-1} = (37 \quad 1 \quad 40 \quad 19),$$

$$Y_2 = X^2 \bullet Y_1^{13} \bullet X^{-2} = (12 \quad 27 \quad 22 \quad 57),$$

$$\ldots$$

$$C = Y_7 = X^7 \bullet Y_6^{13} \bullet X^{-7} = (60 \quad 3 \quad 11 \quad 24).$$

В результате указанных выше действий получают криптограмму C. Для вычисления исходного сообщения M из шифра C найдем дополнительный секретный ключ расшифровывания $d = 1381$, который вычисляется из дополнительного секретного ключа шифрования как

МДМ, обратное e по модулю, равному максимальному значению p порядка элементов группы.

$$Y_6 = X^{-7} \bullet Y_7^{1381} \bullet X^7 = (11 \quad 51 \quad 40 \quad 54),$$
$$Y_5 = X^{-6} \bullet Y_6^{1381} \bullet X^6 = (17 \quad 53 \quad 51 \quad 43),$$
$$\cdots$$
$$M = Y_0 = X^{-1} \bullet Y_1^{1381} \bullet X = (40 \quad 13 \quad 57 \quad 59).$$

Сравнение вычисленного сообщения с исходным сообщением показывает, что криптограмма C расшифрована правильно, т.е. из нее получено исходное сообщение M.

Выводы

В данной работе рассмотрен новый подход в области криптографической защиты информации, позволяющий при меньших значениях ключа достигать большей криптостойкости шифруемого сообщения. Метод достигается путем использования некоммутативных конечных групп, основанных на свойствах алгебры Клиффорда. Алгеброй Клиффорда в данном алгоритме задаются правила генерирования элементов группы, а правило выполнения групповой операции умножения. Требуемая криптостойкость достигается путем выполнения операции $X \circ M^e \circ X^{-1}$ с неизвестным значением X при соответствующем выборе группы Г и ее элементов X и M, а использование ключа меньшей длины в некоторой степени достигается благодаря нелинейному увеличению мощности группы Г.

Работа выполнена при финансовой поддержке по темам НИР в рамках гранта Президента РФ МД-5418.2010.9, ГК №П783 и гранта РФФИ 09-07-000723-а.

ЛИТЕРАТУРА

1. *Молдовян Н.А.* Теоретический минимум и алгоритмы цифровой подписи. СПб.: СПб.: БХВ-Петербург, 2010. 304 с.

2. *Browne J.M.* Grassmann Algebra – Exploring applications of extended vector algebra with Mathematica, 2007.

АНАЛИЗ ВРЕДОНОСНЫХ ОБЪЕКТОВ МЕТОДОМ ДЕКОМПИЛЯЦИИ БИНАРНОГО КОДА

М.О. Шудрак, студент 5-го курса, каф. БИТ

Научный руководитель И.А. Лубкин, ст. преподаватель каф. БИТ, к.т.н.

г. Красноярск, СибГоАУ им. М.Ф. Решетнева, slender.bit@mail.ru

На сегодняшний момент, существует и развивается широкий спектр методов обнаружения и анализа вредоносного кода, но наряду с

этим развитием совершенствуются методы защиты от исследования и детектирования вирусной активности. Чаще всего вирусописатели для реализации защиты от исследования своих разработок применяют технологии полиморфизма, обфускации (запутывающие преобразования) и шифрования бинарного кода.

Цель данной работы состоит в повышении эффективности анализа запутывающих преобразований в бинарном коде вредоносных объектов.

Актуальность рассматриваемой тематики

Наиболее эффективным средством обнаружения полиморфных вирусов является эвристический анализ программного кода, который нередко используется совместно с сигнатурным сканированием для поиска сложных полиморфных вирусов. Также для обнаружения полиморфных вирусов, как правило, используются специально разрабатываемые для каждого вируса алгоритмы обнаружения. Несмотря на высокую эффективность эвристического анализа, такой метод позволяет обнаруживать вредоносные программы с определённой долей вероятности, так как наряду с полиморфной генерацией кода, вирусописатели прибегают и к другим методам защиты (антиотладка и антиэвристика) [2].

