- РАДИОТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ
- РАДИОКОНСТРУКТОРСКИЙ ФАКУЛЬТЕТ
- ФАКУЛЬТЕТ ЭЛЕКТРОННОЙ ТЕХНИКИ
- ФАКУЛЬТЕТ СИСТЕМ УПРАВЛЕНИЯ
- ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ
- ГУМАНИТАРНЫЙ ФАКУЛЬТЕТ
- ФАКУЛЬТЕТ БЕЗОПАСНОСТИ
- ЭКОНОМИЧЕСКИЙ ФАКУЛЬТЕТ
- ФАКУЛЬТЕТ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ
- ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
- ЗАОЧНЫЙ И ВЕЧЕРНИЙ ФАКУЛЬТЕТ
- ФАКУЛЬТЕТ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Преимущества обучения в ТУСУРе:

- Высокое качество образования в ТУСУРе основано на высокой квалификации профессорско-преподавательского состава, а также на передовой исследовательской материально-технической базе;

- Применение передовых технологий обучения, ориентированных на развитие творческого потенциала студентов, основанных на неразрывной связи с научными исследованиями и командной работой над реальными проектами;

- Полученное в ТУСУРе образование гарантирует 100%-ное трудоустройство, достойные условия труда, высокую зарплату и карьерный рост.

Прием документов на очную форму обучения начинается 20 июня и заканчивается 25 июля (если у абитуриента имеется полный комплект результатов вступительных испытаний в форме ЕГЭ или результатов олимпиад школьников, утвержденных Минобрнауки РФ), 5 июля (если абитуриент будет сдавать вступительные испытания в форме ЕГЭ в дополнительные сроки) и 13 июля (если абитуриент будет сдавать вступительные испытания, проводимые ТУСУР самостоятельно). Абитуриент имеет право подать заявление не более чем на 3 направления подготовки и/или специальности ТУСУР, указав их рейтинг.

Вступительные испытания профильной направленности для инженерно-технических направлений - математика, физика, русский язык; для направлений в области IT технологий и информационной безопасности - математика, информатика, русский язык; для экономико-управленческих направлений - математика, обществознание, русский язык; для гуманитарных направлений - история России, обществознание, русский язык.

Конкурс абитуриентов на бюджетные места очной формы обучения проводится с 28 июля по сумме баллов за три экзамена в порядке ее убывания. Возможен прием абитуриентов на бюджетные места по договорам целевого приема. Зачисление в число студентов ТУСУРа на бюджетные места будет вестись с 30 июля по 11 августа включительно, зачисление на платные места - 22 августа.

634050, г. Томск, пр. Ленина, 40, каб. 129
Тел.: (3822) 513-226, 900-100
Факс: (3822) 513-226
E-mail: onir@main.tusur.ru
Сайт: http://tusur.ru/

ТУСУР

НАУЧНАЯ СЕССИЯ ТУСУР–2014

МАТЕРИАЛЫ ВСЕРОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ СТУДЕНТОВ, АСПИРАНТОВ И МОЛОДЫХ УЧЕНЫХ

14–16 мая 2014 г. (В пяти частях)

Часть 3

г. Томск

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

НАУЧНАЯ СЕССИЯ ТУСУР–2014

Материалы

Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2014»

14–16 мая 2014 г., г. Томск

В пяти частях

Часть 3

В-Спектр
2014

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

Н 34 **Научная сессия ТУСУР–2014:** Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 14–16 мая 2014 г. – Томск: В-Спектр, 2014: В 5 частях. – Ч. 3. – 266 с.
ISBN 978-5-91191-305-2
ISBN 978-5-91191-308-3 (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 автоматизированых систем управления и проектирования. Рассматриваются проблемы электроники СВЧ- и акустооптоэлектроники, нанофотоники, физической, плазменной, квантовой, промышленной электроники, радиотехники, информационно-измерительных приборов и устройств, распределенных информационных технологий, вычислительного интеллекта, автоматизации технологических процессов, в частности в системах управления и проектирования, информационной безопасности и защиты информации. Представлены статьи по математическому моделированию в технике, экономике и менеджменте, антикризисному управлению, правовым проблемам современной России, 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

Конференция проводится при финансовой поддержке Российского фонда фундаментальных исследований (РФФИ) в рамках Конкурса научных проектов организации российских и международных молодежных научных мероприятий, проект № 14-07-06806

ISBN 978-5-91191-305-2
ISBN 978-5-91191-308-3 (Ч. 3)

Всероссийская научно-техническая конференция студентов и молодых ученых «Научная сессия ТУСУР–2014»

14–16 мая 2014 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, директор Института системной интеграции и безопасности, председатель правления Томского профессорского собрания, д.т.н., профессор;
- Беляев Б.А., зав. лабораторией электродинамики Ин-та физики СО РАН, д.т.н., г. Красноярск;
- 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.;
- Демидов А.Я., декан РТФ, зав. каф. ТОР, к.ф.-м.н., доцент;
- Дмитриев В.М., зав. каф. МиСА, д.т.н., профессор;
- Еханин С.Г., профессор каф. КУДР, д.ф.-м.н., доцент;
- Ехлаков Ю.П., зав. каф. АОИ, д.т.н., профессор;
- Зариковская Н.В., доцент каф. ЭМИС, 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, зам. зав. каф. КИБЭВС по НР, д.т.н., доцент;
- 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., профессор, г. Новосибирск;
- Семиглазов А.М., профессор каф. ТУ, д.т.н.;
- Суслова Т.И., декан ГФ, зав. каф. ФС, д.ф.н., профессор;
- 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 ТУСУР, зав. каф. УИ, к.э.н.;
- Ходашинский И.А., профессор каф. КИБЭВС, д.т.н.;
- Черепанов О.И., зав. 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, директор ИСИБ, д.т.н., профессор;
- Юрченкова Е.А. – ведущий инженер ОППО ТУСУРа, к.х.н.;
- Ярымова И.А. – зав. ОППО ТУСУРа, к.б.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. Радиоэлектронные системы передачи информации и средства их защиты. 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, сервис и антикризисное управление. 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 биомедицинских электронных и наноэлектронных средств. Председатель секции – Еханин Сергей Георгиевич, зав. каф. КУДР, д.ф.-м.н., доцент; зам. предсе-

дателя – Романовский Михаил Николаевич, доцент каф. КУДР, к.т.н.

Секция 5. Проектирование измерительной аппаратуры. 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. 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.

Секция 7. Радиотехника. Председатель секции – Титов Александр Анатольевич, проф. каф. РЗИ, д.т.н., доцент; зам. председателя – Семенов Эдуард Валерьевич, доцент каф. РЗИ, д.т.н.

Секция 8. 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 9. Инфокоммуникационные технологии и системы широкополосного беспроводного доступа. Председатель секции – Демидов Анатолий Яковлевич, зав. каф. ТОР, к.ф.-м.н.; зам. председателя – Гельцер Андрей Александрович, ст. преподаватель каф. ТОР, к.т.н.

Секция 10. Интегрированные информационно-управляющие системы. Председатель секции – Катаев Михаил Юрьевич, проф. каф. АСУ, д.т.н.; зам. председателя – Суханов Александр Яковлевич, доцент каф. АСУ, к.т.н.

Секция 11. Физическая и плазменная электроника. Председатель секции – Троян Павел Ефимович, зав. каф. ФЭ, проф., д.т.н.; зам. председателя – Смирнов Серафим Всеволодович, проф. каф. ФЭ, д.т.н.

Секция 12. Промышленная электроника. Председатель секции – Михальченко Геннадий Яковлевич, директор НИИ ПрЭ, проф., д.т.н.; зам. председателя – Семенов Валерий Дмитриевич, проф., зам. зав. каф. ПрЭ по НР, к.т.н.

Секция 13. Распределенные информационные технологии. Председатель секции – Ехлаков Юрий Поликарпович, зав. каф. АОИ, д.т.н., проф.; зам. председателя – Сенченко Павел Васильевич, декан ФСУ, доцент каф. АОИ, к.т.н.

Секция 15. Аппаратно-программные средства в системах управления и проектирования. Председатель секции – Шурыгин Юрий Алексеевич, ректор ТУСУРа, зав. каф. КСУП, проф., д.т.н.;

зам. председателя – Коцубинский Владислав Петрович, доцент каф. КСУП, к.т.н.

Подсекция 15.1. Интеллектуальные системы проектирования технических устройств. Председатель секции – Черкашин Михаил Владимирович, декан ФВС, доцент каф. КСУП, к.т.н.

Подсекция 15.2. Адаптация математических моделей для имитации сложных технических систем. Председатель секции – Коцубинский Владислав Петрович, доцент каф. КСУП, к.т.н.

Подсекция 15.3. Инструментальные средства поддержки автоматизированного проектирования и управления. Председатель секции – Хабибуллина Надежда Юрьевна, доцент каф. КСУП, к.т.н.

Секция 16. Вычислительный интеллект. Председатель секции – Ходашинский Илья Александрович, проф. каф. КИБЭВС, д.т.н.; зам. председателя – Костюченко Евгений Юрьевич, доцент каф. КИБЭВС, к.т.н.

Секция 17. 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 18. Методы и системы защиты информации. Информационная безопасность. Председатель секции – Шелупанов Александр Александрович, проректор по НР ТУСУРа, директор ИСИБ, д.т.н., проф.; зам. председателя – Конев Антон Александрович, доцент каф. КИБЭВС, к.т.н.

Секция 19. 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. ЭМИС, к.ф.-м.н.

Подсекция 19.1. Моделирование в естественных и технических науках. Председатель секции – Зариковская Наталья Вячеславовна, доцент каф. ЭМИС, к.ф.-м.н.; зам. председателя – Колотаев Илья Владимирович

Подсекция 19.2. 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 20. 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 22. Экология и мониторинг окружающей среды. Безопасность жизнедеятельности. Председатель секции – Карташев Александр Георгиевич, проф. каф. РЭТЭМ, д.б.н.; зам. председателя – Денисова Татьяна Владимировна, доцент каф. РЭТЭМ, к.б.н.

Секция 23. Социогуманитарные проблемы современности: история, теория, практика. Председатель секции – Суслова Татьяна Ивановна, декан ГФ, зав. каф. ФиС, д.ф.н., проф.; зам. председателя – Грик Николай Антонович, зав. каф. ИСР, д.и.н., проф.

Подсекция 23.1. Актуальные проблемы социальной работы в современном обществе. Председатель секции – Грик Николай Антонович, зав. каф. ИСР, д.и.н., проф.; зам. председателя – Вельш Дарья Владимировна, ассистент каф. ИСР

Подсекция 23.2. Современные социокультурные технологии в организации работы с молодежью. Председатель секции – Суслова Татьяна Ивановна, декан ГФ, зав. каф. ФиС, д.ф.н., проф.; зам. председателя – Орлова Вера Вениаминовна, д.соц.н., проф. каф. ФиС, директор НОЦ «СГТ»; Покровская Елена Михайловна, доцент каф. ФиС, к.ф.н., директор НОЦ ГФ ТУСУРа

Секция 24. Инновационные проекты, студенческие идеи и проекты. Председатель секции – Уваров Александр Фавстович, проректор по инновационному развитию и международной деятельности ТУСУРа, к.э.н.; зам. председателя – Дробот Павел Николаевич, доцент каф. УИ, к.ф.-м.н.

Секция 25. Автоматизация управления в технике и образовании. Председатель секции – Дмитриев Вячеслав Михайлович, зав. каф. МиСА, д.т.н., проф.; зам. председателя – Ганджа Тарас Викторович, доцент каф. МиСА, к.т.н.

Секция 26. Современные информационные технологии. Открытия. Творчество. Проекты. Председатель секции – Смолонская Марина Александровна, зам. начальника учебно-методического управления НОУ «Открытый молодежный университет»; зам. председателя – Титов Роман Васильевич, ведущий методист учебно-методического управления НОУ «Открытый молодежный университет»

Секция 27. Правовые проблемы современной России. Председатель секции – Соколовская Наталья Сергеевна, доцент каф. уголовного права, к.ю.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 – 8–13-я, 25, 26, 27-я секции;
3-й том – 16–18-я секции;
4-й том –15, 19–22-я секции;
5-й том – 23, 24-я секции.

СЕКЦИЯ 16

ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ

*Председатель секции – **Ходашинский И.А.**, профессор каф. КИБЭВС, д.т.н.;*
*зам. председателя – **Костюченко Е.Ю.**, доцент каф. КИБЭВС, к.т.н.*

ПОСТРОЕНИЕ НЕЧЕТКОГО КЛАССИФИКАТОРА НА ОСНОВЕ ПОПУЛЯЦИОННОГО СОРНЯКОВОГО АЛГОРИТМА ОПТИМИЗАЦИИ

А.Е. Анфилофьев, студент 5-го курса каф. КИБЭВС
Научный руководитель И.А. Ходашинский, профессор, д.т.н.
г. Томск, ТУСУР, yowwi00@gmail.com

Моделирование сложных систем осложняется проблемой неточного или неполного описания изучаемого объекта. Одним из решений такой проблемы является нечеткое моделирование. В данной работе рассматривается нечеткий классификатор (основанный на нечеткой логике). Классификация рассматривается как процесс определения некоторого класса объекта исследования в соответствии с какими-либо характерными признаками, которые определяются путем обнаружения связей между имеющимися наборами данных, исходя из которых будет проводиться классификация.

Обработка информации в нечеткой системе осуществляется при помощи базы правил. Каждое правило содержит условную и заключительную часть. Антецедент (IF-часть) включает в себя утверждение, относящееся ко входным параметрам, консеквент (THEN-часть) указывает значение выходной переменной – название класса.

Для создания нечетких классификаторов используются хорошо изученные классические методы, и метаэвристические, которые менее точны, но зачастую эффективнее первых при решении нелинейных, многокритериальных задач оптимизации с ограничениями.

Алгоритм. Рассматривается популяционный сорняковый алгоритм оптимизации. Его суть построена на основе модели способа распространения сорняков на ограниченной площади. Сорняки сначала захватывают территорию, а при достижении максимально возможной концентрации начинают бороться за выживание [2].

Каждый сорняк является решением. Качество решения улучшается путем порождения новых сорняков, и уничтожением менее приспособленных, если достигается максимальный предел количества сорняков. Количество решений увеличивается до определенного максимума и впоследствии остается фиксированным в каждом поколении.

Приводится описание пошагового алгоритма.

Шаг 1. Инициализация исходной популяции.

Задается популяция фиксированного размера. Каждый элемент популяции представляет собой вектор в виде массива, который состоит из необходимого для описания одного состояния нечеткой системы количества переменных (количество входных переменных нечеткой системы, умноженное на количество переменных, описывающих каждую функцию принадлежности, умноженное на количество функций принадлежности для одной переменной).

Каждая функция принадлежности в каждом векторе задается случайным образом в заданных границах диапазона с учетом того, что левая граница каждой последующей функции принадлежности отдельной переменной должна находиться правее левой границы предыдущей функции принадлежности.

Задается максимальное количество, которое может достигнуть популяция сорняков.

Задается количество итераций для работы алгоритма в качестве критерия остановки.

Шаг 2. Генерация нового решения на основе нормального распределения Бокса–Мюллера.

На основе значения фитнес функций, вычисленной на основе среднеквадратичной ошибки, для каждого из векторов вычисляется количество, которое может породить данный вектор (чем меньше значение среднеквадратичной ошибки, тем больше количество порождаемых векторов).

Шаг 3. Оценка качества решения.

Сравниваются значения фитнес-функций, вычисленныго на основе среднеквадратичной ошибки, для всех векторов.

Шаг 4. Удаление «худших» решений.

Если превышен предел популяции, то удаляется то количество векторов, имеющих наибольшее значение среднеквадратичной ошибки, которое вернет популяцию к максимально возможному значению.

Шаг 5. Итерации продолжаются заданное количество раз, начиная с шага 2.

Эксперимент. Данный алгоритм применяется для построения нечеткого классификатора. Для проведения эксперимента выбраны данные из репозитория www.keel.es. В качестве сравнения для тестов бы-

ли выбраны результаты тестов из публикации [3], где проводились эксперименты и представлены результаты сравнения классификации ирисов – классической задачи классификации, с которой начинают тестирование нечеткого классификатора.

ЛИТЕРАТУРА

1. Ходашинский И.А., Дудин П.А. Идентификация нечетких систем на основе непрерывного алгоритма муравьиной колонии // Автометрия. 2012. Т. 48, № 1. С. 63–71.

2. Rad H.S., Lucas C.A. Recommender System based in Invasive Weed Optimization Algorithm // IEEE Congress on Evolutionary Computation (CEC 2007). 2007. P. 4297–4304.

3. KEEL Data-mining software Tool: data, set repository, integration of algorithms and experimental analysis framework. / J. Alcala-Fdez, A. Fernandez, J. Luengo et al // J. of Mult.-Valued Logic & Soft Computing. 2011. Vol. 17. P. 255–287.

КОДИРОВАНИЕ СТРУКТУРЫ НЕЧЕТКОЙ СИСТЕМЫ

А.В. Боровков, аспирант каф. КИБЭВС

Научный руководитель И.А. Ходашинский, профессор каф. КИБЭВС, д.т.н.

г. Томск, ТУСУР, xander27b@gmail.com

Одним из основных преимуществ использования нечетких систем (НС) в качестве классификатора или аппроксиматора является использование базы правил (БП) в удобном для человека виде. Однако БП, полученная на основе перебора всех возможных комбинаций термов, часто является громоздкой, избыточной или плохо отражающей предметную область. Поэтому встает вопрос структурной идентификации НС – определение структуры БП (набора используемых в правилах термов и переменных и самих правил) меньшего размера и/или лучше отражающей предметную область. Подавляющее большинство современных алгоритмов оптимизации рассчитаны на оптимизации функции с фиксированным числом параметров (работают с вектором фиксированной длины), поэтому встает вопрос о том, каким образом кодировать вектор, передаваемый алгоритму оптимизации, чтобы в нем была учтена не только параметрическая, но и структурная составляющая НС.

Очевидно, если взять некоторую нечеткую систему и выключать из ее состава некоторые правила, переменные или части антецедентов (пары вида «Переменная X = Терм 1»), то можно на основе этой системы получить множество НС различной структуры. Подобное изменение структуры может быть использовано для получения более простых НС. Представим базы правил изначальной НС и НС с модифицированной структурой в табличном виде (табл. 1 и 2).

Таблица 1

Полная база правил

	Переменная X	Переменная Y	Переменная Z
Правило 1	Терм X1	Терм Y1	Терм Z1
Правило 2	Терм X1	Терм Y1	Терм Z2
Правило 3	Терм X1	Терм Y1	Терм Z3
Правило 4	Терм X1	Терм Y2	Терм Z1
Правило 5	Терм X1	Терм Y2	Терм Z2

Таблица 2

Модифицированная база правил

	Переменная X	Переменная Y	Переменная Z
Правило 1	Терм X1	Терм Y1	Терм Z1
Правило 2	–	Терм Y1	–
Правило 3	–	–	Терм Z3
Правило 4	Терм X1	–	–
Правило 5	–	Терм Y2	–

Исключение всех предпосылок для одного правила будет означать исключение правила из НС, исключение всех предпосылок для одной переменной будет означать исключение переменной из НС.

Определим способ кодирования информации об исключении предпосылок в виде числового вектора, со значениями, лежащими в отрезке [0; 1].

Таблица 3

Преобразование правил (n = 4)

1	Правило 1			Правило 2			Правило 3			Правило 4			Правило 5		
2	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*	*X*	*Y*	*Z*
3	1	1	1	0	1	0	0	0	1	1	0	0	0	1	0
4	11			15			8			7					
5	0,06875			0,9375			0,5			0,4375					

Разберем табл. 3 по строкам.

1. Правила.

2. Соответствующие правилам 3 предпосылки (предпосылка определяется переменной, которая в ней используется).

3. Закодированное значение включения и выключения предпосылки в базу правил (1 – предпосылка включена, 0 – выключена).

4. Значение получается следующим образом: берется n (в данном случае = 4) элементов 3-й строки, которые составляют бинарный вектор (например, для 1-й группы «1110»), и определяется позиция (номер строки, нумерация с 0) этого вектора в таблице кодов Грея (в данном случае используется зеркальный способ получения кодов Грея). Эта позиция записывается в качестве значения (например, для «1110» зна-

чение будет равно 11). Если в крайней правой группе в строке 3 нехватает элементов, то она дополняется «0» справа.

Нормированные значения от 0 до 1, полученные делением значения из строки 4 на 2^n.

Таким образом, 5-я строка таблицы содержит информацию об использовании предпосылок в базе правил в удобном для обработки алгоритмами оптимизации виде. Использование кодов Грея дает естественное соответствие небольших изменения значений в данном векторе, небольшим изменениям структуры НС. Для обратного преобразования необходимо провести шаги в обратном порядке (значения в строке 4 необходимо округлять до ближайшего меньшего целого).

Данный подход имеет ряд недостатков, таких как избыточность вектора (при выключении большого количества предпосылок размер вектора будет соответствовать начальному) и не возможность получения систем с большим количеством предпосылок в правиле. Однако, все же имеет практическую ценность при условии наличия достаточных вычислительных ресурсов, в задачах упрощения НС.

ЛИТЕРАТУРА

1. Горбунов И.В. Алгоритмы генерации компактных баз правил для нечеткого аппроксиматора / Матер. междунар. заоч. науч.-практ. конф. «Наука, образование, общество: тенденция и перспективы». М.: АР-Консалт, 2013. Ч. 2. С. 98–104.

ПОДХОД, ОСНОВАННЫЙ НА РАЗБИЕНИЯХ, ДЛЯ ДЕКОМПОЗИЦИИ ПОЛИНОМОВ

М.Ю. Перминова, аспирант каф. ПрЭ
Научный руководитель В.В. Кручинин,
профессор каф. ПрЭ, зав. ЛИСМО ИИ ТУСУРа, д.т.н.
г. Томск, ТУСУР, pmy@2i.tusur.ru

В работе будет рассмотрен подход декомпозиции полиномов, основанный на разбиениях.

Пусть даны два полинома $A(x)$ и $B(x)$. Тогда для вычисления композиции $F(x)$ будет верно

$$f(n) = \sum_{k=1}^{n} A^{\Delta}(n,k)b(k). \qquad (1)$$

Известно [1], что коэффициенты $A^{\Delta}(n,k)$ можно представить на основе композиций натурального числа n:

$$A^{\Delta}(n,k) = \sum_{\pi_k \in C_n} a(\lambda_1)a(\lambda_2)\dots a(\lambda_k),$$

где C_n – множество всех композиций натурального числа n; π_k – композиция $\sum_{i=1}^{k} \lambda_i = n$, имеющая ровно k частей.

Рассмотрим связь композиции и разбиения.

Разбиением натурального числа n называется всякая конечная невозрастающая последовательность натуральных чисел $\lambda_1, \lambda_2, \dots, \lambda_r$, для которой

$$\sum_{i=1}^{k} \lambda_i = n.$$

Числа λ_i называются частями разбиения [2].

Известно [1] представление $A^A(n,k)$ на основе разбиений:

$$A^A(n,k) = \sum \binom{k}{j_1 j_2 \dots j_{n-k+1}} a(1)^{j_1} a(2)^{j_2} \dots a(n-k+1)^{j_{n-k+1}},$$

где суммирование ведется по всем последовательностям j_1, j_2,…, j_{n-k+1} ($k = \overline{1,n}$) неотрицательных целых чисел, для которых

$j_1 + j_2 + \dots + j_{n-k+1} = k$ и $j_1 + 2j_2 + \dots + (n-k+1)j_{n-k+1} = n$.

В композиции в отличие от разбиений учитывается порядок частей. Следовательно, мультиномиальный коэффициент показывает, сколько существует вариантов композиций, состоящих из тех же частей разбиения.

Для получения системы уравнений сначала необходимо найти порядок полиномов композиции. Зная порядок исходного полинома, находятся делители этого порядка. Те делители, произведение которых даёт порядок исходного полинома, являются порядками полиномов композиции.

Далее, применяя композиционную формулу (1) и учитывая связь композиции и разбиений, получается система из n уравнений:

$$\sum_{k=1}^{n} \binom{k}{j_1 j_2 \dots j_{n-k+1}} a(1)^{j_1} a(2)^{j_2} \dots a(n-k+1)^{j_{n-k+1}}\, b(k) - f_n, \quad (2)$$

где $n = \overline{1, m \cdot l}$; m и l – найденные ранее порядки полиномов $A(x)$ и $B(x)$ соответственно. В полученной формуле $a(n-k+1)$ – это части разбиения; степень j в $a(n-k+1)^j$ – это число частей разбиения; k в $b(k)$ показывает число частей разбиения.

В (2) степень a не должна превышать порядок полинома, то есть для нахождения системы уравнений используются ограниченные разбиения. Такие ограниченные разбиения исследовал Г. Эндрюс. В его работе [2] описан алгоритм генерации разбиений. Применяя этот алгоритм и формулу (1), всегда можно получить систему уравнений (2). Решив её, можно найти необходимые коэффициенты композиции полиномов.

Пример. Пусть $F(x) = x^6 + 2x^5 + 3x^4 + x^3 - x^2 + 7x$. Необходимо получить систему уравнений для декомпозиции полинома с использованием разбиений.

Порядок исходного полинома равен 6. Значит, порядки полиномов композиции будут 2 и 3. Применяя (2), получаем систему уравнений

- Порядок внешнего полинома равен 3, внутреннего – 2:

$$a_1b_1 - 7 = 0, a_1^2b_2 + a_2b_1 + 1 = 0, a_1^3b_3 + 2a_1a_2b_2 - 1 = 0,$$
$$3a_1^2a_2b_3 + a_2^2b_2 - 3 = 0, 3a_2^2a_1b_3 - 2 = 0, a_2^3b_3 - 1 = 0.$$

- Порядок внешнего полинома равен 2, внутреннего – 3:

$$a_1b_1 - 7 = 0, a_1^2b_2 + a_2b_1 + 1 = 0, a_3b_1 + 2a_1a_2b_2 - 1 = 0,$$
$$2a_1a_3b_2 + a_2^2b_2 - 3 = 0, 2a_2a_3b_2 - 2 = 0, a_3^2b_2 - 1 = 0.$$

В $a_2^3b_3 - 1$ – разбиение числа 6 на 3 позиции, в каждой 2, 1 – коэффициент при x^6 в исходном полиноме; $3a_2^2a_1b_3 - 2$ – разбиение числа 5 на 3 позиции: в двух по 2, в одной – 1; 3 – мультиномиальный коэффициент $\binom{3}{2,1}$ и так далее.

ЛИТЕРАТУРА

1. Кручинин В.В., Кручинин Д.В. Степени производящих функций и их применение. Томск: Изд-во Томск. гос. ун-та систем упр. и радиоэлектроники, 2013. 236 с.

2. Эндрюс Г. Теория разбиений / пер. с англ. М.: Наука. Главная редакция физико-математической литературы, 1982. 256 с.

АЛГОРИТМ ВЫБОРА ПРОГРАММНОГО ПРОДУКТА НА ОСНОВЕ ИНТЕГРАЛА ШОКЕ

А.В. Ахаев, аспирант каф. КИБЭВС

Научный руководитель И.А. Ходашинский, профессор каф. КИБЭВС, д.т.н.

г. Томск, ТУСУР, AkhaevAV@gmail.com

В данной работе решается задача выбора наилучшей альтернативы из нескольких вариантов в соответствии с пользовательскими требованиями. При этом альтернативы оцениваются по нескольким параметрам (функциональным возможностям), что вносит сложность в анализ и обработку данных.

При решении задачи выбора программного продукта (ПП) основной целью является получение наилучшего программного продукта по требованиям пользователя [1]. Под получением наилучшего понимается выбор такого ПП, в котором с учетом всех разнообразных и противоречивых требований будет определена общая ценность, максимально способствующая достижению поставленной цели. В работе приводится решение данной задачи на основе интеграла Шоке.

Алгоритм. Алгоритм выбора программного продукта на основе интеграла Шоке состоит из следующих этапов:

1) определение нечеткой меры на основе обучающей выборки;
2) определение наилучшего программного продукта.

Этап 1. Нечеткий интеграл Шоке от функции $f: A \to R$ на множестве A по нечеткой мере μ определяется как [2]:

$$(c)\int_A f d\mu = \sum_{i=1}^{n} (f(\sigma(i)) - f(\sigma(i-1)))\mu(A_{(i)}), \qquad (1)$$

где σ является перестановкой индексов для ранжирования $f(\sigma(1)) \le \cdots \le f(\sigma(n))$, $A_{(i)} = \{\sigma(i), \ldots, \sigma(n)\}$ и $f(\sigma(0)) = 0$.

Рассматриваемая задача включает n атрибутов и m программных продуктов. Если бы нечеткая мера $\tilde{\mu}$ была известна, то интегральные оценки $\tilde{y}_i$ функциональных возможностей ПП могли быть определены с помощью (1).

Для извлечения нечеткой меры необходима обучающая выборка, в которой есть только экспертные интегральные оценки функциональных возможностей ПП. Для того чтобы определить интегральные оценки других альтернатив, необходимо определить μ такое, что соответствующий вычисленный интеграл Шоке был как можно ближе к значениям выборки. В результате целью является минимизация следующей суммы (и получение максимально близкого к нулю значения) [2]:

$$e = \sum_{j=0}^{m} \left(\tilde{y}_i - \sum_{i=1}^{n} (f(\sigma(i)) - f(\sigma(i-1)))\tilde{\mu}(A_{(i)})\right)^2. \qquad (2)$$

Кроме того, оптимальное решение должно удовлетворять ограничениям: нечеткие меры должны быть монотонными и всегда принадлежать интервалу между 0 и 1. Таким образом, извлечение нечеткой меры является проблемой оптимизации с ограничениями, и варианты решения должны быть проверены на ограничения.

Этап 2. Для определения наилучшего программного продукта по требованиям $\tilde{y}_i$ пользователя необходимо для каждого ПП вычислить интеграл Шоке (1). Максимальное значение интеграла будет соответствовать наилучшему ПП.

Реализация. Рассмотренный алгоритм реализован средствами системы «1С:Предприятие 8» (рис. 1) и обеспечивает выполнение следующих возможностей:

- задание оценок функциональных возможностей ПП;

- определение нечеткой меры на основе обучающей выборки;
- определение интегральной оценки функционального наполнения ПП на основе системы интеграла Шоке;
- вывод результатов по каждому программному продукту;
- сравнение программных продуктов по интегральным оценкам функционального наполнения.

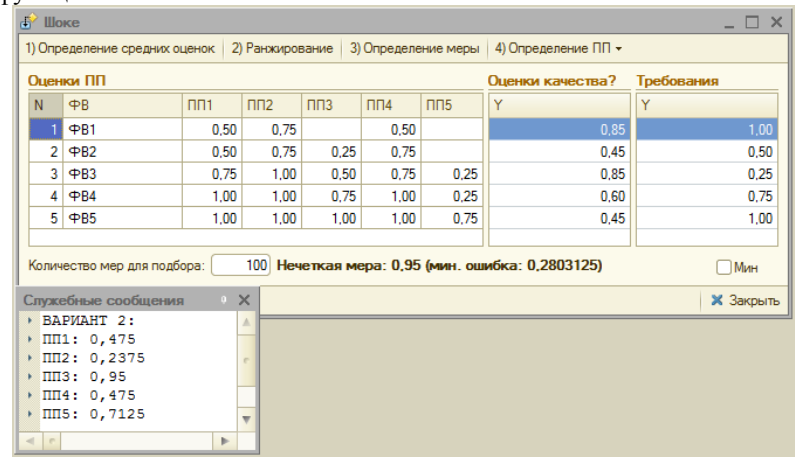


Рис. 1. Программная реализация

На данный момент создан пользовательский интерфейс, позволяющий представлять результаты в наглядной и удобной для проведения анализа форме.

Заключение. Таким образом, предложен алгоритм, позволяющий анализировать программные продукты по функциональному наполнению. На основе представленного алгоритма разработана подсистема, которая является частью экспертной системы [1] и позволяет подобрать наилучший программный продукт по требованиям пользователя.

Для извлечения нечеткой меры $\tilde{\mu}$ в дальнейшем планируется использовать метаэвристические подходы оптимизации.

ЛИТЕРАТУРА

1. Ахаев А.В. Алгоритмы и программные средства построения экспертных систем выбора программных продуктов на примере «1С:Предприятие 8» / А.В. Ахаев, И.А. Ходашинский // Информатика и системы управления. 2013. №4. С. 70–79.

2. Wang X. Fuzzy Measure Extraction for Software Quality Assessment as a Multi-Criteria Decision-Making Problem / X. Wang, M. Ceberio, Sh. Virani, Ch. D. Hoyo, L. Gutierrez // Sets and Systems – Special issue on fuzzy measures and integrals, 1999. Vol. 102, № 3. P. 463–469.

ПОСТРОЕНИЕ НЕЙРОСЕТЕВОЙ МОДЕЛИ ГРУППЫ СКВАЖИН

М.Б. Байдин, В.А. Чурилов, Е.О. Иванов, аспирант
г. Томск, ТУСУР, каф. АОИ, the_scrubs_fan@mail.ru, churilovvictor@mail.ru, egor.o.ivanov@yandex.ru
Проект ГПО АОИ-1301 – «Энергосберегающее ситуационное нейросетевое управление»

При эксплуатации большого количества артезианских скважин единого водоносного пласта часто наблюдается их взаимное влияние, в результате чего образуется депрессия водоносного горизонта, которая растет при увеличении подачи скважин, что приводит к снижению уровня воды в скважинах и возрастанию высоты подъема. Интенсивный отбор из водоносного горизонта может привести к его истощению [1].

Для выполнения требований к технологическим режимам работы всей системы добычи и подачи воды, требований к объемам добываемой воды и сохранения водоносного горизонта необходимо отслеживать, а еще лучше

, заранее определять уровни дебита и понижения для каждой из скважин.

Анализ формулы для расчета значения дебитов (количества добываемой воды) и понижений уровня воды в системе скважин [2] показывает, что для определения понижения уровня воды в скважинах необходимо знать значения дебитов каждой скважины. Для статических и порогово изменяющихся дебитов данная задача не представляет сложности. Однако в случае динамических значений дебитов, например частотного управления насосами скважин, для расчета будущих значений понижений необходимо знать будущие значения дебитов. При этом выбор оптимальных значений дебитов должен быть основан на будущих значениях понижения уровня. Иными словами, для определения понижения уровней в каждой скважине необходимо знать значения дебитов каждой скважины, для определения которых в свою очередь необходимо знать значения понижений уровней. Для выхода из этого замкнутого круга авторы предлагают использовать прогноз обоих показателей каждой скважины – дебита и понижения. Искомый предиктор должен выдавать прогнозные значения дебита и понижения на основе предыдущих значений этих показателей для каждой скважины водоносного горизонта. Это позволит сигнализировать ситуации выхода за пределы максимально возможных уровней понижения уровня и расхождения суммарного дебита водозабора с необходимым потребителю. Также возможен поиск оптимальных значений дебита и понижения каждой из скважин, например в случае использования итерационного подхода.

Для создания предиктора предполагается использование аппарата искусственных нейронных сетей. Перед обучением сети динамике работы скважин необходимо собрать численные данные дебитов Q_i и понижений S_i каждой из скважин. Такие данные могут быть получены с помощью измерительных приборов (например, уровнемеров и расходомеров) и агрегированы на некоторый интервал времени, например 10 дней. Выбор интервала агрегации определяется отдаленностью даты, на которую требуется получить прогноз, от текущей, количеством измеренных данных, требуемой точностью прогноза и скоростью обучения сети. Затем необходимо определиться с датой, на которую необходимо получение прогноза. Это может быть 3, 6, 12 и более месяцев с текущего момента времени, в зависимости от необходимости. Такие данные могут быть сгруппированы в обучающие выборки по принципу: n пар значений Q_i/S_i за интервалы, предшествующие некоторому прошедшему моменту времени t, и одна пара Q_i/S_i на момент времен t. Путем изменения t (сдвиг окна) происходит получение следующей обучающей пары. Выбор количества предшествующих пар значений n основывается на требованиях к качеству и сроку прогноза. Для каждой скважины создадим отдельную многослойную нейронную сеть с $2n$ входами ($2 = Q_i/S_i$) и 2 выходами. Выходы каждой из сетей будут подаваться на еще одну сеть, которая будет учитывать взаимное влияние скважин. Количество входов и выходов последней сети будет равно удвоенному количеству скважин. Таким образом, получим сложную единую сеть в виде каскада сетей.

Заключение. Для решения поставленной задачи расчета и прогнозирования понижения уровня воды в скважине была построена аналитическая модель скважины. На основе аналитической модели планируется произвести обучение нейронной сети по методу обратного распространения ошибки. Обученная на примере из реальных данных сеть позволит составлять прогноз на определенное количество времени.

ЛИТЕРАТУРА

1. Суреньянц С.А., Иванов А.П. Эксплуатация водозаборов подземных вод. М.: Стройиздат, 1989. 80 с.

2. Назаров И.А. Водоснабжение населенных мест и промышленных предприятий. М.: Стройиздат, 1977. 288 с.

НАСТРОЙКА КОНСЕКВЕНТОВ ПРАВИЛ НЕЧЕТКОЙ СИСТЕМЫ ПРИ ПОМОЩИ РЕКУРСИВНОГО МЕТОДА НАИМЕНЬШИХ КВАДРАТОВ

С.А. Черепанов, студент

Научный руководитель И.А. Ходашинский, профессор каф. КИБЭВС, д.т.н.

г. Томск, ТУСУР, sivkinpunk@gmail.com

В настоящее время моделирование является основной методологией познания действительности, т.к. далеко не всегда есть возможность изучать саму систему ввиду тех или иных причин [1]. Строгие математические модели позволяют проводить качественный и количественный анализ свойств изучаемой системы. Однако математическое моделирование требует от разработчика высокого уровня математических знаний и навыков. Поэтому математические модели зачастую составляются математиками, а не исследователями какой-либо предметной области или проблемы. Исследователь в то же время способен дать лингвистическое описание изучаемой системы при помощи различных описаний и правил.

Нечеткое моделирование является эффективным инструментом преобразования этих лингвистических правил и описаний в математические алгоритмы и формулы. Данная область развивается уже достаточно давно и имеет сформированные стандартные процедуры и методы [2].

Весьма популярными в практическом применении в настоящее время являются системы типа синглтон. Система такого типа выполняет отображение из входного пространства $A \subset \mathbb{R}^n$ в выходное пространство $B \subset \mathbb{R}$. Правила в такой системе представлены следующим образом:

$$IF\ x_1 = A_{11}\ AND\ x_2 = A_{21}\ AND \dots AND\ x_n = A_{n1}\ THEN\ y = v_1,$$
$$IF\ x_1 = A_{12}\ AND\ x_2 = A_{22}\ AND \dots AND\ x_n = A_{n2}\ THEN\ y = v_2,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$IF\ x_1 = A_{1R}\ AND\ x_2 = A_{2R}\ AND \dots AND\ x_n = A_{nR}\ THEN\ y = v_R,$$

где A_{ij} – лингвистический терм, которым оценивается переменная x_i, v_i – значение консеквента i-го правила.

Нечеткая система задает отображение $f: \mathbb{R}^n \to \mathbb{R}$:

$$f(x) = \sum_{i=1}^{R} \mu_{A1i}(x_1) \cdot \dots \cdot \mu_{Ani}(x_n) \cdot v_i \Big/ \sum_{i=1}^{R} \mu_{A1i}(x_1) \cdot \dots \cdot \mu_{Ani}(x_n)$$

и может быть представлена как

$$y = f(x; \theta, v),$$

где $\theta = [\theta_1, \theta_2, \dots, \theta_N]$ – вектор параметров антецедентов, $v = [v_1, v_2, \dots, v_R]$ – вектор параметров консеквентов. В данной работе

предлагается применение рекурсивного метода наименьших квадратов для настройки значений вектора r.

Метод наименьших квадратов является одним из наиболее эффективных методов настройки параметров консеквентов правил нечётких систем [3,4].

Пусть имеется обучающая выборка $\{(x_p, t_p) | p = 1, \dots, m\}$. Тогда ошибка нечеткой системы описывается следующим вектором:

$$E = [e_1, e_2, \dots, e_m]^T,$$

где

$$e_p = t_p - f(x_p, \theta, r).$$

Данная ошибка будет минимальной, когда значение выражения

$$\sum_{i=1}^{M} e_i^2 = E^T E$$

будет минимальным. Минимизируя данное выражение по r, получим следующее значение параметров консеквентов:

$$\hat{r} = (\Phi^T \Phi)^{-1} \Phi^T Y, \quad (1)$$

где $Y = [y_1, y_2, \dots, y_m]^T$ – вектор выходных значений системы, а векторы входных данных $x_1, x_2, \dots, x_m$ собраны в матрицу:

$$\Phi = \begin{bmatrix} (x_1)^T \\ (x_2)^T \\ \vdots \\ (x_m)^T \end{bmatrix}$$

Как видно из формулы (1), применение данного метода к реальным данным, поступающим в систему в реальном времени, невозможно по нескольким причинам. Во-первых, при расчётах в данном методе используется вычисление обратной матрицы, что при больших размерностях является вычислительно трудной задачей. А во-вторых, при работе с реальными данными нередко получается так, что определитель искомой матрицы равен 0. Это ведёт к дополнительным оптимизациям и пересчётам, что недопустимо при обработке данных в реальном времени.

Применение рекурсивного метода [5,6] наименьших квадратов позволяет избежать данных проблем. В данном методе вектор параметров высчитывается рекуррентно:

$$\hat{r}(k) = \hat{r}(k-1) + P(k) x_k (y_k - (x_k)^T \hat{r}(k-1)), \quad (2)$$

где $P(k)$ – ковариационная матрица, которая также высчитывается рекуррентно:

$$P(k) = \frac{1}{\lambda} [I - P(k-1) x_k (\lambda I + (x_k)^T P(k-1) x_k)^{-1} (x_k)^T] P(k-1), \quad (3)$$

где $0 \ll \lambda \ll 1$ – фактор забывания (чем меньше, тем большее влияние на результат оказывают новые данные).

В этом случае $\theta(0)$ считается по обычному МНК на специально подготовленной обучающей выборке, не дающей вырожденной матрицы. $P(0)$ также находится традиционным способом.

Как видно из формул (2) и (3), в данном методе при подсчете текущих значений параметров отсутствует вычисление обратной матрицы, что помогает решить вышеописанные проблемы с вычислительной сложностью и вырожденными матрицами.

Рекурсивный метод наименьших квадратов предполагается использовать в дальнейшем для разработки нечеткого самообучающегося классификатора, работающего над данными, поступающими в реальном времени.

ЛИТЕРАТУРА

1. Самарский А.А., Михайлов А.П. Математическое моделирование: Идеи. Методы. Примеры. М.: ФИЗМАТЛИТ, 2002. 320 с.

2. Tron E., Margaliot M. Mathematical modeling of observed natural behavior: a fuzzy logic approach // Fuzzy Sets and Systems. 2004. Vol. 146 P. 437–450.

3. Evsukoff A. Structure identification and parameter optimization for nonlinear fuzzy modeling / Alexandre Evsukoff, Antonio C.S. Brancoa, Sylvie Galichet // Fuzzy Sets and Systems. 2002. № 132. P. 173–188.

4. Wang L.X. Fuzzy basis functions, universal approximation, and orthogonal least-squares learning / L.X. Wang, J.M. Mendel // IEEE Transactions on Neural Networks. 1992. Vol. 3. P. 807–814.

5. Lughofer E. Evolving Fuzzy Systems – Methodologies, Advanced Concepts and Applications. Springer, 2011. 456 p.

6. Passino K. M. Fuzzy Control / Kevin M. Passino, Stephen Yurkovich. Addison Westley, 1997. 522 p.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ТЕСТИРОВАНИЯ ПРОГРАММ

И.В. Черноусов, П.Е. Густокашин, студенты каф. АСУ,
С.А. Черепанов, М.М. Антонов, студенты каф. КИБЭВС
Научные руководители: В.Н. Кирнос, доцент каф. КИБЭВС, к.т.н.,
М.Ю. Катаев, профессор каф. АСУ, д.т.н.
г. Томск, ТУСУР, krusnik.viers@gmail.com
Проект ГПО КИБЭВС-1102 (АСУ-1101) – «Программное обеспечение для организации и проведения спортивного программирования»

Суть проблемы автоматизированного тестирования программ заключается в отсутствии объективных методов оценки корректности решений.

Одним из самых распространенных методов оценки корректности является визуальный анализ программного кода в сочетании с ручной проверкой решения на нескольких наиболее важных с точки зрения проверяющего тестах. Анализ производится человеком и потому не может являться объективным. Небольшое же количество тестов обусловливает низкое качество полученных результатов. Значительно более надежным методом является полноценное тестирование – подача на вход программе небольшого набора тестов и сравнение реальных выходных данных с ожидаемыми выходными данными. Однако для достижения объективной оценки количество тестов должно быть достаточным для того, чтобы были покрыты все возможные ситуации. Очевидно, ручная проверка одной программы требует огромного количества времени и влечет за собой невозможность контроля ограничений.

Кроме того, важна не только корректность программы, но и её качество – оптимальность по потребляемым для решения задачи ресурсам. В процессе применения данной модели к реальной системе возникают новые обстоятельства. В частности, для одной и той же задачи может существовать множество решений, различных по потребляемым ресурсам. В качестве примера возьмем задачу коммивояжера. Сложность переборного решения пропорциональна факториалу от количества вершин в графе. Используя алгоритмы динамического программирования, сложность можно значительно понизить [1].

Для того чтобы отсечь неоптимальные решения, необходимо ввести дополнительные ограничения количества используемого времени и используемой памяти. Если программа превысила хотя бы одно из данных ограничений, то она считается недостаточно оптимальной и завершается.