Новизна данной работы заключается в подходе, используемом для анализа вредоносных объектов. Для этого используется метод анализа бинарного кода вредоносного объекта путём восстановления его алгоритма, а не его исходного кода.

Описание разработанной методики

Рассмотрим предлагаемую методику анализа запутывающих преобразований на следующем тривиальном примере:

```
(1) mov eax, offset dword_40FCC2
(2) mov edx, offset dword_40FCC2+4
(3) mov ebx,eax
(4) mul ebx
(5) sub eax,1
(6) cmp eax,edx
(7) je  condition_1
(8) jmp condition_2
```

Листинг 1. Тривиальный пример хеширования ключа.

Программный код в листинге 1 выполняет хеширование ключа на основе алгоритма, который можно представить в виде функции $y = x^2 - 1$. Теперь применим к программному коду в листинге 1 простейший полиморфный генератор.

```
(1)  mov eax,offset dword_40FCC2
(2)  mov edx,offset dword_40FCC2+4
(3)  mov ecx,0
(4)  sub ecx,72h
(5)  shl edx,eax
(6)  cmp edx,ecx
(7)  sub eax,1
(8)  add ebx,1
(9)  mul ebx
(10) cmp eax,edx
(11) je condition_1
(12) jmp condition_2
```

Листинг 2. Тривиальный пример хеширования ключа с использованием полиморфного генератора.

Таким образом, алгоритм программного кода не изменился, поменялось лишь его представление в машинном коде ($y = (x - 1)(x + 1)$).

Соответствующий уровень абстракции для анализа вредоносного объекта может быть получен путём декомпиляции программного кода. Рассмотрим алгоритм работы декомпилятора подробно на рис. 1.

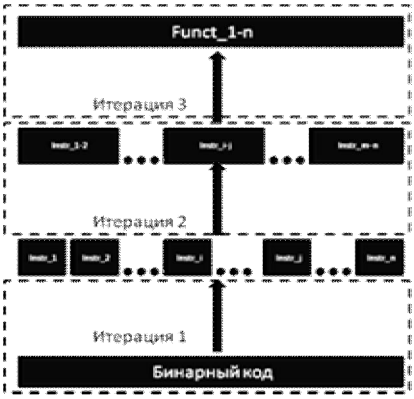


Рис. 1. Алгоритм работы декомпилятора

Итерация 1: Дизассемблирование.

На данном этапе происходит дизассемблирование полученного бинарного кода.

Итерация 2: Интерпретация инструкций.

На данном этапе происходит процесс преобразования одной процессорной инструкции в промежуточный код, описывающий функциональные связи между операндами инструкций и их результатом.

Итерация 3: Анализ.

Данная итерация является заключительным этапом анализа программного кода, в результате которой промежуточный код интерпретируется в связную структуру.

Первый, второй и третий этапы выполняются циклично для каждого участка машинного кода, что позволяет полностью проанализировать программный код вредоносного объекта.

Выводы

Таким образом, результаты данной работы позволяют:

а) оптимизировать детектирование и анализ вредоносных объектов;

б) разработанная методика позволяет не только анализировать программный код вируса, но и предоставляет возможность выделения кода вируса, не несущего определённый функционал.

ЛИТЕРАТУРА

1. http://www.tadviser.ru Статья о полиморфизме компьютерных вирусов.
2. *Собейкис В.* Компьютерная вирусология. М.: Майор, 2006. 512 с.

БИОМЕТРИЧЕСКАЯ СИСТЕМА ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО ГЛАЗНОЙ РАДУЖНОЙ ОБОЛОЧКЕ

А.В. Харитонов, Е.Н. Потехин, студенты 5-го курса МарГТУ,
А.Н. Леухин, д.ф.-м.н., и.о. зав. каф. ИБ МарГТУ

В работе рассмотрены известные алгоритмы распознавания радужной оболочки глаза, а также предложен метод, основанный на контурном анализе изображений. Данный подход позволяет сократить затраты на оборудование и обеспечить достаточный уровень надёжности.