На данный момент существуют системы, способные в автоматическом режиме проверять программы на наборах тестов. Они позволяют проводить олимпиадные соревнования, но мало пригодны для учебного процесса: их адаптация к приему лабораторных работ требует неоправданно высоких трудозатрат. В исходном же виде явным недостатком выступает «спортивность» систем. Возникает неоправданная соревновательность среди студентов, понижается открытость диалога между студентом и проверяющим.

Задачей нашего проекта является разработка системы, позволяющей проводить автоматизированную проверку решений поставленных задач и обладающей следующими характеристиками: высокая производительность, доступность результатов проверки в реальном времени, интерактивное взаимодействие с пользователем, совместимость с правилами олимпиад по программированию АСМ и ВКОШП, возможность проведения на ней лабораторных работ и тренировок.

В первую очередь, необходимо ознакомиться с принятой системой оценки решения. По результатам тестирования решение получает вердикт. Общим вердиктом решения является тот, который находится выше в списке вердиктов. Если одновременно было получено несколько таких вердиктов, выбирается тот, который был получен на более раннем тесте. При одновременном выполнении нескольких условий получения генерируется вердикт, находящийся выше по списку [2]. Сам список вердиктов представлен ниже:

- SE (System error). Ошибка на стороне сервера.
- CE (Compilation error). Ошибка компиляции решения.
- TLn (Time limit exceeded on test *n*. Превышено допустимое время работы на тесте *n*.
- MLn (Memory limit exceeded on test *n*). Попытка использовать больше памяти, чем доступно по условию задачи на тесте *n*.
- REn (Runtime error on test *n*). Программа завершилась с ненулевым кодом возврата.
- PEn (Presentation error on test *n*). Ошибка в формате выходных данных на тесте *n*.
- WAn (Wrong answer on test *n*). Получен неверный ответ на тесте *n*.
- AC (Accepted). Все тесты успешно пройдены, решение верное.

Для реализации данной задачи нами была разработана следующая структура. Система состоит из логически независимых блоков: интерфейса пользователя (сайта), базы данных и сервера тестирования. Пользователь взаимодействует с сайтом, информация с сайта записывается в базу данных, после чего сервер обрабатывает её: ядро тестирующей системы формирует вердикт, который заносится в базу данных и передаётся на сайт.

Сервер является блоком, реализующим бизнес-логику тестирования: поступающий от сайта исходный код сохраняется в базе данных, после чего производится выборка всех непроверенных решений, каждое из которых впоследствии поступает в ядро для последующего тестирования.

Ядро выполняет компиляцию полученного от сервера решения, последующий его запуск на наборе тестов и отслеживание выполнения установленных ограничений [2].

Ознакомившись на сайте с условием задачи и написав исходный код программы для её решения, пользователь использует форму отправки. В форму помещается исходный код с указанием используемого компилятора. В случае успешной компиляции полученный исполняемый файл запускается системой на наборе тестов, соответствующем задаче. Результат тестирования доступен в очереди попыток пользова-

теля на сайте. Он содержит данные об использованном времени и памяти, а также назначенный тестирующей системой вердикт. Кроме того, результаты заносятся в сводную таблицу, содержащую сравнительную характеристику всех пользователей по результатам решений задач одного блока.

Важной особенностью системы является возможность одновременной проверки нескольких решений. Для этого создаются несколько виртуальных машин, каждая из которых подключается к общей базе данных. Каждая из них забирает первое непроверенное решение и обрабатывает его. Для того чтобы не возникло ситуации, когда несколько виртуальных машин забрали одно и то же решение, была реализована атомарность данной операции – в один момент времени только одна машина сможет забрать решение из БД.

На данный момент система уже успешно применяется на практике для проведения как лабораторных занятий, так и олимпиад. Кроме того, на базе этой системы проводятся регулярные тренировки студентов по олимпиадному программированию.

ЛИТЕРАТУРА

1. Cormen T. Introduction to algorithms / T. Cormen, C. Leiserson, R. Rivest, C. Stein – McGraw-Hill Science, 2003. 1056 с.

2. ACM ICPC Regional Rules [Электронный ресурс]. Режим доступа: http://icpc.baylor.edu/regionals/rules, свободный (дата обращения: 25.02.2014).

ПОСТРОЕНИЕ АНСАМБЛЯ КЛАССИФИКАТОРОВ НА ОСНОВЕ ДЕРЕЬВЕВ РЕШЕНИЙ

В.А. Дель, студент каф. КИБЭВС

Научный руководитель И.А. Ходашинский, профессор каф. КИБЭВС, д.т.н.

г. Томск, ТУСУР, Rush.vr@gmail.com

Интеллектуальный анализ данных (data mining) – это научный подход к обнаружению в данных ранее неизвестных, нетривиальных, практически полезных и интерпретируемых закономерностей, необходимых для принятия решений в различных областях человеческой деятельности.

Одним из методов интеллектуального анализа данных является использование деревьев решений. Данный метод имеет следующие преимущества:

– позволяет решать широкий круг задач, таких как классификация, регрессия, кластеризация;

– позволяет обрабатывать различные типы значений: номинальные, непрерывные, дискретные;

– позволяет использовать для обучения наборы данных с пропущенной информацией;

– результат, полученный с использованием данного метода, может быть легко интерпретирован [1].

Целью данной работы является разработка метода повышения точности классификации с использованием деревьев решений путем построения ансамбля классификаторов.

Для построения дерева решений был использован алгоритм C4.5 [2]. Его идея заключается в следующем. Пусть задано некоторое множество T, содержащее объекты, каждый из которых характеризуется m атрибутами, причем один из них указывает на принадлежность объекта к определенному классу. Обозначим метки-классы через $C_1, C_2, \ldots, C_n$. Тогда возможны три ситуации:

1) Множество T содержит один или более примеров, относящихся к классу C_k. Тогда дерево решений для T – это лист, определяющий класс C_k.

2) Множество T не содержит ни одного примера, т.е. является пустым множеством. Тогда этот узел является листом, а класс, ассоциированный с листом, выбирается из другого множества, отличного от T, например из множества, ассоциированного с родителем.

3) Множество T содержит примеры, относящиеся к разным классам. В этом случае следует разбить множество T на некоторые подмножества по определенному критерию. Для этого выбирается один из признаков, имеющий два и более отличных друг от друга значений O_1, O_2, ..., O_n. Множество T разбивается на подмножества T_1, T_2, ..., T_n таким образом, что каждое подмножество T_i содержит все примеры, имеющие значение O_i выбранного признака. Эта процедура рекурсивно вызывается из каждого подмножества до тех пор, пока конечное множество не будет состоять из объектов, принадлежащих одному и тому же классу.

Разбиение производится таким образом, чтобы в узле было как можно больше объектов одного класса и как можно меньше объектов других классов.

Одним из методов повышения точности классификации является использование комбинаций классификаторов. Основная идея заключается в том, что вместо использования одного обученного и хорошо настроенного классификатора используется множество классификаторов, которые обучаются независимо друг от друга и так же независимо предоставляют свое решение относительно выходной переменной класси-

фицируемого примера. После этого их решения объединяются и на их основе формируется единственный ответ. Таким образом, данная система может быть рассмотрена как один классификатор.

В данной работе был построен ансамбль из десяти классификаторов C4.5. Для комбинирования ответов классификаторов был применен метод взвешенного голосования. Тестирование производилось на наборах данных Wine, Iris, Glass, Vehicle. Результаты тестирования представлены в табл. 1.

Таблица 1

Результаты эксперимента

Набор данных	C4.5		Ансамбль	
	Корректность	С.К.О	Корректность	С.К.О.
Wine 5	0,85	0,05	0,88	0,03
Wine 10	0,95	0,06	0,94	0,06
Iris 5	0,95	0,02	0,94	0,03
Iris 10	0,96	0,05	0,95	0,05
Glass 5	0,61	0,06	0,68	0,02
Glass 10	0,67	0,12	0,71	0,13
Vehicle 5	0,67	0,03	0,70	0,02
Vehicle 10	0,75	0,05	0,75	0,03

Числа 5 и 10 означают перекрестную проверку: набор данных разбивается на 5 или 10 частей, затем одна часть используется в качестве проверочной выборки, а остальные – в качестве обучающей выборки. Такая процедура повторяется до тех пор, пока не будет покрыт весь набор данных.

Как видно из таблицы, в целом ансамбль дает лучший результат по сравнению с одиночным классификатором. Локальные ухудшения могут быть связаны с тем, что количество классификаторов в ансамбле недостаточно велико для проведения объективного голосования. Возможны ситуации, когда несколько классификаторов с низким коэффициентом уверенности имели более значительное влияние, нежели классификатор с высоким коэффициентом уверенности (табл. 2).

Таблица 2

Уменьшение точности классификации

Вес классификатора	Класс A	Класс B	Класс C
0,43	0	1	0
0,95	1	0	0
0,47	0	1	0
0,45	0	1	0

В данном случае ансамбль примет решение, что объект принадлежит классу B, хотя на самом деле он принадлежит классу A.

Данный результат можно улучшить, применив другие методы агрегации, например нечеткий интеграл Шоке или Суджено [3], а также задействовав другие алгоритмы построения деревьев решений (ID3, CART).

Результатом исследования является доказанная целесообразность использования ансамблей классификаторов, т.к. даже с использованием простого оператора агрегации (взвешенное голосование) результат получается не хуже, чем у одиночного классификатора. Кроме того, имеются большие возможности для дальнейшего повышения точности, например использование различных алгоритмов классификации в одном ансамбле.

ЛИТЕРАТУРА

1. Rocak L., Maimon O. Data Mining with decision trees. World Scientific Publishing Co. Pte. Ltd, 2009. 244 с.

2. Quinlan J.R. C4.5: programs for machine learning [Текст]. Morgan Kaufmann Publishers Inc, 1993. 302 с.

3. Stevka D. Using fuzzy integral as an aggregation operator in dynamic classifier systems. Praha, 2013. 34 с.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ СЪЕМА ПОДПИСИ

Т.Ю. Дорошенко, студент, Е.Ю. Костюченко, доцент, к.т.н.

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

Разрабатываемое программное обеспечение представляет собой прототип системы аутентификации компьютерной системы по динамике подписи пользователя на графическом планшете. Цель работы – повышение надежности традиционной парольной защиты за счет использования многофакторной аутентификации на основе анализа динамики проставления подписи, проводимого с использованием аппаратов математической статистики и искусственных нейронных сетей.

Важным этапом решения задачи подтверждения подлинности динамической подписи является получение, анализ и хранение динамических характеристик (первичных параметров) подписей, проставляемых на графическом планшете. В связи с этим создан программный модуль для съема подписей.

Основные задачи, решаемые модулем:

− фиксация перемещений пера относительно чувствительной зоны планшета и перехват потока входных данных;

– динамическая отрисовка подписи на специальной панели в режиме реального времени;

– нормализация первичных параметров подписи;

– сохранение нормализованных первичных параметров подписи в базе данных.

Для обеспечения корректного функционирования системы съема подписи с множеством графических планшетов использован стандартизированный программный интерфейс – WinTab.

Алгоритм снятия подписи:

1) при вызове функции подписи – открытие контекста устройства ввода, передающего данные в цифровой форме непосредственно к приложению, без подготовки курсора;

2) каждый раз при возникновении события «Приход пакета», (каждые 5 мс, если перо находится в области действия планшета) вызвать обработчик событий, выполнить пункты 3–8;

3) получение серийного номера пакета, вызвавшего событие;

4) получение пакета с серийным номером пакета, вызвавшего событие;

5) нормализация данных пакета;

6) сохранение пакета в массив WintabPacket;

7) изображение точки на специальной панели;

8) при вызове функции сохранения подписи – закрытие контекста устройства ввода, увеличение счетчика массива.

По серийному номеру пакета извлекаются требуемые показатели: координаты положения пера, сила давления пера на поверхность планшета, угол пера по часовой стрелке и угол наклона пера относительно поверхности графического планшета, время снятия показателей.

Анализ снятых первичных характеристик показал, что в некоторых пакетах некорректно устанавливается штамп времени. Об этой же погрешности говорится и в статье П.С. Ложникова, А.В. Еременко [1]. Рассмотрим суть проблемы на примере используемого дигитайзера WACOM Intuos 3, имеющего частоту дискретизации, равную 200 Гц. Это означает, что когда перо находится в области чувствительности дигитайзера, все поступающие от него пакеты должны иметь штамп времени, кратный 5 мс. Однако в единичных случаях наблюдается отклонение этого значения (в отдельных случаях даже нарушается порядок следования пакетов по штампу времени). При этом можно заметить, что ошибка появляется именно в проставлении штампа – все остальные снимаемые характеристики не имеют скачков. Решено пренебречь данным параметром и при вычислении скоростей на отрезках дискретизации использовать заданную производителем частоту дис-

кретизации, равную 5 мс. При этом для упорядочивания пакетов использовать идентификатор пакета pktID.

Еще одной ошибкой (уже аппаратной части графического планшета) является периодическое одновременное (в одном пакете) проставление значений, больших, чем нуль, для параметров давления и координаты положения кончика пера над планшетом по оси *Z*. Это буквально бы значило, что перо не касается планшета, но оказывает на него давление, что невозможно.

Также особое внимание стоит уделить искажениям, вызванным невозможностью точного воспроизведения подписи одним человеком. К таким искажениям относятся:

– изменение геометрических размеров подписи;
– нестабильность времени воспроизведения подписи;
– изменение угла наклона подписи относительно системы координат.

Используемые алгоритмы для компенсации изменений описаны в автореферате диссертации [2].

При нормализации подписей перед их сохранением в базу данных решаются следующие задачи:

1) удаление нулевых (по параметру давления) значений пакетов в начале и в конце подписи, что предотвращает хранение «мусора» в базе данных, которое впоследствии может снизить информативность сигналов;
2) исправление ошибки «координата Z – давление»;
3) поворот подписи таким образом, чтобы она располагалась параллельно оси абсцисс;
4) нормализация по размеру.

Интерфейс главного окна программы представлен на рис. 1.

Рис. 1. Интерфейс главного окна программы

Реализованный модуль работает под операционной системой Windows. Работа выполнена с использованием среды разработки Microsoft Visual Studio 2010, языка программирования C# и платформы .NET, MySQL Connector, библиотеки WintabDN. Шаблоны для работы с библиотекой WintabDN взяты с электронного ресурса [3].

Следующим этапом работы будет получение вторичных характеристик подписи на основе исходных данных и реализация модуля для аутентификации.

Работа поддержана Министерством образования и науки, проект № 1220 «Фундаментальные основы проектирования информационно-безопасных систем».

ЛИТЕРАТУРА

1. Ложников П. С., Еременко А. В. Идентификация личности по рукописным паролям // Мир измерений. 2009. № 4(98). С. 11–17.

2. Сорокин И. А. Формирование системы признаков для идентификации личности по динамике воспроизведения подписи: автореф. дис. канд. техн. наук. Пенза, 2005. 22 с.

3. WintabDN-шаблоны [Электронный ресурс]. URL: http://sourceforge.net/projects/wintabdn/ (Дата обращения: 10.02.2014).

БАЗА ДАННЫХ ДЛЯ ХРАНЕНИЯ ПАРАМЕТРОВ ДИНАМИЧЕСКОЙ ПОДПИСИ

Т.Ю. Дорошенко, студент, Е.Ю. Костюченко, доцент, к.т.н.

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

Среди систем аутентификации большими перспективами обладают биометрические системы, основанные на поведенческой (динамической) характеристике человека и учитывающие особенности, характерные для подсознательных движений человека в процессе воспроизведения какого-либо действия. Разрабатываемое программное обеспечение представляет собой прототип системы аутентификации компьютерной системы по динамике подписи пользователя на графическом планшете. Цель работы – повышение надежности традиционной парольной защиты за счет использования многофакторной аутентификации на основе анализа динамики проставления подписи, проводимого с использованием аппаратов математической статистики и искусственных нейронных сетей.

Точность работы системы аутентификации зависит от размера пространства первичных и вторичных характеристик подписи. Количество первичных характеристик зависит от возможностей аппаратной составляющей системы и определяется количеством степеней свободы,

которое описывает число квазинепрерывных характеристик взаимного положения планшета и пера. Для обеспечения хранения характеристик эталонных подписей в одном месте и возможности удобного доступа к ним выполнено инфологическое проектирование и реализована база данных в СУБД MySQL [1]. База данных размещена на сервере кафедры КИБЭВС (93.91.166.75:3306).

Таблицы базы данных и атрибуты:

– пользователи: идентификатор пользователя (PK), фамилия, имя, отчество, дата рождения;

– подписи: идентификатор подписи (PK), идентификатор пользователя (FK), дата и время проставления подписи (проставляется в момент сохранения подписи по времени на сервере), комментарий;

– пакеты: идентификатор подписи (FK, PK), серийный номер пакета (PK), трехмерные координаты *X*, *Y*, *Z* кончика пера относительно планшета, сила нажатия (давление) пера на планшет, угол наклона пера относительно планшета и угол пера по часовой стрелке, временной штамп;

– названия параметров: идентификатор параметра (PK), имя параметра, описание параметра;

– значения параметров: идентификатор подписи (FK, PK), идентификатор параметра (FK, PK), номер гармоники (PK), значение параметра.

Концептуальная модель данных представлена на рис. 1.

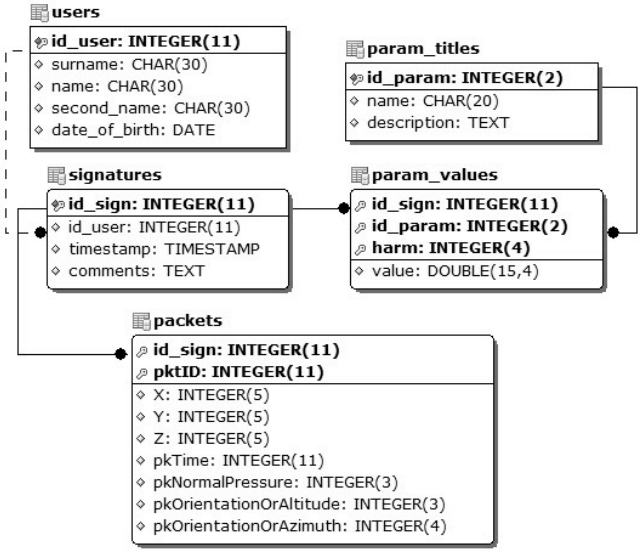


Рис. 1. Концептуальная модель данных

Предоставленные на уровне СУБД права доступа к базе данных: администраторам – полный доступ, пользователям – только INSERT.

В качестве основных характеристик любой биометрической системы принимают ошибки первого (FAR) и второго (FRR) рода. Первое число характеризует вероятность ложного совпадения биометрических характеристик двух людей, а второе – вероятность отказа доступа человеку, имеющему допуск. Таким образом, встает задача предварительной оценки точности определения ошибок первого и второго рода при идентификации пользователей по динамической подписи.

Из теории вероятностей доверительный интервал для оценки неизвестных вероятностей может быть построен по формуле (1) [2]:

$$p = \frac{n}{t^2+n}\left(\omega + \frac{t^2}{2n} \pm t\sqrt{\frac{\omega(1-\omega)}{n} + \left(\frac{t}{2n}\right)^2}\right). \qquad (1)$$

Здесь параметр t определяется уровнем доверительной вероятности на основе функции Лапласа. При уровне доверительной вероятности 0,95 параметр $t = 1, 96$.

Предварительная оценка частоты ошибок первого и второго рода может быть найдена исходя из анализа ошибок аналогов и составляет $\omega_1 = 0{,}01$ для ошибок первого рода и $\omega_2 = 0{,}01$ для ошибок второго рода.

Количество экспериментов по идентификации определяется объемом базы подписей и предварительно составляет 1300 экспериментов по оценке ошибок первого рода и 11700 экспериментов по оценке ошибок второго рода. На настоящий момент в базе содержится порядка 1000 подписей, число точек подписи составляет 1100–1400.

Подставляя эти данные в формулы, получаем предварительные границы доверительных интервалов для ошибок первого и второго рода: $p_1 \in [0{,}0058532; 0{,}0170341]$ и $p_2 \in [0{,}0083510; 0{,}0119706]$. Эти значения позволяют определять вероятность ошибок первого и второго рода с точностью до 0,00559045 и 0,0018098 соответственно.

В результате работы спроектирована и реализована база данных для хранения характеристик динамической подписи для проведения дальнейшего анализа, начато заполнение базы, получены предварительные оценки, позволяющие спрогнозировать порядок размаха доверительного интервала вероятностей ошибок первого и второго рода при дальнейшем эксперименте.

Работа поддержана Министерством образования и науки, проект № 1220 «Фундаментальные основы проектирования информационно-безопасных систем».

ЛИТЕРАТУРА

1. Кузнецов М.В., Симдянов И.В. MySQL 5. СПб.: БХВ-Петербург, 2006, 1024 с.: ил.; 24 см + 1 эл. опт. диск (CD-ROM)

2. Гмурман В.Е. Теория вероятностей и математическая статистика : учеб. пособие для вузов. 10-е изд., стер. М.: Высшая школа, 2004. 479 с.

ОЦЕНКА ЭФФЕКТИВНОСТИ ПАРАЛЛЕЛЬНОЙ РЕАЛИЗАЦИИ АЛГОРИТМА ПЧЕЛИНОЙ КОЛОНИИ ДЛЯ ИДЕНТИФИКАЦИИ ПАРАМЕТРОВ НЕЧЕТКОЙ СИСТЕМЫ

И.В. Горбунов, аспирант

Научный руководитель И.А. Ходашинский, профессор, д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, noby.Ardor@gmail.com

Постановка задачи. При разработке наукоемких приложений достаточно часто приходится отходить от шаблонов проектирования и стандартизированных процессов разработки программного обеспечения ввиду постоянных конфликтов – представления алгоритмов в науке в теоретико-множественном и/или математическом стиле часто противоречат лучшим практикам разработки в объектно-ориентированной парадигме [1].

Распараллеливание программного обеспечения включает в себя поиск алгоритмов, которые можно было бы свести к одному из следующим шаблонов:

- SIMD (Single Instruction–Multiple Data) – одинаковые преобразования выполняются на множестве несвязанных данных. Данный шаблон достаточно легко поддается параллельной реализации и в общем случае показывает наибольшую эффективность от параллельного исполнения.
- MIMD (Multiple Instructions – Multiple Data) – различные данные подвергаются различным преобразованиям, наиболее обобщённый шаблон. При реализации требуется постоянный контроль наличия средств синхронизации, так как различные инструкции выполняются за разное время. Эффективность параллельного выполнения такого шаблона ниже, но именно этот шаблон рекомендуется использовать при медленной сети между вычислительными ресурсами.
- MISD (Multiple Instructions –Single Data) – одни и те же данные подвергаются различным преобразованиям. Очень редко встречается в практике, наиболее эффективен при реализации на устройствах, сильно отличающихся по производительности, например CPU – GPU [2].