Один из механизмов обеспечения информационной безопасности – аутентификация личности. Для этих целей всё чаще используются биометрические технологии. В качестве отличительного, характерного лишь для одного человека признака используют отпечатки пальцев, форму лица, сетчатку и радужную оболочку глаза, ДНК (самый надёжный и наиболее дорогой метод). При распознавании выделяются параметры объекта, уникальные в классе ему подобных. Они должны быть инварианты относительно условий регистрации и изменчивости самого объекта.

Устойчивым, высокоинформативным и выраженным биометрическим признаком является радужная оболочка глаза, благодаря тому, что имеет сложный рисунок и состоит из множества деталей. Рисунок радужки в большой степени случаен, а чем больше степень случайности, тем больше вероятность того, что конкретный рисунок будет уникальным. Математически данная случайность описывается степенью свободы. Исследования показали, что текстура радужки имеет степень свободы, равную 250, что гораздо больше степени свободы отпечатков пальцев (для сравнения – 35) и изображений лиц (20). Данные показатели наряду с практически неизменной структурой узора радужной оболочки глаза делают её надёжным и простым механизмом идентификации личности.

Методы идентификации личности по радужной оболочке основаны на следующем принципе – выделение частотной или какой-либо

другой информации о текстуре радужки из изображения и сохранение этой информации в виде специального кода. Построение кода производится в три этапа:

1. Выделение из общего изображения радужной оболочки глаза.

2. Предобработка полученного изображения. Для извлечения параметров рисунка радужной оболочки глаза необходимо отсеять вариации самой радужки: убрать шум, незначащие детали, блики внутри зрачка от вспышки либо другого яркого источника света.

3. Составление кода.

После проделанных процедур предобработки изображение фильтруется способом, который зависит от конкретного метода. По результатам фильтрации составляется представление в виде кода. Далее выполняется сравнение зафиксированных параметров с эталонами. И на заключительном этапе система решает: совпадают ли биометрические образцы.

Большинство методов работает с изображениями в градациях серого либо с картами яркости изображений, то есть цветовая составляющая является избыточной.

Рассмотрим эти процессы более подробно.

Для локализации радужной оболочки некоторые методы используют специальное оборудование для захвата изображения, мера направлена на получение высокого разрешения с хорошей контрастностью, освещением (при этом человек, которого снимают, не должен чувствовать дискомфорта от слишком яркой вспышки). Кроме того, система камер не должна принуждать человека сесть в определенную позу на фиксированном расстоянии от камеры при специальном освещении. Для этого предлагается специальная система камер.

Иногда, кроме снимка в видимом диапазоне, делается дополнительный снимок инфракрасной камерой.

Для того чтобы отделить собственно радужку от остальных деталей на изображении, в простейшем случае можно использовать выделение краёв (путём анализа первой производной) и последующую аппроксимацию границ радужки простыми геометрическими объектами. Так, окружность зрачка и внешнюю границу радужки можно найти при помощи преобразования Хафа. Другие методы дополнительно определяют границу радужки и век двумя параболами либо просто отрезают те части изображения, которые могут не относиться к радужке.

Если для захвата изображения не было использовано специальной аппаратуры, может понадобиться предварительное подавление нежелательных эффектов, таких как блик внутри зрачка от вспышки либо другого яркого источника света, если эти артефакты мешают корректной работе алгоритма выделения радужки.

Нормализация изображения.

Часто для дальнейшей работы производится перевод изображения радужки из полярных координат в декартовы. Однако есть методы, не требующие такого перевода.

После такого приведения к полученному изображению можно применить гауссов фильтр или медианную фильтрацию для устранения высокочастотного шума. После этого изображение все ещё слабоконтрастно, и для повышения надёжности производят выравнивание гистограммы.

Часто, помимо этого, производится отбрасывание малозначащих частей изображения – это могут быть верхняя и нижняя строки (по несколько пикселей) изображения после его перевода в декартовы координаты или устранение бликующих областей, портящих рисунок радужки.

После проведенной предобработки изображение радужки готово к тому, чтобы из него можно было извлечь более формальную информацию.

К классическим способам составления кода можно отнести пространственно-частотную свертку изображения фильтрами Габора. Каждый бит кода определяется знаком результата воздействия двухмерного фильтра Габора на некоторую небольшую окрестность текстуры радужки. Для кода Daugman и подобных ему в качестве сравнения используется расстояние Хэмминга (количество отличающихся бит кода). Развитием этого направления является применение специальных симметричных функций Circular symmetric filter.

Другой модификацией кода на основе фильтров Габора является составление кода на основе среднего абсолютного отклонения (average absolute deviation, AAD) отфильтрованного изображения от оригинального. В этом случае функцией сравнения будет выступать евклидово расстояние между векторами.

Wildes использует декомпозицию изображения на основе Laplacian of Gaussian filters. Результирующее изображение представляется как лапласова (многомасштабная) пирамида изображений, подвергнутых действию гауссовых фильтров, и призвано представлять пространственные характеристики радужки. В этом случае для дальнейшего сравнения используется нормированная корреляция обрабатываемого изображения и изображений из базы данных. Нормализованная корреляция показывает меру соответствия точек двух изображений или областей изображений друг другу.

В современных системах для распознавания применяются статистические методы, нейронные сети, используются градиентные или спектральные признаки.

Методы во многом ориентированы на уменьшение размерности исходных данных. Сокращение пространства признаков улучшает кластеризацию образов (отделение друг от друга). Распознавание в сокращенном пространстве признаков позволяет значительно уменьшить размер эталона, оставляя только те признаки, которые имеют принципиальное значение для конкретного образа. Распространенный метод понижения размерности – это анализ главных компонент. Суть метода анализа главных компонент заключается в получении максимально декоррелированных коэффициентов, характеризующих входные образы. Метод анализа главных компонент выделяет из многомерных исходных данных совсем небольшое число компонент, сохраняя при этом структуру информации.

Приведём примеры некоторых систем распознавания.

John Daugman

Система была спроектирована им в 1992 г. Основа для составления кода – фильтры Габора, критерий сравнения кодов – расстояние Хэмминга. Код представляется в виде двоичной переменной 512 байт (4096 бит), имеющей запатентованное название IrisCode. Это наиболее ранняя и, по-видимому, наиболее развитая система, имеются коммерческие разработки.

Richard Wildes

Предложил систему в 1996 г. Использует преобразование Хафа для локализации радужки, лапласову пирамиду фильтров Гаусса (мультимасштаная декомпозиция) для составления кода, в качестве критерия сравнения берётся нормализованная корелляция. Для захвата изображения используется специальное оборудование.

В 1998 г. был предложен метод составления кода, основанный на вейвлет-преобразованиях (W. Boles). Изображение радужки представляется одномерной функцией, которая фильтруется вейвлетами специального вида. Код составляется с помощью точек, в которых результирующее представление обнуляется.

Seung-In Noh

Коммерческая разработка. В основе лежит использование анализа независимых компонент с переменной разрешающей способностью (Multiresolution Independent Component Analysis).

Кратко перечислим основные проблемы, стоящие перед разработчиком систем распознавания по радужке, и способы их решения.

1. Затенение радужки веками. Эта проблема может решаться специальным алгоритмом поиска век или отбраковкой частей изображения при сравнении последовательных кадров.

2. Затенение радужки ресницами.

3. Блики от окружающих предметов на роговице. Роговица работает как сферическое зеркало, отражая окружающий мир. Эти отражения могут быть в несколько раз ярче деталей радужки и полностью подавлять их. Для решения этой проблемы применяют высокоинтенсивное в узкой области спектра освещение (значительно превосходящее солнечное по освещенности, лучше всего использовать ближний ИК, не видимый и не раздражающий человека) и регистрация изображения в этой же области спектра.

4. Различный размер зрачка при изменяющихся условиях съемки. Аффинное преобразование изображения радужки к стандартному размеру решает эту проблему лишь в первом приближении, так как растяжение радужки подчиняется нелинейному, весьма сложному закону. Для решения этой проблемы предлагается, например, запоминать размер зрачков человека при регистрации в системе, а при распознавании добиваться аккомодации зрачков до этого размера, манипулируя яркостью специального источника видимого света.