После нахождения шаблона в части алгоритма стоит проверить обязательное условие Бернстайна, смысл которого в том, что выходы и

входы частей алгоритма, подлежащие распараллеливанию, не должны пересекаться и выходы одной части не должны быть входом другой [3].

Введем в общие метрики качества параллельной реализации алгоритма

$$E(p)=\frac{t_{\text{пос}}}{p \bullet t_{\text{пар}}},$$

где $t_{\text{пос}}$ – время, затраченное на последовательное выполнение алгоритма; $t_{\text{пар}}$ – время, затраченное на последовательное выполнение алгоритма; p – количество вычислительных потоков [2].

Результаты работы. В данной работе будет описываться локально параллельный подход, применимый к многопроцессорным серверам, у которых каждый процессор многоядерный. Распараллеливанию подверглась реализация алгоритма вывода нечеткой системы синглтон [4] по шаблону SIMD, так как нечеткий аппроксиматор в процессе обучения с учителем по таблице наблюдения для вычисления ошибки работает над каждой строкой таблицы наблюдения независимо. Кроме указанного здесь шаблона, также был опробован шаблон MISD, каждое правило вычисляется в отдельном потоке для одной строки наблюдения, но ввиду того, что количество правил много меньше количества образцов, данный шаблон оказался менее эффективным по сравнению с SIMD во всех случаях. Наиболее эффективен данный подход при разделении таблицы наблюдения на величину количества_ядер (количество_вычислительных_потоков) – 1. Обозначим этот подход к распараллеливанию как A_1.

Далее был распараллелен алгоритм пчелиной колонии для идентификации параметров. Алгоритм представлен в статье [5]. Для каждого вида пчел был применен шаблон SIMD, так как они фактически не зависят друг от друга. Дальнейшее исследование показало, что рабочие пчелы и наблюдатели могут действовать независимо друг от друга это позволило свести их выполнение к шаблону MIMD. Обозначим использование SIMD-подхода к распараллеливанию как A_2, а MIMD – как A_3.

Эксперименты проводились на трех процессорах с разным количествам ядер и разной архитектурой.

В таблице приведены среднее время выполнения в секундах по 50 тестам (для нивелирования влияния фоновых процессов) и эффективность параллельной реализации при идентификации параметров аппроксиматора 1000 итераций алгоритма пчелиной колонии на тестовом наборе Ele-2 из репозитория KEEL.

Сравнение эффективности параллельной реализации

Вид паралелизации	i5-2410M (2,3 ГГц) $p = 4$		i7-3770K (3,5 ГГц) p=8		Opteon 6272 (2,1 Ггц) $p = 8$	
	t, сек	$E(p)$, %	t, сек	$E(p)$, %	t, сек	$E(p)$, %
Нет	912	25	534	12,5	2107	12,5
A_1	540	42,22	226	29,54	884	29,79
A_2	499	45,69	186	35,89	**560**	**47,03**
A_3	508	44,88	224	29,80	567	46,45
A_1+A_2	**365**	**62,47**	**159**	**41,98**	669	39,37
A_1+A_3	514	44,36	211	31,64	842	31,28

Анализ результатов. Как видно из таблицы, редко какая эффективность реализации превосходит 50%, однако не стоит забывать, что результаты получены на технологии hyper threading, которая добавляет потоки с учетом на конвейер внутри каждого ядра, но аппаратных ядер фактически так и остается в два раза меньше. Лучшим решением согласно результатам является модель A_1+A_2. На результат A_1+A_2 для Opteon 6272 повлияла особенность архитектуры процессора состоящего из двух отдельных блоков по 8 ядер, связанных более медленным кэшем 3-го уровня. Все варианты распараллеливания превосходят гипотезу Минского, а значит, являются эффективными.

Работа выполнена при финансовой поддержке РФФИ (Проект 12-07-00055).

ЛИТЕРАТУРА

1. Интеллектуальные высокопроизводительные программные комплексы моделирования сложных систем: концепция, архитектура и примеры реализации / А.В. Бухановский [и др.] // Известия высших учебных заведений. Приборостроение: ежемесячный научно-технический журнал / М-во образования и науки Рос. Федерации, Федер. агентство по образованию, СПбГУ ИТМО. СПб., 2009 . Т. 52, № 10. С. 5–24.

2. Карпов В.Е. Введение в распараллеливание алгоритмов и программ // Компьютерные исследования и моделирование. 2010. Т. 2, № 3. С. 231–272.

3. Wilkinson B., Allen M. Parallel programming techniques and applications using networked workstations and parallel computers. Pearson Education, 2005. 468 p.

4. Ходашинский И.А., Дудин П.А., Горбунов И.В. Алгоритмы муравьиной и пчелиной колонии для обучения нечетких систем // Доклады ТУСУРа. 2009. № 2 (20). С. 157–161.

5. Ходашинский И.А., Горбунов И.В. Оптимизация параметров нечетких систем на основе модифицированного алгоритма пчелиной колонии // Мехатроника, автоматизация, управление. 2012. №10. С. 15– 20.

ИНИЦИАЛИЗАЦИЯ НЕЧЕТКИХ СИСТЕМ НА ОСНОВЕ РЕЗУЛЬТАТОВ КЛАСТЕРИЗАЦИИ МЕТОДОМ *K* БЛИЖАЙШИХ СОСЕДЕЙ

Е.Н. Гусакова, аспирант
Научный руководитель И.А. Ходашинский, профессор, д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, rouxrenard@list.ru

Идентификацией нечеткой системы называется установление основных закономерностей между наборами входных и выходных переменных. Основными методами инициализации нечетких систем на основе таблиц наблюдений являются следующие методы: метод k средних [1], идентификация на основе регрессионных моделей [2] и др. В данной работе рассматривается метод инициализации, основанный на результатах кластеризации методом k ближайших соседей.

Описание алгоритма. Алгоритм k ближайших соседей является алгоритмом классификации, однако главный принцип данного алгоритма (объекты одного класса расположены ближе друг к другу, чем к объектам другого класса) [4] может быть использован и в алгоритме кластеризации. В качестве исходных данных для кластеризации используется таблица наблюдений, где каждый элемент представляет собой вектор значений параметров и класс элемента. Также в качестве исходных данных используются следующие параметры: q – минимальное число объектов, являющихся соседями для объектов одного кластера; R – радиус поиска соседей; k – число соседей. Алгоритм кластеризации представлен ниже.

Шаг 1. Для каждого объекта из таблицы наблюдений выбираются все объекты, евклидово расстояние до которых $\leq R$. Из них выбираются k объектов, которые ближе всего. Если у объекта число соседей, расстояние до которых $\leq R$, меньше k, то они все считаются соседями.

Шаг 2. Для каждой пары объектов Z_i и Y_i, кластеры которых не определены, выбираем k – минимальное число соседей, имеющееся у каждого из этих объектов. Если $k–q$ и более соседей Z_i и Y_i совпадают, помечаем их и их совпадающие соседи меткой одного кластера. Если соседи не совпадают, переходим к следующей паре объектов.

Шаг 3. Каждому из объектов, кластер которых не определен, выбираем k ближайших соседей объекта и помечаем его меткой того кластера, к которому относится большая часть его соседей. В этом случае возможны следующие варианты:

а) а) соседи в равной степени относятся к разным кластерам. В этом случае добавляем объект к тому кластеру, центр которого меньше сместится в случае его добавления;

б) соседи не отнесены ни к одному из кластеров: тогда точку и ее соседей помечаем как относящихся к новому кластеру.

Шаг 4. Если остались точки с неопределенным кластером, помечаем их меткой нового кластера.

Шаг 5. Каждому из полученных кластеров поставить в соответствие один из классов. Для этого для каждого кластера C выбирается класс A, если объектов класса A больше всего в данном кластере.

Шаг 6. Выбираем два кластера. Для каждого из них считаем расстояние между двумя максимально удаленными объектами кластера: $d_{\max i} = \max(x_i)$. Считаем расстояние D между кластерами: минимальное расстояние между объектами из разных кластеров. Если $D > d_{\max 1}$ и $D > d_{\max 2}$ и оба кластера относятся к одному классу, то объединяем кластеры.

В результате работы алгоритма получаем C кластеров, каждый из которых соответствует одному лингвистическому правилу базы правил нечеткой системы. Далее определяются центры кластеров. Вектор центр кластера вычисляется следующим образом:

$$v_k = \frac{\sum_{i=1}^{K} r_i}{K}.$$

В результате получаем матрицу центров кластеров $V = \{v_1, v_2, \dots v_m\}$, где каждое $v_k = \{v_{k1}, v_{k2} \dots v_{kn}, v_{(kn+1)}\}$, где v_{ki} – значение i-й координаты в k-м кластере; $v_{(kn+1)}$ – значение координаты выходной переменной в k -м кластере.

Кроме центров кластеров вычисляются также векторы границ кластеров:

$U = \{\min_{i\in[1;K]} r_{1i}, \min_{i\in[1;K]} r_{2i} \dots \min_{i\in[1;K]} r_{mi}\}$ – левая граница;

$W = \{\max_{i\in[1;K]} r_{1i}, \max_{i\in[1;K]} r_{2i} \dots \max_{i\in[1;K]} r_{mi}\}$ – правая граница.

Каждый выделенный кластер соответствует одному лингвистическому правилу базы правил. Каждый лингвистический терм, находящийся в антецеденте нечетких правил, задается своей функцией принадлежности. В качестве функции принадлежности выбрана треугольная функция, которая описывается формулой

$$\mu(x) = \begin{cases} 1 - \dfrac{v - x}{v - u}, u \le x \le v, \\ 1 - \dfrac{x - v}{w - v}, v \le x \le w, \\ 0, \text{в прочих случаях.} \end{cases}$$

Таким образом, для каждого k-го кластера получаем набор функций

$$\mu_k(x) = [\mu_{k1}(x), \mu_{k2}(x) \dots \mu_{km}(x)].$$

После построения функций принадлежности формируем правила нечеткой базы.

Результаты эксперимента. В качестве тестовых данных использовались данные keel: Iris, NewThyroid, Wine. В табл. 1–3 представлены результаты кластеризации на этих наборах данных.

Таблица 1

Результаты кластеризации (Iris)

Класс	Кол-во элементов в кластере 1	Кол-во элементов в кластере 2	Кол-во элементов в кластере 3
iris-setosa	50	0	0
iris-versicolor	0	45	5
iris-virginica	0	1	49

Таблица 2

Результаты кластеризации (NewThyroid)

Класс	Кол-во элементов в кластере 1	Кол-во элементов в кластере 2	Кол-во элементов в кластере 3
1	0	150	0
2	16	19	0
3	0	8	22

Таблица 3

Результаты кластеризации (Wine)

Класс	Кол-во элементов в кластере 1	Кол-во элементов в кластере 2	Кол-во элементов в кластере 3
1	54	0	5
2	4	45	22
3	5	12	31

В качестве примера приведем нечеткую систему, построенную на основе результатов кластеризации для набора данных Iris. База правил данной нечеткой системы выглядит следующим образом:

ЕСЛИ SepalLength = A_1 И SepalWidth = B_3 И PetalLength = C_1 И PetalWidth = D_1
ТО Класс = iris-setosa
ЕСЛИ SepalLength = A_2 И SepalWidth = B_1 И PetalLength = C_2 И PetalWidth = D_2
ТО Класс = iris-versicolor
ЕСЛИ SepalLength = A_3 И SepalWidth = B_2 И PetalLength = C_3 И PetalWidth = D_3
ТО Класс = iris-virginica

где A_i, B_i, C_i и D_i – функции принадлежности для различных параметров. Нечеткая система, построенная на данных результатах кластеризации, правильно классифицирует 82,667% на обучающей выборке и 84% на тестовой выборке.

Заключение. Результаты экспериментов показывают, что на основе результатов кластеризации методом k ближайших соседей могут быть получены нечеткие системы, дающие довольно высокие резуль-

таты классификации. Преимуществом таких нечетких систем является их высокая интерпретируемость: так как каждому классу соответствует лишь один кластер, то количество правил в итоговой базе правил будет соответствовать числу классов.

ЛИТЕРАТУРА

1. Ходашинский И.А. Идентификация нечетких систем: методы и алгоритмы // Проблемы управления. 2009. № 4. С. 15–23.

2. Штовба С.Д. Нечеткая идентификация на основе регрессионных моделей параметрической функции принадлежности // Проблемы управления и информатики. 2006. №6. С. 38–44.

3. Дубинин А.А. Нечеткое моделирование сложных систем на основе прямого и обратного логического вывода: дис. … канд. техн. наук. 05.13.01. Воронеж, 2011. 152 с.

4. Воронцов К.В. Лекции по метрическим алгоритмам классификации. М.: МФТИ, 2007. 14 с. Режим доступа: www.ccas.ru/voron/download/MetricAlgs.pdf

ВЫБОР ПОРОГА РАЗЛИЧИЯ ПРИ СЕГМЕНТАЦИИ РЕЧЕВОГО СИГНАЛА НА ВОКАЛИЗОВАННЫЕ И НЕВОКАЛИЗОВАННЫЕ СЕГМЕНТЫ

К.С. Крючков, студент

Научный руководитель Е.Ю. Костюченко, доцент, к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, kruchkoff.k@gmail.com

Сегментация речевого сигнала является одной из важнейших задач в системах обработки речевого сигнала и представляет собой процесс поиска границ между элементами речевого сообщения: фразами, словами, слогами, фонемами. Использование сегментации на вокализованные и невокализованные участки позволяет в дальнейшем применять различные алгоритмы при обработке звуков различных классов.

Различают два способа сегментации: автоматическую и ручную. Ручная сегментация может быть использована при исследовании и анализе единичных сигналов, т.к. требует значительных затрат сил и времени, к тому же ее результаты субъективны и практически не могут быть достоверно воспроизведены. Автоматическая сегментация не лишена своих минусов, однако уже может быть использована при обработке речевого сигнала в режиме реального времени, а также дает воспроизводимые результаты [1].

В данной работе был проанализирован алгоритм сегментации речевого сигнала на основе поиска периодической структуры сигнала

при помощи сверток набора масок и исходного сигнала [2]. Предложенный автором алгоритм состоит из трех шагов:

1) определение наличия периодической структуры на дискретном временном отсчете;
2) определение границ сегментов;
3) устранение ошибочно проставленных границ.

Для определения наличия периодической структуры применяется свертка речевого сигнала с набором масок на каждом временном отсчете, представляющем собой частотный срез речевого сигнала после одновременной маскировки для различных частот основного тона. Набор масок может быть сформирован аналитически. После одновременной маскировки сигнал и маски имеют двоичный формат, что позволят вычислить меру различия между ними по формуле

$$d(k_0, t) = \sum_k P_0(k, t) \oplus P_м(k, k_o),$$

где $P_0(k, t)$ – анализируемый речевой сигнал после одновременной маскировки, а $P_м(k, k_0)$ – набор масок для определения периодической структуры сигнала [2, 3]. Если мера различия превышает некоторый установленный порог, то сегмент признается невокализованным и вокализованным в противном случае. Данная работа посвящена исследованию зависимости количества ошибок сегментации от величины порога с целью выбора его оптимального значения. Под оптимальным, в данном случае, подразумевается такое значение порога, при котором количество ошибок минимально.

В ходе работы рассмотрено три типа ошибок: ошибки первого рода, ошибки второго рода и ошибки точности, которые представляют собой пропуск границы сегмента, простановку лишней границы, а так же ситуацию, когда границы сегмента определены правильно, однако разница между значением, полученным в результате ручной сегментации, и значением, полученным в результате автоматической сегментации, больше некоторого порогового значение ε.

Величина порога сравнения изменялась в диапазоне от 2 до 12. Графики зависимости количества ошибок сегментации в процентном отношении от величины порога представлены на рис. 1–3.

Из полученных экспериментальных данных видно, что с ростом величины порога до значения 10 растет количество ошибок второго рода. Минимум количества ошибок первого рода приходится на величины порога 12 и 7, а минимум ошибок точности достигается при пороге сегментации 7.

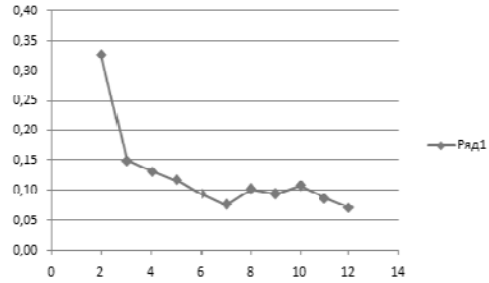


Рис. 1. График зависимости ошибки первого рода от величины порога

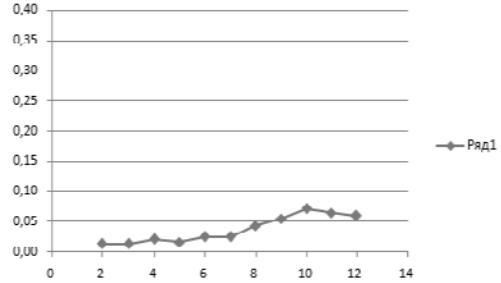


Рис. 2. График зависимости ошибки второго рода от величины порога

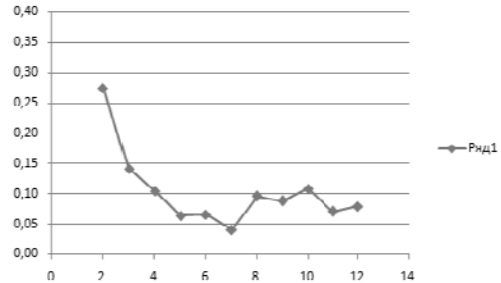


Рис. 3. График зависимости ошибки точности от величины порога

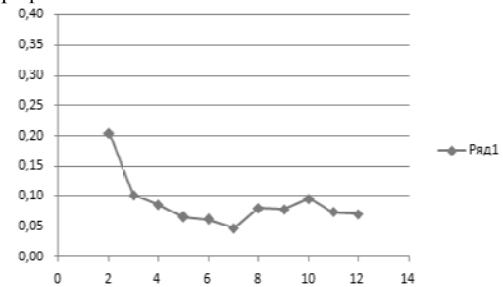


Рис. 4. График зависимости суммарной ошибки от величины порога

Минимум суммарной ошибки достигается при значении порога равном 7, что делает данное значение оптимальной величиной порога, при неизменности остальных параметров, в исследуемом алгоритме сегментации.

ЛИТЕРАТУРА

1. Сорокин В.Н., Цыплихин А.И. Сегментация и распознавание гласных // Информационные процессы. 2000. Т. 4, №2. С. 202–220.

2. Конев А.А. Модель и алгоритмы анализа и сегментации речевого сигнала: автореф. дис. … канд. техн. наук. М., 2007.

3. Конев А.А., Мещеряков Р.В. Алгоритм сегментации речевого сигнала на вокализованные и невокализованные участки // Сб. тр. XIX сессии Российского акустического общества. Т. III. М.: ГЕОС, 2007. С. 56–60.

ПРИОБРЕТЕНИЕ МЕДИЦИНСКИХ ЗНАНИЙ В МЕДИЦИНСКОЙ ЭКСПЕРТНОЙ СИСТЕМЕ ДИФФЕРЕНЦИАЛЬНОЙ ДИАГНОСТИКИ

Н.В. Ле[1], О.А. Трушкина

Научный консультант Д.П. Панченко

Научный руководитель В.А. Камаев, профессор каф. «САПР и ПК», д.т.н. г. Волгоград, ВолгГТУ; nvien.vstu@gmail.com1

При проектировании экспертной медицинской системы диагностики в качестве источника знаний выступают знания и опыт группы врачей – закономерности области диагностики, полученные в результате практической деятельности и профессионального опыта. Для представления знаний выбрано сочетание фреймовой и нечетко-продукционной моделей. Фреймовая модель предназначена для представления статических знаний о текущем состоянии области диагностики. Нечетко-продукционная модель предназначена для представления динамических знаний о переходах между состояниями области диагностики [1]. По методологии построения экспертных систем одна важная задача заключается в приобретении знаний [2]. Приобретение медицинских знаний – это процесс получения необходимых знаний от экспертов-врачей и накопления их с целью дальнейшего использования. Приобретение знаний состоит из 4 этапов: построение базы знаний; извлечение знаний из отправленных анкет; обучение нечетких баз знаний; проверка базы знаний.

Построение базы знаний. Врачи с участием инженера по знаниям описывают область медицинской диагностики и диагностическое состояние в виде гибридной модели представления знаний. *Формализация гибридной модели* представления знаний является подготови-

тельным этапом. Инженер по знаниям создает фреймовую и нечетко-продукционную модели представления знаний.

На этапе *формирования фреймовой иерархии* врачи описывают текущее состояние области диагностики следующим образом: определение специальностей, заболеваний, групп симптомов, симптомов; создание взаимодействий между объектами области; отображение количественных оценок поступающих симптомов и количественной интегральной оценки каждого заболевания.

На этапе *формирования нечетко-продукционных правил* врачи описывают переходы между состояниями области диагностики следующим образом: описание входных и выходных переменных (симптомов и заболеваний); задание функций принадлежности для созданных переменных; создание нечетко-продукционных правил.

Извлечение знаний из отправленных анкет. Данный подход основан на формировании ответов на электронное письмо, отправленное пациентом, согласно подготовленной анкете, и выделении из них новых знаний, характеризующих его содержание. В качестве источника знаний выступает диагностическое решение, сформированное врачам для медицинской консультации, в которой система не могла поставить конечный диагноз. *Формирование подготовленной анкеты* является подготовительным этапом. Для этого задается перечень понятий, необходимых для описания структуры анкеты (возможная специальность; вопросы-ответы и др., затем формируется иерархия понятий на основании их связей.

На этапе *заполнения анкеты и отправления врачам* все поля анкеты заполняются информацией медицинской диагностики. Затем анкета в письме отправляется врачам по возможной специальности.

На этапе *получения письма и формирования ответов на вопросы* врач решает принимать письмо и отвечать на вопросы. Отвеченное письмо отправляется пациенту на его электронную почту.

На этапе *формирования новых нечетко-продукционных правил* происходит сопоставление отвеченных анкет с базой знаний для извлечения новых фактов, которые сохраняются в виде правила.

Обучение нечетких баз знаний. Для повышения эффективности обучения нечетко-продукционной модели представления знаний, решающей задачу формирования базы знаний, предлагается использование генетического алгоритма [3]. Для этого первым необходимо задавать способ *кодирования/декодирования нечетко-продукционной модели представления знаний*, которая определяет некоторые параметры (параметры функции принадлежности; коэффициенты специфичности и уверенности), которые сводятся в единственный вектор. Значение одного параметра лежит в определенной окрестности, которую можно

разбить на 2^16 интервалов. Затем для кодирования номера интервала можно использовать 16-битовое значение в коде Грея, при котором соседние числа отличаются меньшим количеством позиций.

Для *создания начальной популяции хромосом* случайным образом выполняется генерация 100 хромосом с начальной инициализацией значений генов в заданной окрестности, используя метод гауссиан. Затем с использованием операции композиции объединить набор генов в единую хромосому для оценки приспособленности хромосом.