5. Патологические и возрастные изменения. На радужке весьма отчётливо отражается состояние организма, в том числе разного рода патологии (болезни, травмы, отравления). В связи с этим возникает вопрос об устойчивости (по времени) распознавания объекта, подверженного этим изменениям. Однако на радужке существует значительное число врожденных и не изменяющихся в течение всей жизни признаков. Врожденные и приобретенные признаки разделить практически невозможно, но человека можно распознавать на основании совпадения даже незначительной доли признаков.

6. Неопределенность угла поворота радужки. В системе с регистрацией двух радужек или в системе, комбинирующей радужку и лицо, эта проблема не существует. Для «одноглазой» системы можно определять угол по конфигурации век, децентрации зрачка или по какому-либо выдающемуся характерному признаку на радужке. Однако все эти признаки изменяются со временем. В таком случае остаётся перебирать углы поворота (существенно увеличивается время) или вычислять признаки, инвариантные к повороту (таких признаков в десятки раз меньше, следовательно, сильно снижается надежность).

Контурный анализ радужной оболочки глаза позволяет выделить на изображении радужки характерные признаковые структуры, по которым будет проходить дальнейшее распознавание. Первоначально необходимо выделить интересующую область, то есть радужку от внутреннего края до внешнего. Затем сформировать контуры, выполнить их нормирование и занести в базу.

Весь процесс формирования контуров радужной оболочки глаза состоит из нескольких частей. На первом этапе применяется оператор

Собеля, позволяющий выделить границы. Результатом применения оператора в каждой точке изображения является либо вектор градиента яркости в этой точке, либо его норма. Оператор Собеля основан на свёртке изображения небольшими сепарабельными целочисленными фильтрами в вертикальном и горизонтальном направлениях.

После этого изображение подаётся на детектор Canny, что позволяет получить оптимальное обнаружение краёв интересующих областей. Метод Canny обладает двумя важными свойствами: низкий уровень ошибок и хорошая локализованность краевых точек – это позволяет сохранить максимальное число признаков радужной оболочки глаза.

Для формирования контура используется алгоритм Розенфельда, который состоит из нескольких шагов. На первом шаге необходимо просканировать сцену с целью отыскания верхнего левого граничного пикселя. На втором шаге необходимо проследить линию контура согласно граничным точкам. На третьем шаге нужно сформировать код, которым будет описываться контур. В качестве такого кода используется код Фримена.

Задача распознавания сводится к определению двух наборов контуров, принадлежащих разным объектам, максимально схожих друг с другом. Метод инвариантен к углу поворота радужной оболочки глаза, а также к размеру зрачка, что снимает ряд связанных с распознаванием проблем.

Выводы

В данной работе приведён обзор методов распознавания личности на основе радужной оболочки глаза человека. Затронуты основные специфические моменты, а также ряд проблем, связанных с обработкой радужной оболочки.

В целом алгоритмы распознавания по радужке при наличии изображения хорошего качества способны дать исключительно высокую надежность распознавания (EER ~ 10^{-6}).

Основное препятствие практической реализации заключается в трудности получения таких изображений, что приводит к высоким требованиям на условия регистрации.

Предложенный в статье метод контурного анализа позволяет существенно снизить издержки на оборудование и обеспечить приемлемый уровень верного распознавания личности по его радужной оболочке.

Работа выполнена при финансовой поддержке по темам НИР в рамках гранта Президента РФ МД-5418.2010.9, ГК №П783 и гранта РИ 09-07-000723-а.

ЛИТЕРАТУРА

1. *Li Ma, Yunhong Wang, Tieniu Tan.* Iris Recognition Using Circular Symmetric Filters // Proceedings of the 16 th International Conference on Pattern Recognition (ICPR'02). P. 20414–20418.

2. *Christel-loic Tisse, Lionel Martin, Lionel Torres, Michel Robert.* Person identification technique using human iris recognition // Proc. of Vision Interface, 2002. P. 294–299.

3. *Li Ma, Yunhong Wang, Tieniu Tan.* Iris Recognition Based on Multichannel Gabor Filtering // ACCV2002: The 5th Asian Conference on Computer Vision.2002. January. Melbourne, Australia. P. 23–25.

4. *Фурман Я.А., Кревецкий А.В., Передреев А.К. и др.* Введение в контурный анализ; приложения к обработке изображений и сигналов. М.: Физматлит, 2003. 588 с.

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ КОДЕ

Е.А. Даньшин, студент 5-го курса

Научный руководитель Е.М. Давыдова, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, ugin.dan@gmail.com

Согласно статистике на 1000 строк исходного кода приходится примерно от 20 до 50 ошибок, которые, как правило, носят непреднамеренный характер: недостатки проектирования, разработки, программирования и в большей степени тестирования, а также недостатки используемого языка программирования, создавая основную категорию уязвимостей программного обеспечения – ошибки разработки и тестирования. Наибольшую опасность представляют недекларированные возможности программного обеспечения. К этой категории уязвимостей относятся, например, инженерные «бэкдоры», которые позволяют обходить процедуры контроля целостности и/или аутентификации.

Анализ и выявление уязвимостей программного кода может быть основным или добавочным методом тестирования программного обеспечения, называемым тестированием безопасности. Наиболее распространено применение анализаторов программного кода для выявления уязвимостей и недекларированных возможностей ПО. Основными способами анализа являются статистический и динамический анализ исходного кода, а также контроль целостности всего исходного кода.

Стоит отметить, что наибольшую опасность представляют уязвимости, заложенные (чаще допущенные из-за невнимательности разработчиков) в приложении на самых ранних этапах его жизненного цикла (на этапе разработки), а именно уязвимые сигнатуры в исходных текстах тестируемого программного обеспечения. На практике боль-

шая часть программного обеспечения на рынке информационных технологий проходит лишь этапы внутреннего тестирования (альфа-тестирование), основной целью которого является выявление ошибок в разработанном ПО. При этом о тестировании безопасности программного обеспечения чаще всего не задумываются. Основная проблема заключается в том, что пока нет никакого российского стандарта или руководящего документа, в котором описывался бы процесс тестирования по требованиям безопасности. В РД НДВ [1] приводятся только основные положения и требования к уровням контроля при проведении испытаний на отсутствие недекларированных возможностей в программных изделиях.

Реализация и проведение анализа, как статистического, так и динамического, в основном основываются на накоплении базы данных уязвимостей и недостатков языков программирования как процессе сопоставления строк исходного кода значениям базы данных (подклассы: поиска по сигнатурам и эвристического анализа уязвимостей), а так же более долгом и трудоемком способе – экспертном анализе (ручном анализе).

Проверка кода «вручную» должна считаться вспомогательным решением, а не лучшим подходом к поиску уязвимых мест кода или заменой других подходов. Проверка кода также не должна рассматриваться в качестве замены моделирования угроз, фаззинга или соблюдения рекомендаций по программированию. По сравнению с другими подходами проверка кода обычно более дорогостояща, поэтому должна использоваться преимущественно для наиболее важных областей и проблем, где эффективность других подходов ограничена.

Проверка программного кода наиболее успешна при планировании и выполнении в контексте других относящихся к безопасности процессов, например, моделировании уязвимости программ (рис. 1). Кроме того, результаты проверки кода могут иметь дополнительную ценность, способствуя выполнению других связанных с безопасностью задач, таких как тестирование и проектирование.

Основным способом анализа уязвимости программного обеспечения является проведение пошаговой проверки исходного кода (трассировки) для каждого теста как по безопасности, так и по функционалу. Более лучший результат могли бы дать применение совместно с трассировкой анализа по «структуре» как всей программы, так и отдельных ее частей (процедур, функций, классов и подклассов), а также накопление базы данных уязвимостей «структур», так как возможна ситуация, что в исходном коде программы не будет обнаружено ошибок, но целиком программа работает некорректно.