Каждой хромосоме из популяции ставится в соответствие *оценка ее приспособленности в популяции*, вычисление которой выполняется на основании обучающих выборок и векторов параметров модели. Процесс обучения считается законченным, если выполняется условие того, что полученная оценка больше порогового значения.

Селекция хромосом. В процедуре селекции, основанной на принципе колеса рулетки, чем больше секторы на колесе рулетки (т.е. соответствующая оценка приспособленности хромосомы), тем выше шанс, что выбрана именно эта хромосома, к которой в дальнейшем после выполнения операции декомпозиции применяются генетические операторы для создания потомков для следующей популяции.

Применение генетических операторов к хромосомам. В генетических алгоритмах за передачу генов родителей потомкам отвечает оператор скрещивания (вероятность 90%). Операторы мутации и инверсии (вероятность 10%) предназначены для того, чтобы поддерживать разнообразие хромосом в популяции.

Формирование новой популяции. Результативные хромосомы необходимо поместить в популяцию после выполнения операции композиции. Для сокращения популяции до исходного числа хромосом применяется оператор редукции.

После останова работы генетического алгоритма получается обученная модель, аппроксимирующая с заданной точностью данные из обучающей выборки и формирующая базу знаний, состоящую из системы нечетко-продукционных правил.

Проверка базы знаний предназначена для оценки полноты и целостности базы знаний по тестирующей выборке [2].

Заключение. В результате работы предложены основные этапы приобретения медицинских знаний: построение базы знаний; извлечение знаний из отправленных анкет, обучение нечетких баз знаний, проверка базы знаний. Построение базы знаний предназначено для формализации гибридной модели представления знаний, а также формирования фреймовой иерархии и нечетко-продукционных правил. Извлечение знаний из отправленных анкет предназначено для формирования новых правил на основании диагностических ответов на элек-

тронное письмо пациента. Предполагается генетический алгоритм для обучения нечетких баз знаний с целью тонкой настройки коэффициентов и параметров в нечеткой базе знаний.

ЛИТЕРАТУРА

1. Сошников Д.В. Инструментарий JULIA для построения распределенных интеллектуальных систем па основе продукционно-фреймового представления знаний // Труды МАИ. М.: МАИ, 2002. №7.

2. Статические и динамические экспертные системы: учеб. пособие / Э.В. Попов, И.Б. Фоминых, Е.Б. Кисель, М.Д. Шапот. М.: Финансы и статистика, 1996. 320 с.

3. Митюшкин Ю.И., Мокин Б.И., Ротштейн А.П. Soft-Computing: идентификация закономерностей нечеткими базами знаний. Винница: УНІВЕРСУМ-Вінниця, 2002. 145 с.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ НЕЧЕТКИХ СИСТЕМ НА ОСНОВЕ СОЦИАЛЬНОГО АЛГОРИТМА

М.А. Мех, студент

Научный руководитель И.А. Ходашинский, профессор, д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС maxcimkj93@gmail.com

Проект ГПО КИБЭВС-1211 – «Нечёткие системы»

Аппроксимация на основе таблиц наблюдений является актуальной задачей для многих сфер как исследовательской, так и производственной деятельности. Существует множество методов построения аппроксимирующей модели, в том числе и построение нечеткого аппроксиматора. Целью данной работы является исследование алгоритма оптимизации параметров нечеткого аппроксиматора метаэвристическим алгоритмом, основанным на имитации социальных процессов.

Описание нечеткой системы. Построение нечеткой системы осуществляется на основе таблицы наблюдений: $T = \{t_1, t_2, \ldots, t_M\}$, где $t_k = (x_k, y_k)$, где $x_k = [x_{k1}, x_{k2}, \ldots, x_{kn}]$ – вектор входных значений, y_k – выходное значение, M – число наблюдений, n – число входных переменных.

На основе таблицы наблюдений для каждой переменной определяются лингвистические термы, разбивающие область значений. В данной работе каждый терм определяется 3 точками. Исходя из разбиения переменных на нечеткие множества, формируется база правил нечеткой системы. Нечеткое е-правило в системе типа синглтон имеет вид

$$\text{IF } x_1=A_{1i} \text{ AND } x_2=A_{2i} \text{ AND } \ldots \text{ AND } x_n=A_{ni} \text{ THEN } y = r_i,$$

где r_j – действительное число, которым оценивается выход y; A_{ji} – j-й терм i-го правила. На основе сформированной базы правил нечеткая система осуществляет отображение $F: \mathbb{R}^n \rightarrow \mathbb{R}$, отображение определяется формулой: $F(x) = \frac{\sum_{i=1}^{m} \mu_{A1i}(x_1)\mu_{A2i}(x_2)\ldots\mu_{Ani}(x_n) r_i}{\sum_{i=1}^{m} \mu_{A1i}(x_1)\mu_{A2i}(x_2)\ldots\mu_{Ani}(x_n)}$, где $x = [x_1, \ldots, x_n]^T \in \mathbb{R}^n$; m – число правил нечеткой модели; μ_{Aji} – функция принадлежности, указывающая степень принадлежности x_j к множеству Aji. Параметры нечеткой системы хранятся в виде вектора $V = [s_{11i}, s_{21i}, s_{31i}, \ldots, r_1, r_2, \ldots, r_m]$, где S_{lij} – l-й параметр i-го терма j-й переменной. Ошибка вывода результатов нечеткого аппроксиматора оценивает параметры нечеткой системы и вычисляется по формуле: $RMSE = \frac{1}{M}\sqrt{\sum_{j=1}^{M}(y_j - F(x_j))^2}$. Оптимизация параметров заключается в поиске набора параметров нечеткой системы, удовлетворяющего минимальному значению функции ошибки.

Описание алгоритма оптимизации. Ход вычислений:

Шаг 1. Формирование популяций, группировка популяций, определение лидеров в популяциях, в группах.

На данном этапе для каждого вектора вычисляется значение ошибки RMSE. Значения сортируются, количество векторов, равное N_p, имеющих минимальное значение ошибки, выбираются как лидеры. Значения целевой функции для лидеров нормируются. В зависимости от NC_i для каждого лидера вычисляется потенциал по формуле: $U_i = \frac{NC_i}{\sum_{i=1}^{N_p} NC_i}$, где NC_i – нормированное значение RMSE лидеров. На основе потенциала определяется количество векторов в популяции лидера по формуле $Count_i = round(U_i * N_p)$, где $Count_i$ – количество векторов в популяции i-го лидера. Следующим шагом согласно вычисленному размеру для каждого лидера формируются популяции. Вычисляется вес каждой из популяций:

$$FC_i = F(L_i) + \xi \frac{1}{Count_i} \sum_{j=1}^{Count_i - 1} F(V_j),$$

где ξ – константа (обычно порядка 0,1); L_i – вектор-лидер i-й популяции. Популяции с наименьшим значением веса определяются как лидеры. Вес популяций-лидеров нормируется и вычисляется потенциал обладания. На основе потенциала определяется количество популяций в каждой группе и происходит формирование групп из множества популяций.

Шаг 2. Поиск с помощью генетического алгоритма.

Шаг 3. Ассимиляция групп популяций.

Шаги с 3.1–3.4. Повторяются для каждой группы популяций.

Шаг 3.1. Ассимиляция векторов в популяциях.

Ассимиляция заключается в приближении векторов к вектору-лидеру в популяции на величину X с отклонением Θ, где X – случайная величина, распределенная по закону $U(0, \beta * d)$, $\beta > 0$ – коэффициент ассимиляции; Θ – угол отклонения распределен по закону $U(-\gamma, \gamma)$; γ – заданный параметр; d_{ij} – дистанция между вектором $\mathbf{V}_i$ из популяции и вектором-лидером $\mathbf{L}_j$, вычисляется как евклидово расстояние.

Шаг 3.2. Революция в популяциях.

Операцией революции обозначают процесс случайного изменения позиции вектора в популяции с определенной вероятностью.

Шаг 3.3. Ассимялиция в группах.

Изменение позиции популяции внутри группы осуществляется путем движения векторов популяций в направлении вектора-лидера ведущей популяции в группе.

Шаг 3.4. Революция в группах.

Процесс случайного изменения позиции популяции в группе с определенной вероятностью.

Шаг 3.5. Изменение позиций.

Перевычисление *RMSE* векторов, переопределение лидеров.

Шаг 3.6. Определение и исключение слабейших популяций.

Вычисляется вес групп популяций, определяется группа с наибольшим весом и одна из ее популяций разыгрывается между другими группами. Определяется вектор $\mathbf{W}=[CS_1, CS_2, \ldots, CS_{N_{gp}-1}]$, где CS_i – потенциал владения популяций для i-й группы, N_{gp} – кол-во групп. Далее создается вектор $\mathbf{H}$ размерностью $N_{gp} - 1$ и заполняется значениями, распределенными по закону $U(0,1)$. Финальный вектор $\mathbf{D}= \mathbf{W}-\mathbf{H}$. Группа, имеющая наибольшее значение вектора $\mathbf{D}$, получает разыгрываемую популяцию. Группы популяций, потерявшие все популяции, устраняются из алгоритма.

Шаг 4. Повторение шагов 2–3 в зависимости от количества итераций.

ЛИТЕРАТУРА

1. Ходашинский И.А., Дудин П.А. Идентификация нечетких систем на основе непрерывного алгоритма муравьиной колонии // Автометрия. 2012. Т. 48, № 1. С. 63–71.

2. Fatemeh Ramezani. Shahriar Lotfi Social-Based Algorithm (SBA) // Applied Soft Computing. 2012. P. 1–13.

3. Esmaeil Atashpaz-Gargari, Caro Lucas. Imperialist Competitive Algorithm: An Algorithm for Optimization Inspired by Imperialistic Competition // IEEE. 2007. P. 8.

ПОСТРОЕНИЕ НЕЧЕТКОГО КЛАССИФИКАТОРА НА ОСНОВЕ ПОПУЛЯЦИОННОГО АЛГОРИТМА «КУКУШКИН ПОИСК»

Д.Ю. Минина, студентка 5-го курса каф. КИБЭВС
Научный руководитель И.А. Ходашинский, профессор, д.т.н.
г. Томск, ТУСУР, pound_2007@mail.ru

Моделирование сложных систем осложняется проблемой неточного или неполного описания изучаемого объекта. Одним из решений такой проблемы является нечеткое моделирование. В данной работе рассматривается нечеткий классификатор (основанный на нечеткой логике). Классификация рассматривается как процесс определения некоторого класса объекта исследования в соответствии с какими-либо характерными признаками, которые определяются путем обнаружения связей между имеющимися наборами данных, исходя из которых будет проводиться классификация.

Обработка информации в нечеткой системе осуществляется при помощи базы правил. Каждое правило содержит условную и заключительную часть. Антецедент (IF-часть) включает в себя утверждение, относящееся ко входным параметрам, консеквент (THEN-часть) указывает значение выходной переменной – название класса.

Для создания нечетких классификаторов используются хорошо изученные классические методы, и метаэвристические, которые менее точны, но зачастую эффективнее первых при решении нелинейных, многокритериальных задач оптимизации с ограничениями.

Алгоритм. Рассматривается малоизученный популяционный алгоритм оптимизации «кукушкин поиск». Его суть построена на основе модели способа размножения кукушки с ее способностью находить недавно построенные гнезда и подкладывать в них свои яйца, которые в итоге могут быть выкинутым хозяином гнезда.

Каждое гнездо является решением. Качество решения (пригодность гнезда) улучшается путем порождения нового решения из существующего и замещения «плохих» гнезд на новые. Количество решений остается фиксированным в каждом поколении.

Приводится описание пошагового алгоритма.

Шаг 1. Инициализация исходной популяции.

Задается популяция фиксированного размера. Каждый элемент популяции представляет собой вектор в виде массива, который состоит из необходимого для описания одного состояния нечеткой системы количества переменных (количество входных переменных нечеткой системы, умноженное на количество переменных, описывающих каждую функцию принадлежности, умноженное на количество функций принадлежности для одной переменной).

Каждая функция принадлежности в каждом векторе задается случайным образом в заданных границах диапазона с учетом того, что левая граница каждой последующей функции принадлежности отдельной переменной должна находиться правее левой границы предыдущей функции принадлежности.

Задается «начальное положение кукушки», т.е. задается случайный вектор, который является текущим решением.

Задается вероятность, с которой гнездо может быть «покинуто» хозяином, т.е. вероятность удаления вектора из множества популяции.

Задается количество итераций для работы алгоритма в качестве критерия остановки.

Шаг 2. Генерация нового решения на основе полетов Леви.

Выполняется «случайное перемещение кукушки», которое выражено изменением текущего вектора решения по закону Леви.

Случайным образом выбирается другое решение (вектор из текущей популяции).

Шаг 3. Оценка качества решения.

Сравниваются значения фитнес-функций, вычисленных на основе среднеквадратичной ошибки, для данных векторов (текущего вектора и случайно выбранного).

В случае если фитнес-функция вектора текущего решения «лучше», то заменяем случайно выбранное решение на «кукушкино» (текущее).

Шаг 4. Удаление «неудачных гнезд» (решений).

Выбирается заранее заданное количество «худших» решений (с наибольшим значением среднеквадратичной ошибки), для каждого из которых генерируется случайная вероятность. Если значение случайной вероятности оказывается больше заранее заданной, то гнездо удаляется (удаляется вектор решения).

Вместо удаленных векторов генерируется новый, по правилам шага 1 (и далее повторяются все шаги).

Шаг 5. Итерации продолжаются заданное количество раз.

Эксперимент. Данный алгоритм применен для построения нечеткого классификатора. Эксперимент проводился на данных из репозитория www.keel.es. Результаты тестов сравнивались с публикацией [3], где проводились аналогичные эксперименты на тех же данных. В таблице приведены результаты сравнения классификации ирисов – классической задачи классификации, с которой начинают тестирование нечеткого классификатора.

Набор данных содержит 3 класса цветков ириса: Iris Setosa (Ирис щетинистый), Iris Versicolour (Ирис разноцветный) и Iris Virginica (Ирис вирджиника). Каждому классу соответствует 50 записей. Также

набор данных содержит 4 атрибута, по которым определяется класс, это: длинна чашелистика, ширина чашелистика, длина лепестка и ширина лепестка.

Результаты сравнения работы созданного классификатора с зарубежными аналогами

Набор данных	Среднее (обучающая выборка)	СКО	Среднее (тестовая выборка)	СКО
Ant Miner	97,26	0,74	96,00	3,37
Core	95,48	1,42	92,67	4,67
Thrift	97,48	0,36	**96,67**	3,33
Hider	97,33	0,36	**96,67**	3,33
Sgerd	93,50	2,42	92,93	4,33
Алгоритм «кукушкин поиск»	**98,83**	0,41	94	5,73

В работе алгоритм описан математически, приведены более подробные описания экспериментов.

ЛИТЕРАТУРА

1. Ходашинский И.А., Дудин П.А. Идентификация нечетких систем на основе непрерывного алгоритма муравьиной колонии // Автометрия. 2012. Т. 48, № 1. С. 63–71.

2. Kaveh A., Bakhshpoori T., Ashoory M. An efficient optimization procedure based on cuckoo search algorithm for practical design of steel structures // International Journal of Optimization in Civil Engineering. 2012. № 2. P. 1–14.

3. KEEL Data-mining software Tool: data, set repository, integration of algorithms and experimental analysis framework / J. Alcala-Fdez, A. Fernandez, J. Luengo et al. // J. of Mult.-Valued Logic & Soft Computing. 2011. Vol. 17. P. 255–287.

АВТОМАТИЧЕСКОЕ РАСПОЗНАВАНИЕ МУЗЫКАЛЬНЫХ НОТ

А.А. Онищенко, студент каф. КИБЭВС

Руководитель А.А. Конев, доцент каф. КИБЭВС

г. Томск, ТУСУР, _o_s_a_@bk.ru

Перед многими непрофессиональными музыкантами стоит проблема перевода своего вокального и музыкального творчества в партитуры (ноты), соответствующие правилам сольфеджио (нотной грамо-

ты). Автоматическое распознавание звучащих нот при помощи специального программного обеспечения позволило бы ускорить и повысить удобство записи партитур.

Каждой музыкальной ноте соответствует определенная частота. Фактически соответствующая ноте частота – это частота основного тона звукового сигнала. Интересен тот факт, что это утверждение не может быть обратимо – существуют некоторые частоты, которым не соответствуют ноты. Это накладывает некоторые сложности в распознавании нот. Соотношение между музыкальными нотами и соответствующими им частотами приведено, например, в [1]. Еще одной проблемой являются особенности человеческого голоса. Наш голос в отличие от инструментов выдает ноты с некоторыми погрешностями, и конечно у разных людей погрешности отличаются. Это зависит от пола, возраста и степени владения голосом. Необходимо учесть и то, что нужно отслеживать не только сами ноты, но и их длительности и длительности пауз, т.к. этому тоже соответствуют правила сольфеджио. Немалую роль играет качество обрабатываемой записи.

По результатам исследовательской работы для получения параметров речевого сигнала, необходимых для вычисления частоты тонов, использовался программный комплекс, реализующий модель периферической части слуховой системы человека. Этапы обработки сигнала с использованием программного комплекса:

– предварительная фильтрация, позволяющая получить параметры речевого сигнала, одновременная маскировка;

– сегментация речевого сигнала на вокализованные и невокализованные участки;

– определение каналов фильтрации, соответствующих гармоникам вокализованных участков и определение значений частоты и интенсивности этих гармоник.

Далее представлен разработанный алгоритм распознавания музыкальных нот (рис. 1):

A /B – начало/конец ноты;

MinDuration – минимальная длительность ноты;

Det – диапазон ноты/2;

Line – строка из файла;

Note() – функция определения принадлежности частоты к ноте;

notes /note – массив найденных нот/ноты из массива notes;

NOTESN – массив нот после проверки на минимальную длительность;

SeqFilter() – функция фильтрации «лишних нот».

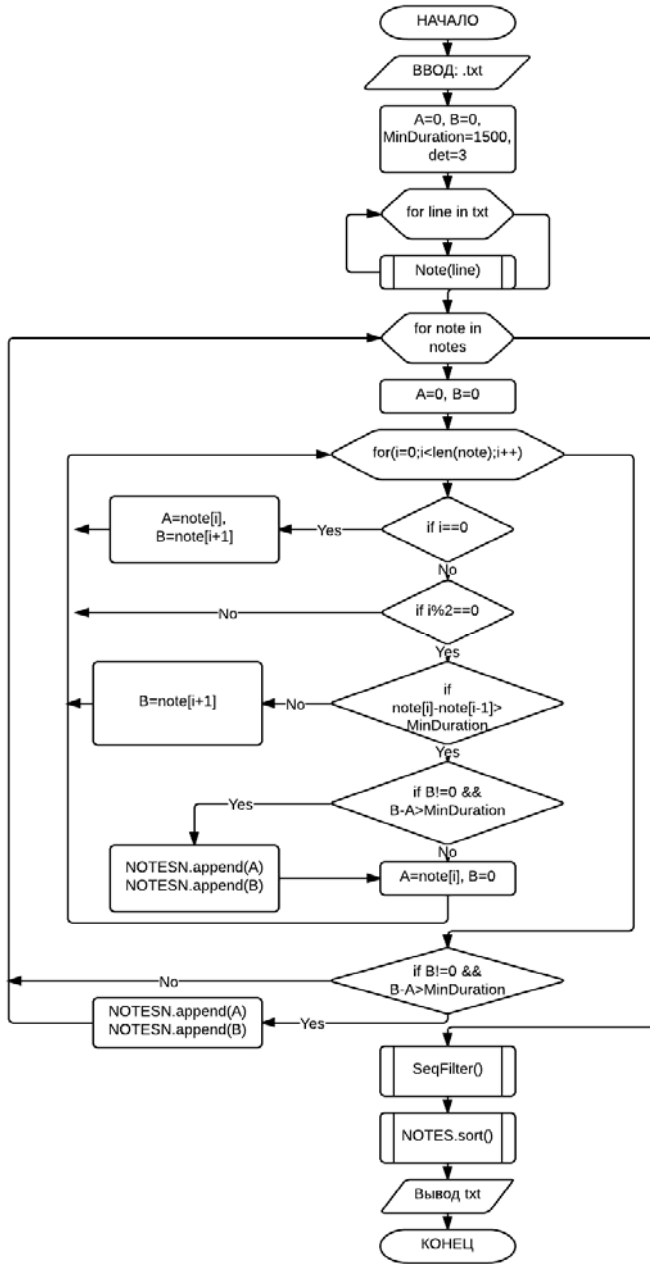


Рис. 1. Алгоритм распознавания музыкальных нот

На рис. представлены входные данные в графическом. Используется аудиозапись с произношением нот: ми, до, ре, ми, до (стаккато). В результате работы алгоритм точно определяет нужные ноты (рис. 3).

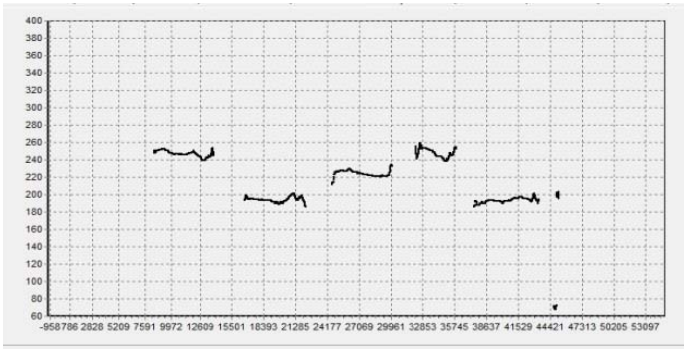


Рис. 2. Входные данные в графическом виде

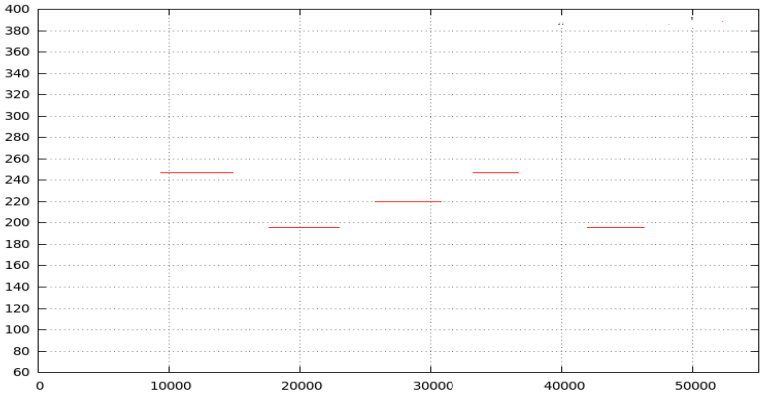


Рис. 3. Результат работы алгоритма

ЛИТЕРАТУРА

1. Октавная система [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/, свободный (дата обращения: 15.02.2014).

2. Черных Д.В., Конев А.А., Мещеряков Р.В. Элементы программного комплекса для оценки биометрических параметров в защищённых системах // Электронные средства и системы управления: матер. докл. междунар. науч.-практ. конф. Томск: В-Спектр, 2011. С. 188–190.