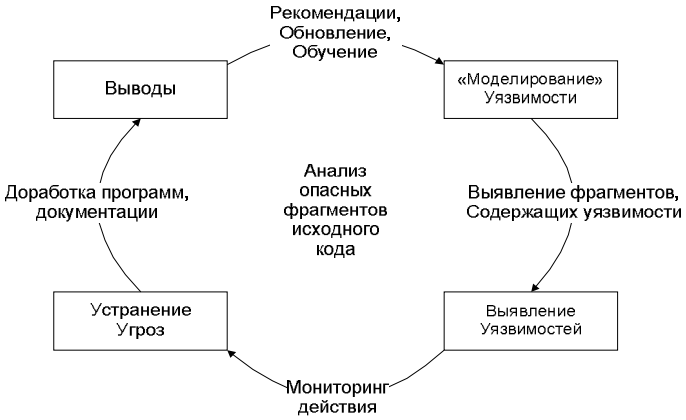


Рис. 1. Контекст процессов безопасности программного кода

Также способом улучшения безопасности программного обеспечение может быть следование требованиям ГОСТ Р ИСО/МЭК 15408 «Информационные технологии. Методы и средства обеспечения безопасности», так как этот стандарт в значительной степени дополняет требования Руководящего документа «Защита от несанкционированного доступа к информации. Ч. 1», согласно которому возможна разработка требований и заданий по безопасности программного обеспечения как превентивный способ защиты программного обеспечения на этапе разработки.

ЛИТЕРАТУРА

1. *Руководящий* документ. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. М.: Гостехкомиссия России, 1998.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, каф. КИБЭВС, sma@keva.tusur.ru

Вопросы защиты персональной информации в России поднимались только после громких судебных или общественных разбирательств, повлекших некоторый общественный резонанс у населения. Вследствие такого отношения к личной информации трудно говорить об адекватных мерах, применяемых для защиты этих данных.

До ратификации Европейской конвенции и принятия Закона «О персональных данных» [1, 2] в российском законодательстве не было документа, который бы тем или иным образом регламентировал действия организаций, направленных на работу с подобной информацией. В разных документах в той или иной степени упоминалось о необходимости получать согласие на оглашение или обработку личной информации в пределах компетенции организации. Примерами таких нормативно-правовых актов могут служить непосредственно Конституция РФ, которая устанавливает нормы личной и семейной тайны, ФЗ «О средствах массовой информации», в котором говорится, что «…журналист обязан получать согласие на распространение в СМИ сведения о личной жизни гражданина от самого гражданина или его законных представителей…» и т.д. [3].

Некоторая упорядоченность действий при работе операторов по обработке персональных данных (ПДн) появилась с принятием профильного закона, но изначальная закрытость документов органов-регуляторов оставила непонимание основных мероприятий, которые должны обеспечить безопасность личной информации. Следствием такого отношения вышеупомянутых органов стала негативная реакция у операторов к необходимости защиты ПДн. Негативное отношение операторов, нестрогое описание необходимых и достаточных действий для приведения информационных систем обработки ПДн (ИСПДн) к нормам законодательства, непонимание как самих операторов, так и организаций-профессионалов в области информационной безопасности привели к срывам сроков, обозначенных законодательством.

Анализ нормативных документов и практика их применения показали, что прямое использование установленных регламентов невозможно для многих сфер деятельности. Этот факт доказывает появление соответствующих приказов, распоряжений, писем и других нормативно-распорядительных документов у большего числа министерств и ведомств Российской Федерации. Наибольшую активность в данном вопросе проявило Министерство здравоохранения и социального развития. Результатом деятельности Минздравсоцразвития стал не единичный документ, а полный пакет документов, основой которого стали все документы, разработанные ФСТЭК, ФСБ и Роскомнадзором, адаптированный к отрасли.

Если рассматривать ПДн, которые обрабатываются в информационных системах здравоохранения, то вопроса, к какой категории их отнести, не возникает. Сфера высшего образования представлена информационными системами разных классов. Так, сбор, обработка и хранение предполагают наличие данных от общедоступных (фамилия, имя, отчество, дата рождения и т.д.) до специальных категорий (на-

циональность, медицинские данные и т.д.). С учетом размеров университетов (количества сотрудников, студентов), специфики деятельности и сложности процессов образования несложно предположить, что регламентные работы по защите персональных данных в вузе будут сложно структурированы и трудозатратны относительно времени, материальных затрат и человеческих ресурсов.

Обозначенные ограничения оказывают серьезное влияние на процесс защиты ПДн в вузе. Временные ограничения можно разделить на две составляющие:

1. Официальное время, установленное законодательством для приведения существующих ИСПДн к нормам. На данный момент установленная дата 01.07.2011.

2. Реальное время осуществления необходимых действий для выполнения норм, установленных законодательством.

Специалисты, занимающиеся обеспечением защиты ПДн, могут оказывать влияние только на реальное время, официальное время определяется законодательными структурами и организациями-регуляторами. На управление реальным временем оказывают влияние следующие факторы. Во-первых, четкое изложение методики проведения работ, методика должна быть адаптирована к определенной области функционирования. Если такой адаптации не существует, то процесс затягивается во времени, т.к. специалистам приходится обобщенную методику приводить к реалиям данной сферы. Во-вторых, автоматизация как всего процесса в целом, так и его частей, позволяющая сокращать время осуществления анализа и обработки данных, а также оказания помощи в принятии решений. В-третьих, квалификация персонала, которая также оказывает влияние на процессы сбора, обработки и принятие решений.

Так как университеты преимущественно являются государственными организациями и бюджетными учреждениями, то вопрос материальных затрат является важным. Затраты на обеспечение защиты ПДн складываются из нескольких составляющих:

1) самостоятельное определение классов ИСПДн или привлечение сторонних организаций-профессионалов;
2) внедрение и сопровождение технологий защиты ПДн;
3) модификация внутренних процессов работы.

Вопрос привлечения организаций-профессионалов определяется еще и необходимостью наличия в организации лицензий регуляторов на оказание услуг и проведения работ по защите информации. Очевидно, что не каждый университет обладает подобными лицензиями, вследствие этого значительная часть расходов уходит на первые два пункта из-за «несостоятельности» вузов. А модификация внутренних

процессов работы очевидна, исходя из условий и ограничений, накладываемых специализированными методами и средствами защиты информации.

Человеческие трудозатраты также возможно разделить на несколько частей в зависимости от этапа процесса защиты ПДн и показателей квалификации специалистов.

Итак, из вышеописанных проблем и ограничений можно сделать вывод, что вопрос модернизации методик под конкретную сферу является актуальным и сложным. Исходя из наличия параметров, которые не могут изменяться специалистами в процессе модернизации (например, срок исполнения норм, или рекомендации регуляторов обязательные к исполнению), его решение лежит не только в практической плоскости, но и в научной.

ЛИТЕРАТУРА

6. ФЗ от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
7. ФЗ от 27.07.2006 №152-ФЗ «О персональных данных».
8. ФЗ от 27.12.1991 №2124-1 «О средствах массовой информации».

СОДЕРЖАНИЕ

СЕКЦИЯ 11

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

*Председатель секции – **Давыдова Е.М.**, доцент, зам. зав. каф. КИБЭВС по УР, к.т.н.;*
*зам. председателя – **Зыков Д.Д.**, доцент каф. КИБЭВС, к.т.н.*

СЕКЦИЯ 14

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель секции – **Шелупанов А.А.**, проректор по НР ТУСУРа, зав. каф. КИБЭВС, д.т.н., проф.;*
*зам. председателя – **Мещеряков Р.В.**, зам. начальника НУ ТУСУРа, доцент, зам. зав. каф. КИБЭВС по НР, к.т.н.*

Научное издание

Научная сессия ТУСУР–2011

Материалы
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2011»

4–6 мая 2011 г.

В шести частях

Часть 3

Корректор – **В.Г. Лихачева**
Верстка **В.М. Бочкаревой**

Издательство «В-Спектр».
Сдано на верстку 01.04.2011. Подписано к печати 30.04.2011.
Формат $60\times84^{1}/_{16}$. Печать трафаретная.
Печ. л. 22,25. Усл. печ. 21.
Тираж 170 экз. Заказ 12.

Тираж отпечатан в издательстве «В-Спектр».
ИНН/КПП 7017129340/701701001, ОГРН 1057002637768
634055, г. Томск, пр. Академический, 13-24, т. 49-09-91.
E-mail: bmwm@list.ru