ПОДСИСТЕМА ПЛАНИРОВАНИЯ ТРАЕКТОРИИ МНОГОЗВЕННОГО МАНИПУЛЯТОРА НА ОСНОВЕ АЛГОРИТМА МУРАВЬИНЫХ КОЛОНИЙ

А.О. Шлетгауэр, студент 5-го курса каф. АСУ
Научный руководитель А.Н. Горитов, профессор каф. АСУ, д.т.н.
г. Томск, ТУСУР, ArisTem108@gmail.com

Аппарат компьютерного моделирования РТС (робототехнических систем), предоставляющий возможность планировать траекторию перемещения программно-управляемых механизмов с учетом находящихся в зоне обслуживания препятствий, позволит снизить стоимость и сроки проектирования промышленных роботов, рассчитать оптимальные траектории движения рабочих органов и сформулировать алгоритмы управления.

Задача планирования состоит в том, чтобы построить путь из исходной точки в конечную и не допустить столкновений с препятствиями. В процессе движения манипулятор не может выйти за пределы зоны обслуживания. Данная задача решается с учетом физических и геометрических ограничений [1].

Применение муравьиного алгоритма к задаче планирования. Рассмотрим многозвенный манипулятор, содержащий m кинематических узлов. Каждый кинематический узел задает либо вращение, либо линейное перемещение. Узел характеризуется значением обобщенной переменной, которая может принимать значения из некоторого множества допустимых значений. Положение РТС в пространстве можно описать как совокупность значений обобщенных переменных. Предполагается, что система изначально обладает информацией о внешнем пространстве и находящихся там препятствиях.

Представим граф, элементами которого являются положения РТС в пространстве, а ребрами – переходы от одного положения к другому. Тогда задачу планирования траектории можно свести к задаче поиска пути между вершинами на графе. Однако размер графа, многократно увеличивающийся с увеличением числа кинематических узлов, не позволяет использовать для решения классические алгоритмы.

Алгоритм муравьиных колоний – один из эффективных полиномиальных алгоритмов для нахождения приближённых решений задач поиска маршрутов на графах, базирующийся на моделировании поведения колонии муравьев. Колония муравьев может рассматриваться как многоагентная система, в которой каждый агент функционирует автономно, по простым правилам [2].

Основу социального поведения муравьев составляет самоорганизация – множество механизмов, обеспечивающих достижение систе-

мой глобальной цели в результате низкоуровневого взаимодействия ее элементов. Самоорганизация является результатом следующих компонентов: случайность, многократность, положительная обратная связь, отрицательная обратная связь.

Многократность взаимодействия реализуется итерационным поиском маршрута одновременно несколькими муравьями. При этом каждый муравей рассматривается как независимый агент, решающий свою задачу.

Положительная обратная связь реализуется как имитация поведения муравьев типа «оставление следов – перемещение по следам». Чем больше феромона оставлено на тропе – ребре графа, тем больше муравьев будет передвигаться по ней. При этом на тропе появляются новые следы, привлекающие муравьев. Для задачи планирования обратная связь реализуется стохастическим правилом: вероятность включения ребра графа в маршрут муравья пропорциональна количеству феромона на нем.

Применение такого вероятностного правила обеспечивает реализацию и другой составляющей самоорганизации – случайности. Количество откладываемого муравьем феромона на ребре графа обратно пропорционально длине маршрута. Чем короче путь, тем больше феромона будет отложено на соответствующих ребрах. Отложенный феромон выступает как усилитель, он позволяет хорошим маршрутам сохраняться в глобальной памяти муравейника.

Использование только положительной обратной связи приведет к преждевременной сходимости решений – в таком случае все муравьи будут двигаться одинаковыми субоптимальными маршрутами. Для исследования всего пространства решений используется отрицательная обратная связь – испарение феромона (уменьшение во времени количества отложенного на предыдущих итерациях феромона).

Таким образом, для каждого муравья переход от одной вершины i к другой вершине j зависит от трех составляющих: памяти муравья (список посещенных муравьем вершин), привлекательности вершины и следа феромона на ребре *(i, j)*.

За вероятность перехода k-го муравья из вершины i в вершину j, на t-й итерации, отвечает вероятностно-пропорциональное правило:

$$\begin{cases} P_{ij,k}(t) = \dfrac{\left[\tau_{ij}(t)\right]^{\alpha} \cdot \left[\eta_{ij}\right]^{\beta}}{\sum_{l \in J_{i,k}} [\tau_{il}(t)]^{\alpha} \cdot [\eta_{il}]^{\beta}}, \text{если } j \in J_{i,k}, \\ P_{ij,k}(t) = 0, \text{если } j \notin J_{i,k}, \end{cases}$$

где α и β – два регулирующих параметра, задающие веса следа феромона и привлекательности вершины при выборе маршрута, а J – список посещенных муравьем вершин.

Заключение. Муравьиные алгоритмы основаны на имитации самоорганизации социальных насекомых посредством использования динамических механизмов, с помощью которых система достигает глобальной цели в результате локального низкоуровневого взаимодействия элементов. Эти алгоритмы обеспечивают решения задач не хуже общих метаэвристических технологий оптимизации и некоторых проблемно-ориентированных методов.

Ряд экспериментов показывает, что эффективность муравьиных алгоритмов растет с ростом размерности решаемых задач [3]. Качество получаемых решений во многом зависит от настроечных параметров в вероятностно-пропорциональном правиле выбора пути. Возможно, что динамическая адаптационная настройка этих параметров может способствовать получению лучших решений.

ЛИТЕРАТУРА

1. Горитов А.Н. Моделирование манипуляционных робототехнических систем в условиях неполной информации о внешней среде. Томск: Изд-во Института оптики атмосферы СО РАН, 2005. 276 с.

2. Штовбса С.Д. Муравьиные алгоритмы // Exponenta Pro. Математика в приложения. 2003. №4.

3. Макконел Дж. Основы современных алгоритмов. 2-е изд., доп. М.: Техносфера, 2004. 308 с.

ЗАДАЧА ЭНЕРГОЭФФЕКТИВНОГО УПРАВЛЕНИЯ ГРУППОЙ ВОДОДОБЫВАЮЩИХ НАСОСОВ И ЕЕ РЕШЕНИЕ НЕЙРОСЕТЬЮ ХОПФИЛДА

Е.О. Иванов, аспирант каф. АОИ,
Д.И. Цыбусов, А.А. Даниленко, студенты
г. Томск, ТУСУР, egor.o.ivanov@yandex.ru, demonbusov1@yandex.ru, danilenkoprogaleksandr@gmail.com

Проект ГПО АОИ-1301– «Энергосберегающее ситуационное нейросетевое управление»

Имеется группа вододобывающих насосов, работающих на заполнение резервуара. Каждый насос характеризуется своей подачей Q_i ($м^3/ч$) и потребляемой мощностью N_i (кВт), поэтому различно значение удельной стоимости перекачки единицы воды $C_i = N_i / Q_i$.

Обычно насосы вводятся в избыточном количестве, поэтому все включенные насосы обладают суммарной подачей Q_z, большей, чем реальная потребность [1].

Сложность предсказания количества требуемой воды приводит к применению простейших экономически и технологически не выгод-

ных алгоритмов управления: включение и выключение насосов при достижении уровня воды в резервуаре определенных отметок.

Выгодней поддерживать уровень воды в резервуаре на определенной отметке путем включения насосов, суммарно подающих количество воды, равное потребляемому. При этом целесообразно использовать средний интервал времени управления, например час.

Для определения предполагаемого значения оттока из резервуара предполагается использовать краткосрочное прогнозирование с помощью многослойных нейронных сетей.

Зная прогноз водопотребления на час вперед и расхождение уровня воды в резервуаре с необходимым, можно определить суммарное количество воды, которое необходимо подать в резервуар в течение следующего часа.

Возникает задача определения, какие насосы следует включить, а какие выключить, для определения оптимального распределения нагрузки. Таким образом, приходим к многокритериальной задаче оптимизации: снижение стоимости и соответствие требуемой производительности.

Нейросетевая постановка задачи. Обозначим: $x_i \in \{0,1\}$ – состояние насоса в текущий момент времени, где 1 соответствует состоянию «включен», а 0 – «выключен», общее количество насосов обозначим n. Таким образом, при $x_i = 0$ выключенный насос не будет увеличивать суммарную удельную стоимость, а включенный ($x_i = 1$) – будет на величину C_i. Тогда решением задачи будет поиск вектора состояний всех насосов X, который будет минимизировать их суммарную удельную стоимость и отклонение от суммарной необходимой подачи Q_z.

Представим задачу в терминах сети Хопфилда с бинарными состояниями нейронов $x_i \in \{0,1\}$ и функцией энергии $E = E(t)$ дискретной сети с дискретным временем:

$$E = \alpha(\sum_i x_i Q_i - Q_z)^2 + \beta \sum_i x_i c_i \ ,$$

где α и β – неотрицательные вещественные константы, определяющие вклад критериев оптимальности в энергию сети.

Построив уравнение динамики сети согласно [2] и сопоставив с динамикой сети Хопфилда, находим матрицу весов w_{ij} [формула (1)] и вектор порогов u_i [формула (2)]:

$$w_{ij} = -2\alpha Q_i^2 \delta_{ij} - 2\alpha Q_j Q_i (1 - \delta_{ij}) \ , \qquad (1)$$

$$u_i = -2\alpha Q_z Q_i + \beta c_i \ , \qquad (2)$$

где δ_{ij} – символ Кронекера.

Моделирование. В качестве задачи для моделирования рассматривалась группа из 18 насосов (реальные данные).

Алгоритм на основе сети Хопфилда сравнивался с двумя простейшими алгоритмами: включение насосов в порядке возрастания их мощностей, пока не возникнет приближение к желаемой суммарной подаче и включение насосов в порядке возрастания удельной стоимости добычи кубометра воды.

Для сравнения алгоритмов было реализовано приложение в среде Lazarus на языке Object Pascal. А также для отображения работы алгоритмов была написана графическая модель водозабора 1-го уровня с использованием графической библиотеки «Andorra 2d».

Так как получение решения задачи необходимо выполнять ежечасно, в процессе моделирования оценивалась не скорость получения решения, а его качество.

Моделирование выполнялось многократно. Модель Хопфилда запускалась на вычисления с коэффициентами $\alpha = 1{,}0$ и $\beta = 0{,}24$, подобранные экспериментально с расчетом на минимальное расхождение в количестве воды.

Проведем анализ результатов моделирования (таблица) различных подходов на одинаковых данных.

Результаты моделирования

Алгоритм	Сумма N	Сумма C	Среднее
Хопфилд	206820	374680	0,552
Минимизация N_i	234160	375610	0,623
Минимизация C_i	199190	376910	0,528

Во 2-м столбце представлена суммарная мощность, потребленная всеми включенными насосами за все время моделирования. В 3-м столбце находится суммарное значение подачи каждого из алгоритмов. По условию суммарная необходимая подача всех насосов составляла 374100 м^3. Как видим, сеть Хопфилда сгенерировала наилучшее значение. Последний столбец показывает среднюю удельную стоимость каждого кубометра воды. Здесь сеть Хопфилда показала приемлемые, но не лучшие результаты. Но вместе с тем сеть Хопфилда оставляет много места для маневра: подбирая значения коэффициентов, можно регулировать «вес» каждого из критериев оптимальности.

Заключение. Таким образом, представленная дискретная сеть Хопфилда, решающая задачу оптимизации работы группы насосов, показала хорошие результаты моделирования. Получение более качественных решений задачи может быть достигнуто переходом на непрерывную модель функционирования сети Хопфилда путем включения частотного управления.

ЛИТЕРАТУРА

1. Замятин Н.В., Иванов Е.О. Задача энергоэффективного управления группой вододобывающих насосов и ее решение нейросетью Хопфилда // Доклады ТУСУРа. 2013. № 4 (30). С. 168–172.

2. Меламед И.И. Нейронные сети и комбинаторная оптимизация // Автомат. и телемех. 1994. Вып. 11. С. 1–38.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ НЕЧЕТКИХ СИСТЕМ НА ОСНОВЕ АЛГОРИТМА «ВЕЛИКИЙ ПОТОП»

О.К. Сонич, студентка 3-го курса

Научный руководитель И.А. Ходашинский, профессор,д.т.н.

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

Проект ГПО КИБЭВС-1211 – «Нечёткие системы»

При исследовании сложных систем и процессов специалисты сталкиваются с проблемой невозможности или же трудоемкости их реализации с помощью аналитических моделей, данная проблема решается использованием нечетких моделей [1].

В данной работе проводится аппроксимация функции с помощью нечетких систем, а параметры нечеткого аппроксиматора настраиваются с помощью алгоритма «Великий потоп» [2].

Описание нечеткой системы. В данном разделе рассмотрим построение нечетких аппроксиматоров. Нечеткая модель может быть построена либо на основе знаний эксперта, либо на основе таблицы наблюдений. В данном случае рассматриваем построение нечеткой модели типа синглтон на основе таблицы наблюдений. В входе работы оперируем такими параметрами, как входной вектор $\mathbf{x}$, вектор параметров антецедентов $\boldsymbol{\theta}$, скалярный выход системы y, вектор параметров консеквентов $\mathbf{r}$. Тогда нечеткая система может быть представлена как

$$y = f(\mathbf{x}, \boldsymbol{\theta}, \mathbf{r}).$$

Рассматривая построение правил в нечеткой системе типа синглтон, оперируем следующими параметрами: лингвистический терм A_{ij}, который оценивает переменная x_i, тогда i-е правило имеет следующий вид [1]:

$$\text{IF } x_1 = A_{1i} \text{ AND } x_2 = A_{2i} \text{ AND } \ldots \text{ AND } x_n = A_{ni} \text{ THEN } y = r_i.$$

На рис. 1 представлен пример лингвистических термов, определяемых треугольными функциями принадлежности, задаваемых тройкой параметров.

После формирования базы правил производится формирование вектора нечеткой системы и расчет ошибки (RMSE). Пусть дано множество обучающих данных (таблица наблюдений) $\{(\mathbf{x}_p;\ t_p),\ p=1,\ldots,m\}$,

тогда среднеквадратическая функция ошибки, являющаяся численным критерием адекватности модели, вычисляется по следующей формуле (1):

$$E(\mathbf{x}_p,\boldsymbol{\theta},\mathbf{r})=\frac{\sqrt{\sum_{p=1}^{m}(t_p-f(\mathbf{x}_p,\boldsymbol{\theta},\mathbf{r}))^2}}{m}. \quad (1)$$

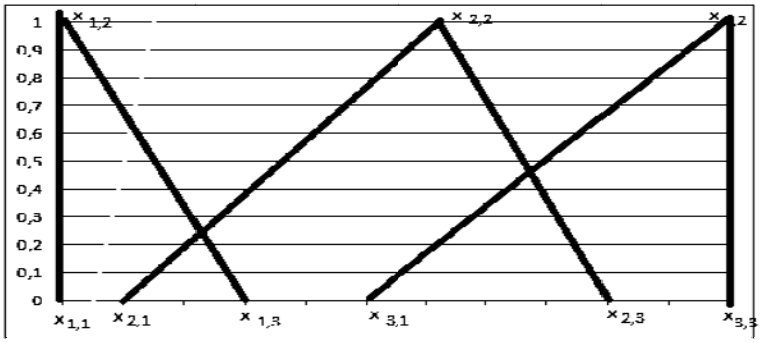


Рис. 1. Разбиение переменной на 3 лингвистических терма треугольного типа

И получим следующий вектор, который и будет обрабатывать алгоритм «Великий потоп» (рис. 2):

RMSE				…			…	

Рис. 2. Вектор нечеткой системы

Алгоритм «Великий потоп». Рассмотрим собственно алгоритм, с помощью которого будет настраиваться нечеткая система. Если говорить обобщенно, то алгоритм «Великий потоп» можно охарактеризовать следующим образом: на ограниченном участке уровень воды постепенно увеличивается, наша задача – пройти по местности так, чтобы не замочить наших ног и подняться на самую возможно высокую точку.

Теперь рассмотрим более конкретно алгоритм «Великий потоп». Введем основные обозначения: x_i^o – текущее решение, x_i^c – новое решение, f^o – текущее значение целевой функции, f^c – новое значение целевой функции, UP – параметр увеличивает или уменьшает уровень в зависимости от поставленной задачи, u – равномерное случайное число, сгенерированное в интервале [0,1], p – заранее оговоренное нечетное целое, $LEVEL$ – уровень воды, параметр, используемый в решении, или критерий приемлемости.

Первым шагом случайно генерируем точку x_i^o в пределах диапазона данных, далее вычисляем значение целевой функции f^o с учетом сгенерированной точки и присваиваем это значение как начальное зна-

чение переменной *LEVEL*. Далее мы осуществляем поиск точки-кандидата (точки, в которую мы можем переместиться) по следующей формуле:

$$x_i^c = x_i^o + (10 * u - 5)^p ; i = 1,2, \dots, n.$$

Вычисляем значение целевой функции с учетом точки-кандидата f^c и сравниваем её значение с текущим f^o: если значение f^o больше значения f^c, то присваиваем значение $f^o = f^c$ и изменяем уровень воды по следующей формуле:

$$LEVEL = LEVEL - UP * (LEVEL - f^c).$$

Если же значение текущей функции меньше значения новой целевой функции, то ищем новую точку-кандидата. К сожалению, алгоритм может и не найти подходящие число за допустимое количество итераций, тогда сообщаем текущее значение x_i^o как оптимальное. Условием выхода из алгоритма являются достижение наперед заданного количества итераций или же выполнение следующего условия: $((x_i^o - x_i^c)/ x_i^c) < 0.000001$. После выполнения какого-либо из условий, мы сообщаем текущее решение как оптимальное [3].

Заключение. В настоящие время ведется программная реализация алгоритма «Великий потоп» на базе нечеткого аппроксиматора и проверка результатов работы алгоритма.

ЛИТЕРАТУРА

1. Ходашинский И.А., Дудин П.А. Идентификация нечетких систем на основе непрерывного алгоритма муравьиной колонии // Автометрия. 2012. Т. 48, № 1. С. 45–71.

2. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы: Пер. с польск. И.Д. Рудинского. М.:Горячая линия – Телеком, 2006. 452 с.

3. Ravi V. Modified Great Deluge Algorithm versus Other Metaheuristics in Reliability Optimization, Computational Intelligence in Reliability Engineering (SCI) 40. 2007. P. 21–36.

СТИЛЕМЕТРИЯ ДЛЯ ОПРЕДЕЛЕНИЯ АВТОРСТВА АНОНИМНЫХ ТЕКСТОВ В СЕТИ

И.С. Созинова, студентка каф. КИБЭВС

Научный руководитель А.С. Романов, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, irishechka7371@gmail.com

Глобальная сеть Интернет стала неотъемлемой частью нашей жизни. Поэтому злоумышленники проявляют к ней большой интерес. Возникает проблема их отслеживания в сети. Сегодня науку, называемую стилеметрией, можно использовать для борьбы с хакерами,

«троллями» и создателями вредоносных программ, встречающихся в Интернете. Стилеметрия может служить для определения оскорбительных текстов, расовой дискриминации, для отнесения текста к определенной категории

Стилеметрия – филологическая система средств и приемов количественного измерения стилистических характеристик (параметров) текста (например, лексико-статистических) [2].

В то же время стилеметрия – анализ уникального стиля личных текстов также может быть использована работодателями для поиска информаторов, заявляющих о злоупотреблениях компании, жалобщиков и несогласных.

«Ваш стиль письма делает вашу интернет-анонимность труднодостижимой», – говорит американский исследователь, разработавший онлайн-средство анализа стиля текстов [3].

На сегодняшний день в результате многочисленных исследований можно выделить несколько типов стилеметрических характеристик текстов, по которым возможно проведение атрибуции: символьные, лексические, синтаксические, семантические, тематические [1].

Для того чтобы на их основе провести стилеметрический анализ текста, необходимо использовать определенные методы, позволяющие производить замену повествовательных источников их оределенными количественными характеристиками. В целом, весь процесс стилеметрического исследования текста может быть разбит на этапы (рис. 1).

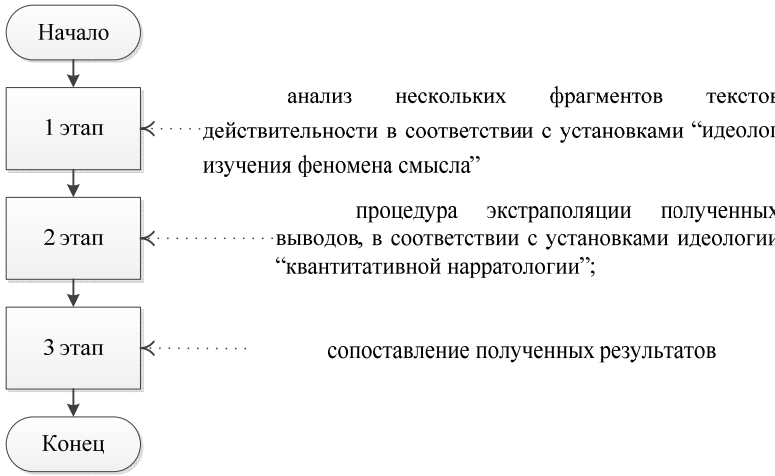


Рис. 1. Этапы стилеметрического анализа текста

При стилеметрическом анализе на протяжении многих десятилетий применялись различные подходы, которые можно разбить на 2 категории (рис. 2).

Следует отметить, что детерминистские подходы при автоматизированном анализе текстов начали приобретать популярность сравнительно недавно в связи со стремительным развитием вычислительной техники и распространением применения технологий искусственного интеллекта.

Рис. 2. Подходы при стилеметрическом анализе текстов

Был произведен ряд исследований, которые доказывают эффективность применения детерминистского подхода в сфере стилеметрического исследования текстов в сетях [4]. Большинство программных продуктов, например Атрибутор, информационная система СМАЛТ, использующие статистические подходы при исследовании текстов известных писателей, демонстрируют довольно высокую точность, но имеют ограниченную и уже достаточно хорошо изученную область применения, специализируясь на атрибуции текста.

ЛИТЕРАТУРА

1. Stamatatos E. A Survey of Modern Authorship Attribution Methods [electronic source] / E. Stamatatos. Electronic data. Dept. of Information and Communication Systems Eng. University of the Aegean. Samos, 2005. Access mode: http://www.icsd.aegean.gr/lecturers/stamatatos/papers/survey.pdf

2. Kenny A. A Stylometric Study of the New Testament // A. Kenny. Text data. Oxford, 1986.

3. Khaicy G. Why hackers should be afraid of how they write [Elecronic source]: The Sydney Morning Herald, January 16, 2013. access mode: http://www.smh.com.au/it-pro/security-it/why-hackers-should-be-afraid-of-how-they-write-20130116-2csdo.html

4. Мещеряков Р.В. Модели определения авторства текста [Электронный ресурс] / Р.В. Мещеряков, Н.С. Васюков. Томск, 2009. Режим доступа: http://www.tusur.ru/ru/science/events/session/archive.html

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ НЕЧЕТКИХ СИСТЕМ НА ОСНОВЕ АЛГОРИТМА МИННОГО ВЗРЫВА

С.Р. Субханкулова, студентка 3-го курса каф. КИБЭВС
Научный руководитель И.А. Ходашинский, профессор каф. КИБЭВС
г. Томск, ТУСУР, sophi1059@gmail.com
Проект ГПО КИБЭВС-1211 – «Нечёткие системы»

В последнее время нечеткое моделирование является одной из наиболее активных и перспективных направлений прикладных исследований в области управления и принятия решений, когда в описании технических систем и бизнес-процессов присутствует неопределенность, которая затрудняет или даже исключает применение точных количественных методов и подходов [1].

Цель данной работы состоит в том, чтобы улучшить результаты работы модуля нечёткого управления за счёт оптимизации его параметров посредством алгоритма минного взрыва.

Модуль нечёткого управления. Основная задача нечеткого моделирования заключается в нахождении конечного множества локальных отношений вход-выход, которые описывают систему или процесс в виде нечетких «ЕСЛИ-ТО» правил. Известно, что моделирование систем включает два основных этапа: идентификацию структуры и идентификацию параметров. Идентификация структуры – определение таких характеристик нечеткой модели, как число нечетких правил, количество лингвистических термов, на которое разбиты входные и выходные переменные. К задачам идентификации параметров относятся нахождение оптимальных значений параметров антецедентов и консеквентов правил [2].

На начальном этапе моделирования нечёткой системы мы имеем таблицу наблюдений. Нужно задать термы для каждой входной переменной. Для этого в таблице наблюдений нужно найти минимальное и максимальное значения для каждой входной переменной $x_1, \ldots, x_n$.

Если известны интервалы изменения входных и выходных переменных, то можно разделить каждый из этих интервалов на *pi* пересекающихся отрезков (p_i – число лингвистических термов, на которое разбивается *i*-я переменная). Параметры отрезка определяют параметры функции принадлежности лингвистического терма LX_{ij}, заданного на данном отрезке [3].

Пусть *i*-я переменная определена на интервале [0, 10], разделим указанный интервал на следующие пять (p_i = 5) неравных отрезков: (0, 2), (1, 5), (2,5; 7), (4, 10), (9, 10). Лингвистические термы, определенные на отрезках, обозначим следующим образом: *T*1, *T*2, *T*3, *T*4, *T*5, т.е. $\mathbf{FX}_i$ = { *T*1, *T*2, *T*3, *T*4, *T*5}. Допустим, выбран треугольный тип функции принадлежности. Тогда один из возможных способов описания *i*-й переменной нечеткими значениями приведен на рис. 1 ($Ti = (a_i, b_i, c_i)$, i = 1, …, 5). Здесь функция принадлежности терма *T*1 задана тройкой (0, 0, 2), *T*2 – (1, 3, 5) и т.д.

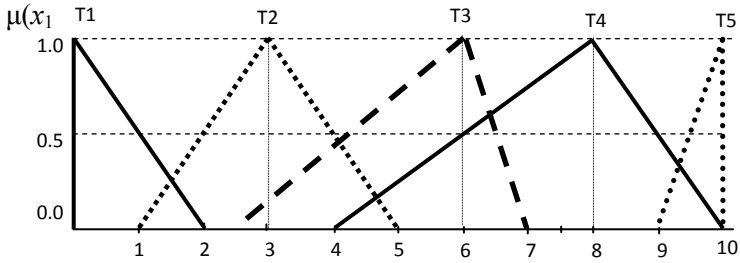


Рис.1. Случайное разделение переменной на пять лингвистических термов и соответствующие им функции принадлежности треугольного типа

После формирования термов формируется база правил. Пробегая по правилам, рассчитываем ошибку.

Далее формируется вектор, в который мы заносим ошибку, параметры, задающие треугольные функции для каждой входной переменной, и консеквенты.

Для определения неизвестных параметров антецедентов и нужно оптимизировать работу нечёткой системы.

Алгоритм «Минный взрыв». Идея алгоритма основана на наблюдении взрыва мины, в результате которого разлетающиеся осколки сталкиваются с другими минами, что также вызывает взрыв, и т.д.

Чтобы разобраться в ситуации, рассмотрим минное поле, где цель состоит в том, чтобы очистить его от мин, взорвав их все. Для этого нужно найти самую взрывоопасную мину, расположенную в оптимальной точке *X**.

Когда мина взорвалась, разлетается большое число осколков, и урон от взрыва вычисляется как *RMSE*, т.е. фитнес-целевой функции.

Работа алгоритма:

Шаг 1. Определить начальные параметры алгоритма: X_0 – начальная точка взрыва, фактор исследования – μ и уменьшающий коэффициент – α, максимальное число осколков N_s [4].

Шаг 2. Проверяется значение фактора исследования.

Шаг 3. Вычисление расстояния осколка и его местоположение.

Если $\mu > k$, где k – номер итерации, то перейти к шагу 4. Иначе: перейти к шагу 9.

Шаг 4. Вычисляется направление движения осколка.

Шаг 5. Генерируются новые осколки и вычисляется их новое положение.

Шаг 6. Проверка ограничений для генерации осколков.

Шаг 7. Передача результатов расчёта предыдущего шага в нечёткую систему, вычисление ошибок и сохранение решения с наименьшим значением ошибки.

Шаг 8. Замена лучшего промежуточного решения результатом, полученным на предыдущем шаге в случае, если ошибка для его решения будет меньше.

Шаг 9. Уменьшить расстояние осколка.

Шаг 10. В случае невыполнения условий останова перейти к шагу 2, иначе – прекращение работы алгоритма.

Заключение. В ходе данной работы был рассмотрен метаэвристический алгоритм для оптимизации параметров нечёткой системы – «Mine Blust Alghoritm». В дальнейшем планируется улучшить результаты работы алгоритма за счёт настройки его параметров в зависимости от сложности решаемой задачи и таблицы наблюдений.

ЛИТЕРАТУРА

1. Леоненков А. Нечёткое моделирование в среде MATLAB и fuzzyTECH. М., 2005. 736 с.

2. Ходашинский И.А., Гнездилова В.Ю., Дудин П.А., Лавыгина А.В. Основанные на производных и метаэвристические методы идентификации параметров нечетких моделей // Тр. VIII Междунар. конф. «Идентификация систем и задачи управления» SICPRO '08. Москва, 26–30 января 2009 г. М.: Институт проблем управления им. В.А. Трапезникова РАН, 2009. С. 501–529.

3. Ходашинский И.А. Технология идентификации нечетких моделей типа синглтон и Мамдани // Тр. VII Междунар. конф. «Идентификация систем и задачи управления» SICPRO'08. М.: Институт проблем управления, 2008. С. 137–163.

4. Mine blast algorithm: A new population based algorithm for solving constrained engineering optimization problems / A. Sadollah, A. Bahreininejad, H. Eskandar, M. Hamdi // Applied Soft Computing (13). 2013. P. 2592–2612.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ НЕЧЕТКИХ СИСТЕМ НА ОСНОВЕ ГРАВИТАЦИОННОГО АЛГОРИТМА

А.В. Цой, студент каф. КИБЭВС

Научный руководитель: И.А. Ходашинский, профессор каф. КИБЭВС

г. Томск, ТУСУР, dobrii@gmail.com

Проект ГПО КИБЭВС-1211 – «Нечёткие системы»

Методы аппроксимации используются в компьютерном моделировании и идентификации параметров исследуемых систем в тех случаях, когда описание объекта задано в виде таблицы наблюдений и отсутствует математическая модель данного объекта. Среди большого разнообразия методов и средств решения проблем аппроксимации особое место занимают нечеткие аппроксиматоры, в силу их способности работать в условиях неопределенности данных, а также интерпретировать эти данные.

Цель работы состоит в описании гравитационного алгоритма для оптимизации нечеткого аппроксиматора.

Нечеткая система. На начальном этапе у нас имеется таблица наблюдений, состоящая из значений входных переменных $x_{1i}, x_{2i} \dots x_{ni}$ и значений выходных переменных $O(x_{1i}, x_{2i} \dots x_{ni})$, $i = \overline{1,n}$. Необходимо для каждой входной переменной задать термы. Имея минимальное и максимальное значения для каждой переменной, нужно разделить каждый интервал на необходимое число термов так, чтобы область определения входных данных была покрыта полностью.

В работе использованы треугольные функции принадлежности для определения термов, т.к. они задаются всего 3 переменными (a_i, b_i, c_i), требуют меньшего количества машинных вычислений при определении степени принадлежности, что сокращает общее время оптимизации [1].

$$\mu(x) = \begin{cases} \dfrac{x-a}{b-a}, & a \le x \le b, \\ \dfrac{x-c}{b-c}, & b \le x \le c, \\ 0, & \text{в других случаях.} \end{cases}$$

После создания термов формируется база правил. При помощи базы правил рассчитывается ошибка. Далее формируется вектор $\mathbf{X_i}$, в который мы заносим ошибку *MSE*, параметры, задающие треугольные функции принадлежности для каждой входной переменной (a_j, b_j, c_j) и консеквенты (O_k), рассчитанные при помощи базы правил (рис. 1).

MSE	a_1^1	b_1^1	c_1^1	a_2^1	b_2^1	c_2^1	...	a_n^j	b_n^j	c_n^j	O_1	O_2	...	O_L

Рис. 1. Сформированный вектор

Изменяя параметры и повторяя действия, будет получено несколько векторов – популяция. У каждого вектора – своя ошибка MSE. Суть оптимизации нечеткой системы сводится к минимизации ошибки путем подбора соответствующих антецедентов и консеквентов.

Гравитационный алгоритм оптимизации. В гравитационном алгоритме агенты представляют собой набор масс (векторов), которые взаимодействуют друг с другом на основе ньютоновских законов движения и гравитации: «Каждая частица во вселенной притягивает другую частицу с силой, прямо пропорциональной произведению их масс и обратно пропорциональной квадрату расстояния между ними».

Алгоритм может рассматриваться как отдельная система масс. Это как искусственный мир масс, повинующийся законам гравитации и движения Ньютона. Точнее, массы соблюдают законы.

Закон гравитации (всемирного тяготения): каждая частица притягивает другую частицу, и сила тяжести F_{ij} между двумя частицами прямо пропорциональна произведению их масс и обратно пропорциональна расстоянию между ними:

$$F_{ij} = G\frac{M_j \times M_i}{R^2}.$$

Сама гравитационная постоянная G изменяется во времени.

Закон движения: текущая скорость массы эквивалентна сумме доли ее предыдущей скорости и изменений в скорости. Изменение скорости или ускорение любой массы равно отношению силы к массе [2].

Рассмотрим работу гравитационного алгоритма пошагово.

Шаг 1. Инициализация. Задается максимальное количество итераций T. Задается β – коэффициент, уменьшающий G, что позволяет контролировать точность поиска. Задается популяция из n векторов:

$$\mathbf{X_i} = \left(x_i^1 \dots x_i^d \dots x_i^n\right), i = \overline{1,n}.$$

Шаг 2. Рассчитывается ошибка, т.е. $MSE(\mathbf{X_i}, t)$, где $i = \overline{1,n}$.

Шаг 3. Находится G. Находится лучшее и худшее решение: $best(t)$ и $worst(t)$ соответственно:

$$worst(t) = \max\ MSE_i(t),$$
$$best(t) = \min\ MSE_i(t), где\ i = \overline{1,n}.$$

Шаг 4. Рассчитывается масса M при помощи $m_i(t)$ и ускорение a:

$$m_i(t) = \frac{MSE_i(\mathbf{X_i}, t) - worst(t)}{best(t) - worst(t)},$$

$$M_i(t) = \frac{m_i(t)}{\sum_{j=1}^{T} m_j(t)},\ \text{где}\ i = \overline{1,n},\ \ a_i^d(t) = \frac{\sum_{j=1, j\neq i}^{M} rand_j F_{ij}^d(t)}{M_{ii}(t)},$$

где $rand_j$– случайное число в интервале [0, 1].

Шаг 5. Рассчитывается скорость $v_i^d(t)$ и местоположение агентов $x_i^d(t)$:

$$v_i^d(t+1) = rand_i \times v_i^d(t) + a_i^d(t),$$
$$x_i^d(t+1) = x_i^d(t) + v_i^d(t+1).$$

Шаг 6. Если текущая итерация меньше T, то переходим к шагу 2 [2].

Заключение. В данной работе было рассмотрено описание нечеткой системы, а также метаэвристического «гравитационного алгоритма» для оптимизации параметров нечеткой системы.

ЛИТЕРАТУРА

1. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы / Пер. с польск. И.Д. Рудинского. М.:Горячая линия – Телеком, 2006. 452 с.

2. Esmat Rashedi GSA: A Gravitational Search Algorithm // Department of Electrical Engineering, Shahid Bahonar University of Kerman. 2009. 18 с.

СЕКЦИЯ 17

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.*

СОЗДАНИЕ РОБОТА НА ПЛАТФОРМЕ ARDUINO

С.И. Анищенко, студент каф. КИБЭВС
Научный руководитель О.В. Пехов, ассистент каф. КИБЭВС
г. Томск, ТУСУР, office@tusur.ru

Сейчас на кафедре активно развивается направление робототехники, создан клуб робототехники для проведения на его базе экскурсий и занятий учащихся. Исследование расширит поле деятельности направления, при помощи него будет создан робот со своей оригинальной и продуманной конструкцией, эффектной моделью работы, что и заинтересует людей проектированием и созданием технических устройств и в частности роботов.

Главной целью являлось исследование платформы Arduino на возможность создания на его базе роботизированной системы, а дополнительной – изучение последовательности и вариантов создания робота.

Платформа Arduino, изображенная на рис. 1, имеет следующие достоинства для изготовления учебной роботизированной системы:

– открытая архитектура, исходные коды;

– простое для работы программное обеспечение (загрузчики, язык программирования);

– множество поддерживаемых устройств и библиотек для работы с ними;

– 6 аналоговых входов МК для подключения датчиков;

– 6 выводов широтно-импульсной модуляции для регулирования нагрузки исполнительных устройств.

По принципу работы создаваемое нами устройство робот – автоматизированное устройство. Действуя по заранее заложенной программе и получая информацию о внешнем мире от датчиков (аналогов органов чувств живых организмов), робот самостоятельно осуществляет производственные и иные операции, обычно выполняемые чело-

веком (либо животными). При этом робот может как иметь связь с оператором (получать от него команды), так и действовать автономно.

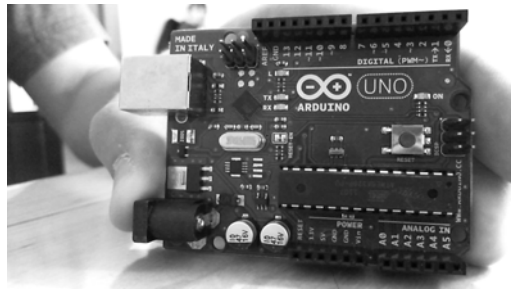


Рис. 1. Плата Arduino

Робот характеризуется различными типами движения и, в частности, количеством используемых в движении элементов (колес, ног) и двигателей, приводящих их в движение, поэтому в ходе исследования требовалось выработать концепцию, какой тип робота будет создан. Проанализировав цели и возможности платы Arduino, было решено создать шагающего шестиногого робота, прообразом движения которого станет модель передвижения паука, при этом модель позволит подключать и меньше количество конечностей для отработки других алгоритмов движения. В качестве двигателей будут использоваться сервоприводы HXT900 с углом вращения в 90°, что удовлетворяет механике модели передвижения конечностей паука.

Для создания робота было проведено всестороннее моделирование. Роботизированная система была декомпозирована, составлена схема взаимодействия подсистем, изображенная на рис. 2, выявлены основные элементы и их варианты реализации.

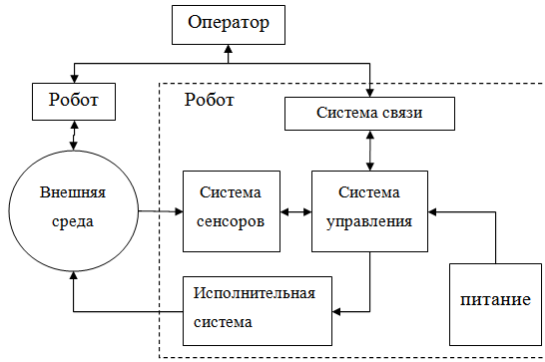


Рис. 2. Схема взаимодействия систем робота

Одним из вариантов для изготовления множественных конструкций робота будет использоваться перспективная технология 3D-печати, возможности которой подходят для быстрого создания точных, продуманных вариантов деталей и макетов робота.

УСТАНОВКА ХИМИЧЕСКОЙ ОБРАБОТКИ ПЕЧАТНЫХ ПЛАТ

В.А. Бахарев, А.И. Радостев, студенты каф. КИБЭВС
Научный руководитель Л.А. Торгонский, доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, alexandrradostev@gmail.com

Выполняемая работа посвящена созданию автоматизированной установки для химической обработки печатных плат (ПП). Её созданием решаются задачи обучения и приобретения опыта построения, программирования технологических установок с микропроцессорным управлением.

Схематично установка изображена на рис. 1. Для реализации транспортных операций в развитие конструкции установки, рассмотренной в работе, применён штатив с транспортными механизмами и шаговыми двигателями (Шд) для перемещения по трем координатам (*X*, *Y*, *Z*), изображенный на рис. 1.

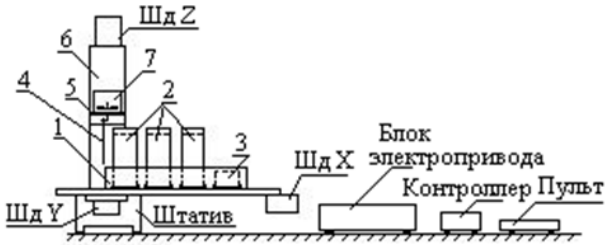


Рис. 1. Установка химобработки ПП

Для питания двигателей штатива используется силовой «Блок электропривода», рассчитанный на пошаговое внешнее цифровое управление двигателями штатива. В рассматриваемой установке на столе штатива (в координатах *X*, *Y*) устанавливается и фиксируется ванна *1*, в которой предусматривается установка трёх вертикально ориентированных емкостей с растворами *2* и одна емкость *3* для сбора капель жидкости в зоне термической сушки ПП. Плата *4* навешивается на кронштейне *5*, закрепляемом на траверсе *6*, и может перемещаться по вертикали (координата *Z*) относительно плоскости стола, ванны *1* и емкостей *2*, *3*. Стол с ванной *1* и ваннами *2* растворов в процессе обра-

ботки перемещается по координате *X*, а по координате *Y* только позиционируется относительно положения платы *4* при настройке установки. На кронштейне *5* установлен термовентилятор *7*, который перемещается одновременно с платой *4* и включается на задаваемое с пульта время при сушке платы после завершения процесса травления и промывки платы. В трёх ёмкостях *2* установки (для освежения, травления, отмывки) контролируются допустимый уровень наполнения и концентрация (или загрязненность) растворов. Недостаточность наполнения и превышение пороговых значений загрязнения растворов отображаются на пульте оператора осведомительными световыми индикаторами. Доступен контроль до пяти градаций состояния концентраций растворов в каждой из трёх ванн *2* на общее встроенное табло цифровой индикации. Оператор может принимать решение о запуске с пульта управления процессом независимо от состояния осведомительных индикаторов. Время сушки планируется задавать с пульта оператора.

Пульт управления установкой предусматривает наличие кнопок запуска (старт) и остановки (стоп), а также наличие индикаторов в виде светодиодов, которые оповещают оператора о наличии реактивов в емкостях и необходимости замены раствора для травления. Если проверка не обнаружила нарушений требований, то установка готова к запуску.

Контроллер (МК) через устройство связи с объектами контроля получает информацию от датчиков наличия растворов в сосудах и датчиков степени загрязненности растворов, управляет индикацией и контролирует состояния кнопок и переключателей «Пульта». Информация с микроконтроллера обрабатывается и передается на индикаторы, расположенные на пульте управления.

В процессе работ выполнено экспериментальное исследование режимов и ресурсов управления блоком электропривода. В качестве двухфазного управляемого генератора применена микроЭВМ [2] со встроенной клавиатурой, модулем отображения и параллельным портом вывода сигналов управления с логическими усилителями на выходе.

На каждый импульс «step» блок питания двигателей отрабатывает один шаг на повороте вала шагового двигателя (ШД). Шаг для одной из четырёх фаз по паспортным данным двигателей равен $1{,}8^{\circ}$, но блоком приводов отрабатывается на каждый импульс «step» пакет четырёх фаз, что составляет $7{,}2^{\circ}$. Исследованием установлено, что поворот червячного вала на один оборот совершается после подачи 960 импульсов «step». Линейное перемещение стола установки на 10 мм по любой из трёх координат исполняется пятью оборотами червячного вала. Максимальная линейная скорость перемещения в установке по координатам составляет 3,5 мм/с.

Результаты экспериментального управления позволили перейти к проработке конструкции установки и алгоритма управления транспортом плат по концептуальному сценарию для автоматизированной установки химической обработки печатных плат.

ЛИТЕРАТУРА

1. Достанко А.П. Технология и автоматизация производства радиоэлектронной аппаратуры. М.: Радио и связь, 1989. 623 с.

2. РР3.059. 004 ПС. Учебный микропроцессорный комплект // Паспорт. 1986. 35 с.

РАЗРАБОТКА МЕТОДИЧЕСКИХ УКАЗАНИЙ ДЛЯ ПРОВЕДЕНИЯ ЛАБОРАТОРНЫХ РАБОТ НА ТРЕНАЖЕРЕ УЗЛА УЧЕТА ГАЗА

Е.С. Барисенок, студент каф. КИБЭВС

Научный руководитель О.В. Пехов, ассистент каф. КИБЭВС

г. Томск, ТУСУР, elizaveta-barisenok@yandex.ru

В учебных программах предусматривается как теоретическое, так и производственное образование. Задачи, методы и обучение направлены к одной цели – подготовке высококвалифицированных специалистов. Для обучения персонала используется стенд-тренажер узла учета газа, после обучения специалисты могут самостоятельно выезжать на производственные объекты и выполнять работу.

Данный стенд-тренажер узла учета газа (стенд СТУ) [1] предназначен для изучения принципов работы узлов расхода газа, а именно узлов на базе диафрагмы камерной стандартной (ДКС), работающей совместно с датчиком разности давления и вычислителем, турбинного счетчика газа, работающего совместно с вычислителем Суперфлоу, расходомера и расходомера-счетчика вихревого.

Принцип работы стенда СТУ заключается в том, что с помощью системы кранов и запасных линий организовывается маршрут движения потока воздух. С помощью регулятора прямого действия устанавливается рабочее давление в пневматической системе.

На энергозависимые узлы стенда подается питающее напряжение. Включается компрессор. Сжатый воздух подается на вход стенда. Посредством контрольных устройств осуществляется считывание показаний датчиков. Направление движения потока показано на рис. 1.

Комплектность стенда составляет порядка 24 приборов, предназначенных для снятия параметров газа в стенде СТУ. Основными приборами являются вычислительный комплекс Суперфлоу [2] и коррек-

тор СПГ [3]. Используются для автоматического снятия показаний с датчиков стенда СТУ.

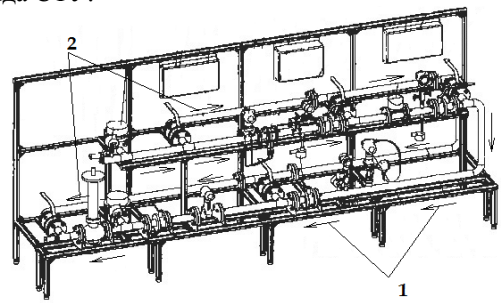


Рис. 1. Стенд СТУ. Направление движения потока: *1* – движение по основной линии; *2* – движение по запасной линии трубопровода

Используются расходомеры, которые предназначены для измерения давления в трубопроводе в автоматических системах.

Диафрагма (ДКС) предназначена для измерений расхода жидкостей, пара, газов методом переменного перепада давления в комплекте с датчиками разности давлений.

При работе с данным стендом СТУ допускаются специалисты, прошедшие обучение по специальности слесарь КИПиА и имеющие соответствующие свидетельства, изучившие теоритические основы метрологии и техники безопасности, так как установка является взрывоопасной.

Лабораторные работы разрабатываются для получения специалистами практического опыта работы со средствами измерений, узлов учета. Полученные знания будут применяться специалистами как на производственных объектах, так и на предприятии. Задачей лабораторных работ является научить специалистов выполнять настройку вычислительного оборудования, средств измерений и отдельных узлов стенда СТУ.

Методическое пособие должно включать в себя шесть лабораторных работ.

Лабораторная работа №1. Ознакомление со стендом СТУ.

Цель работы: изучение технической документации стенда СТУ и выполнение включение системы.

В данной работе необходимо изучить документацию стенда СТУ, выполнить включение компрессора, установить нужное давление в газопроводе.

Лабораторная работа №2. Настройка параметров корректора СПГ 762. 2 и вычислительного комплекса «Суперфлоу-IIE».

Цель работы: изучение методов настройки параметров корректора СПГ762. 2 и вычислительного комплекса «Суперфлоу-IIE».

В ходе выполнения работы требуется изучить техническую документацию корректора СПГ 762.2 и вычислительного комплекса «Суперфлоу-IIE», согласно ей произвести настройки параметров. Протестировать показания параметров в рабочей системе.

Лабораторная работа №3. Настройка счетчиков газа СГ16МТ, Rosemount 8800DR, Annubar PROBAR3051-SFA.

Цель работы: изучение технической документации приборов и выполнение необходимой настройки с помощью полевого коммуникатора.

В ходе данной лабораторной работы следует изучить органы управления полевого коммуникатора, схемы подключения, поиск прибора и научиться выполнять смену диапазона датчиков.

Лабораторная работа №4. Настройка датчиков давления Метран-75, Метран-150, Rossemount 3051C, Rosemont 2088.

Цель работы: изучение возможностей удаленного конфигурирования датчиков давления при помощи полевого коммуникатора.

В ходе данной лабораторной работы необходимо изучить органы управления полевого коммуникатора, схемы подключение, поиск прибора и научиться выполнять смену диапазона датчиков.

Лабораторная работа №5. Настройка платы вычислителя Суперфлоу-IIE для работы с датчиком дифференциального давления (в паре с диафрагмой), датчиком абсолютного давления и температуры.

Цель работы: исследование настройки платы вычислителя Суперфлоу-IIE для работы с датчиком дифференциального давления.

При исполнении данной лабораторной работы необходимо научиться выполнять настройку платы для работы с датчиком, используя терминал CHIT.

Лабораторная работа №6. Настройка корректора СПГ 761.2 для работы со счетчиком газа СГ-16МТ-100, для работы с датчиком расхода 3051SFA, для работы с вихревым датчиком расхода 8800.

Цель работы: изучение подключения и настройки корректора СПГ 761.2 для работы со счетчиком газа СГ-16МТ-100, расходомером 3051SFA и датчиком расхода 8800.

В ходе лабораторной работы будет изучен порядок выполнения настройки для взаимодействия корректора с расходомерами, входящими в состав стенда СТУ (СГ-16МТ-100, Rosemount 2088, Annubar PROBAR3051-SFA).

ЛИТЕРАТУРА

1. Стенд-тренажер СТУ. Руководство по эксплуатации 16.0012.000.00 РЭ.
2. Комплекс многониточный измерительный микропроцессорный «Суперфлоу-IIE». Руководство по эксплуатации ЗИ2.838.009 РЭ1.
3. Корректор расхода газа СПГ-761. Руководство по эксплуатации РАЖГ. 421412.026 РЭ.

ВЫСОКОЧАСТОТНЫЙ ГЕНЕРАТОР ДЛЯ АБЛЯЦИИ БИОЛОГИЧЕСКОЙ ТКАНИ

Е.А. Батеев, студент каф. КИБЭВС
Научный руководитель Н.М. Федотов, зав. лаб. безопасных биомедицинских технологий ЦТБ, к.т.н.
г. Томск, ТУСУР, evbateev@gmail.com

Уже несколько лет лаборатория медицинской электроники «Биоток» при участии студентов кафедры КИБЭВС занимается разработкой устройства, предназначенного для проведения катетерных абляций при нарушениях ритма сердца (деструктора). Основной проблемой, с которой пришлось столкнуться при разработке, является высокий уровень электромагнитных помех, исходящих от генератора деструктора и влияющих на работоспособность других устройств медицинского назначения. Целью данной работы является разработка высокочастотного генератора деструктора, при работе которого бы исключалось влияние на другие устройства медицинского назначения.

Требования, предъявляемые к генератору, показаны в таблице. Также требуется реализовать защиту от короткого замыкания и режима холостого хода. Для обеспечения необходимой информацией о ходе операции необходимо реализовать обратную связь по току и напряжению.

Электрические параметры генератора

Параметр	Значение
Входное напряжение, В	48
Диапазон выходной мощности, Вт	0–200
Диапазон сопротивления нагрузки, Ом	50–200
Частота преобразования, кГц	100
Форма выходного сигнала	Синусоидальная
Частота выходного сигнала, кГц	440
Амплитуда выходного напряжения, В	0–200

На рис. 1 изображена функциональная электрическая схема генератора. На вход подается постоянное напряжение 48 В. Входным фильтром добиваются снижения уровня пульсаций в цепи, а также ограничивают диапазон частот входного напряжения. Контроллер источника питания – микросхема, на основе которой можно спроектировать импульсные источники питания различных типов. Данные контроллеры содержат в себе драйвер управления ключом преобразователя, а также обычно предусмотрена защита от короткого замыкания и/или режима холостого хода. Демпфирующая цепь (демпфер) предназначена для ограничения коммутационного выброса напряжения на ключе (транзисторе). Трансформатор Т1 используется для накопления магнитной энергии и передачи ее по принципу обратного хода. По-

средством регулирования напряжения от 0 до 3 В на схеме управления можно управлять выходным напряжением генератора. Также на схему управления поступает сигнал обратной связи по напряжению, позволяющий контроллеру источника питания регулировать выходное напряжение. Тактовый генератор подает импульсы на драйвер, который в свою очередь управляет силовыми ключами. Выходной фильтр представляет собой LC-цепь и предназначен для формирования синусоидального сигнала [1]. Трансформаторная гальваническая развязка необходима для защиты человека от поражения электрическим током. Выходной сигнал помимо катетера поступает на систему индикации для отслеживания текущего значений выходного напряжения и тока.

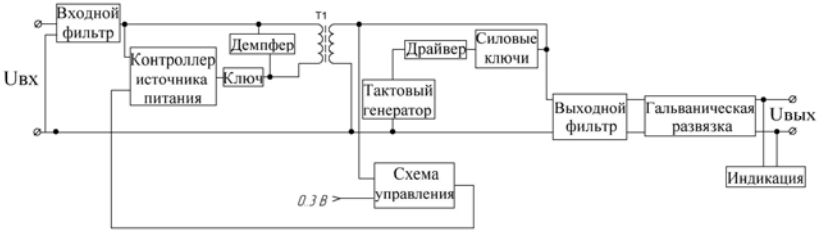


Рис. 1. Функциональная схема генератора

На момент написания статьи проект находится на этапе сборки макета устройства. В ближайшей перспективе планируется ряд испытаний, таких как испытания на ЭМС, а также тепловой анализ устройства.

ЛИТЕРАТУРА

1. Пат. 134036 RU, МПК A61B 18/10. Высокочастотный генератор для абляции биологической ткани / Н.М. Федотов, Е.А. Батеев, А.С. Коблош. №2013123144/14; Заяв. 21.05.2013; Опубл. 10.11.2013. Бюл. №31.

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ ВОССТАНОВЛЕНИЯ ПОВЕРХНОСТЕЙ ДЛЯ КОНТРОЛЯ ЭНЕРГЕТИЧЕСКОГО СОСТОЯНИЯ ЗАЛЕЖЕЙ С ПОМОЩЬЮ КАРТ ИЗОБАР

А.А. Бердников, студент каф. АСУ

г. Томск, ТУСУР, berdnikov_andrey@mail.ru

Нефтегазодобывающая промышленность страны в своем развитии прошла несколько существенно отличающихся друг от друга периодов. Особенно сложен последний, современный период, характеризующийся коренным изменением состояния всей социально-хозяйст-

венной обстановки в отрасли и в стране в целом. Этому периоду свойственно резкое ухудшение сырьевой базы нефтяной промышленности. Оно связано со вступлением многих нефтяных залежей в сложную позднюю стадию разработки, когда основная часть запасов уже отобрана и извлечение оставшихся запасов требует значительно больших усилий.

Среди вводимых в разработку залежей нефти возрастает удельный вес залежей с высокой вязкостью нефти, со сложным геологическим строением, с низкой фильтрующей способностью продуктивных пород, а также приуроченных к большим глубинам с усложненными термодинамическими условиями, к шельфам морей и т.д. Таким образом, и на старых, и на новых залежах возрастает доля так называемых трудноизвлекаемых запасов нефти.

Как следствие, возросла необходимость повышения уровня методов геолого-промыслового изучения характера размещения текущих запасов нефти и газа в пластах и обоснования технологических мероприятий по их извлечению. Особую актуальность приобрела проблема изучения структуры остаточных запасов нефти, сохранившихся в залежах после реализации принятых систем разработки; решение этой проблемы имеет важнейшее значение для проектирования вторичных и третичных методов воздействия с целью увеличения нефтеизвлечения.

Нефтегазопромысловое геологическое исследование залежей и месторождений осуществляется непрерывно в процессе разведки, освоения, эксплуатационного разбуривания и разработки вплоть до полного истощения залежей.

Таким образом, значение нефтегазопромысловой геологии состоит в обобщении и анализе всесторонней информации о месторождениях и залежах нефти и газа как объектах народнохозяйственной деятельности с целью геологического обоснования наиболее эффективных способов организации этой деятельности, обеспечения рационального использования и охраны недр и окружающей среды.

Важнейшей характеристикой работы пласта при анализе разработки является энергетическая характеристика. Она характеризуется существующим в нем пластовым давлением. Чем оно выше, тем полнее может быть использована залежь нефти.

В процессе эксплуатации для рационального использования энергии пласта необходим постоянный контроль распределения пластового давления в залежи. Осуществляется это путем систематических замеров забойных и пластовых давлений и построением карт изобар – линий, соединяющих точки с одинаковыми значениями пластовых давлений, приведенных к условной уровненной поверхности.

Эти карты строят на определенные даты, причем для их построения необходимо иметь достаточное количество одновременных замеров пластовых давлений по всей площади залежи. Под одновременными следует понимать замеры, сделанные в течение нескольких суток. Карты изобар строят путем линейной интерполяции значений пластовых давлений между точками скважин.

Карты изобар используют для контроля над разработкой нефтяных и газовых залежей, по ним рассчитывают значения среднего взвешенного по площади или по объему пластового давления по залежи в целом (в пределах внешнего контура нефтеносности), по зонам отбора (включаются точки скважин, по которым производится отбор нефти и газа) или по блокам разработки. Основная задача изучения карт изобар – определение режима работы залежи, т.е. изменения пластового давления в связи с отбором жидкости, газа, пластовой воды, воздействием на пласт, с учетом геолого-промысловых особенностей продуктивных пластов по площади залежи.

При построении карты используют данные о приведенном пластовом давлении. Для решения некоторых специальных задач могут быть построены карты абсолютного (замеренного у пласта) динамического пластового давления. При построении карты на установленную дату следует использовать замеры давления в скважинах, максимально приближенные во времени к этой дате. Однако на практике в связи с необходимостью поочередной остановки скважин для замера выполнение нужного количества измерений требует значительного времени – до одного-двух месяцев, а иногда и более.

На практике построение карт изобар сводится к применению алгоритма построения изолиний в области, представляющей собой сетку скважин. Итак, есть область, на которой проведен ряд измерений некоторой величины Z. Эти измерения проведены в равномерно распределенном наборе точек (x, y), которые являются узлами сетки скважин. Требуется спроектировать алгоритм выделения изолиний на основе регулярной сетки.

ЛИТЕРАТУРА

1. Эксплуатация нефтяных и газовых скважин [Электронный ресурс]. Режим доступа: http://judywhiterealestate.com/oil8.htm, свободный.

2. Карты изобар [Электронный ресурс]. Режим доступа: http://neftrussia.ru/karty-izobar/, свободный.

3. Изобары. Материал из википедии [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/%D0%98%D0%B7%D0%BE%D0%B1%D0%B0%D1%80%D1%8B, свободный.

СИНХРОНИЗАЦИЯ ИМПУЛЬСОВ ИЗЛУЧЕНИЯ РЕНТГЕНОВСКИХ УСТАНОВОК С СОКРАЩЕНИЯМИ СЕРДЦА

П.С. Боев, студент каф. КИБЭВС
Научный руководитель Н.М. Федотов, к.т.н.
г. Томск, ТУСУР, waka.packmaca@yandex.ru

Задача рентгеноскопии сейчас сводится к контрольному слежению за положением инструмента и его манипуляциями, что удобнее делать в квазистационарных режимах, синхронизированных с сокращениями сердца (с ЭКГ). Использование таких режимов позволяет не только следить за состоянием сердца в статичном положении, но и в несколько раз снизить поглощенную пациентом дозу при выполнении хирургической операции.

Необходимо устройство синхронизации для управления излучением рентгеновских установок, позволяющее производить синхронизацию с ЭКГ.

Структурная схема связи устройств, для которых производится синхронизация, показана на рис. 1.

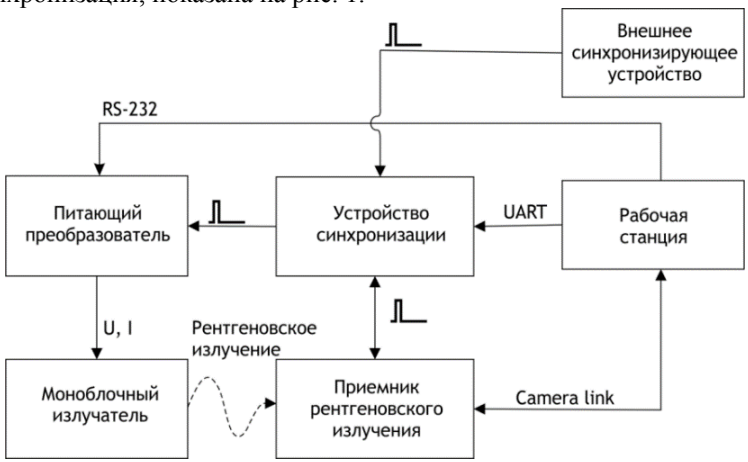


Рис. 1. Структурная схема связи устройств

Результаты работы. В ходе работы разработано устройство синхронизации, предназначенное для управления излучением рентгеновских установок интервенционной кардиохирургии, позволяющее сократить дозу облучения, получаемого пациентом при проведении хирургических операций в области сердца, за счет снижения количества импульсов излучения в минуту.

Разработана структурная схема устройства синхронизации (рис. 2). Спроектирована печатная плата устройства синхронизации. Разработаны управляющие алгоритмы для устройства и программное обеспечение управляющего контроллера.

Рис. 2. Структурная схема устройства синхронизации

Составлена система команды устройства синхронизации:

– SX – установить время излучения моноблочным излучателем;
– SE – установить время съемки приемником;
– ST – установить время между соседними кадрами;
– SD – установить время предварительной съемки;
– SM – установить режим работы приемника;
– SC – выбор непрерывного или импульсного излучения;
– SE – включение внешней синхронизации.

Заключение. К основным отличительным особенностям и преимуществам разработанного устройства можно отнести следующие:

– устройство представляет гибкий командный интерфейс, позволяющий детально настраивать её работу;

– устройство производит синхронизацию со внешними устройствами, например регистратором электрокардиограммы;

– устройство позволяет снизить дозу облучения за счет регулирования количества снятых рентгеновских снимков за единицу времени.

ЛИТЕРАТУРА

1. Technology Brief. MediGuide for intravascular evaluation of coronary anatomy [Электронный ресурс]. Режим доступа: http://www.health.qld.gov.au/healthpact/docs/briefs/WP093.pdf (дата обращения: 01.03.2013).

2. Technical manual. Dexela X-Ray detector panels: 2923, 2315, 1512, 1207. Doc no 122 0000131 version 2.0 DX-001116. 18/11/2010.
3. MX Series X-Ray Monobloc Generator Family. June 2011 4535-888-01031.

ЭЛЕКТРОННЫЙ ДЕКАНАТ

И.В. Ботнаренко, Я.К. Кротов, И.С. Куренков, Д.С. Терентьев, студенты каф. КИБЭВС
Научный руководитель Е.М. Давыдова, доцент, к.т.н.
г. Томск, ТУСУР, ИСИБ, ФБ, SertyRUS@gmail.com
Проект ГПО ФВС-1207 – «Система накопления знаний»

Многие отечественные вузы, при внедрении информационных технологий в управление учебным процессом сталкиваются с отсутствием подходящего открытого ПО, а также высокой стоимостью имеющихся на рынке решений автоматизации для вузов. Первоочередной задачей Open Source проекта «Электронный деканат» является адаптация СДО Moodle к особенностям организации учебного процесса в отечественных учебных заведениях, а в перспективе – разработка гибкой системы автоматизации бизнес-процессов в вузах. Система разрабатывается как модуль СДО Moodle и сама имеет развитую модульную архитектуру, позволяющую адаптировать ее под потребности каждой организации без модификации кода базовой системы.

Выбирая средства для реализации дистанционного обучения, многие учебные заведения обращают свой взгляд на СДО Moodle. И это не случайно. Moodle очень удобна для решения этой задачи. Среди ее достоинств – кроссплатформенность, русифицированный дружественный интерфейс, обширная справочная система, широкий набор методов подачи материала. Одним из основных достоинств является универсальность с точки зрения организации учебного процесса – СДО Moodle реализует среду обучения, в которой студенты могут взаимодействовать с учебными материалами, с преподавателями и друг с другом. Это является ключом к универсальности Moodle, позволяя применять эту систему для организации самых разных видов обучения в организациях разных типах.

Однако в Moodle нет групп, как их понимают в отечественных учебных заведениях, учебного плана, расписания, ведомостей и других неотъемлемых атрибутов реального учебного процесса практически любого нашего образовательного заведения.

Поэтому организации, начинающие внедрение Moodle, сталкиваются с проблемой организации учебного процесса, обеспечения отчетности, а также контроля за учебным процессом.

Таким образом, существует насущная потребность в адаптации СДО Moodle к традициям отечественной системы образования. Данную задачу призвана решить система «Электронный деканат» для СДО Moodle.

Free Dean's Office (электронный деканат) – это модуль для среды дистанционного обучения Moodle, который добавляет возможность управления процессом обучения, типичным для российских школ, колледжей и вузов. Free Dean's Office позволяет оперировать такими объектами, как «Специальность», «Дисциплина», «Курс» («Параллель»), «Академическая группа» («Класс»), «Семестр» («Учебный год»), «Учебный план слушателя», «Нагрузка преподавателя», «Итоговые оценки по дисциплинам», «Расписание», «Текущие оценки и посещаемость», «Журнал успеваемости и посещаемости», «Зачетная книжка» («Дневник»), «Табельный номер преподавателя» и т.д.

Free Dean's Office является свободным программным обеспечением и распространяется под лицензией GNU GPL. Разрабатывается как публичный проект на сайте http://sourceforge.net/projects/freedeansoffice/. Активную поддержку проекту оказывают ГОУ Центр образования «Технологии обучения» и ряд других организаций.

Целью данной работы является создание «Электронного деканата», являющегося основным механизмом учебного процесса. Разработка этой системы проводилась на примере кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) Томского государственного университета систем управления и радиоэлектроники (ТУСУР).

В соответствии с этим были решены важнейшие задачи, стоящие перед нами в процессе выполнения работы:

– анализ и создание базы данных «Электронный деканат»;

– анализ, развертка, заполнение и тестирование системы «Электронный деканат» (Free Dean’s Office);

– внедрение системы «Электронный деканат» (Free Dean’s Office) в учебный процесс.

В результате того, что каждый вуз пробует найти свои подходы к автоматизации учебного процесса, большинство образовательных учреждений несут дополнительные издержки на разработку собственных систем при отсутствии гарантий достижения поставленных целей. При этом используемые подходы зачастую несовместимы и не позволяют построить единое информационное пространство, удобное для образо-

вательных учреждений. Автоматизированная информационная система «Электронный деканат», на наш взгляд, менее громоздка, проста в установке и эксплуатации, обеспечивает полный набор функций, она дешевле, и, как нам кажется, ее высокие технологические свойства позволяют рекомендовать ее как типовую вузовскую программу.

Основной функцией «Электронного деканата» является хранение и обработка информации о ходе учебного процесса и его участниках, а также автоматизация взаимодействия между тремя участниками учебного процесса по электронной формой обучения: администрация – преподаватель – студент. Электронный деканат позволяет выполнять ряд функций традиционного деканата на более технологичном уровне, значительно сокращая время выполнения определенной работы традиционного деканата.

Связка СДО Moodle + «Электронный деканат» полезна организациям, которые внедрили или только собираются внедрять дистанционное обучение, прежде всего вузам, но не только им: модульная архитектура и открытость исходных кодов дает возможность адаптации под нужды любых организаций. ЭД дает возможность автоматизации управления учебным процессом и переноса привычной среды очного обучения на дистанционные курсы. Кроме того, ЭД разрабатывается российским сообществом программистов. Это дает легкую и быструю обратную связь и возможность принять участие в разработке нужных вам возможностей, тем самым сэкономив время, силы и деньги.

ЛИТЕРАТУРА

1. Сведения о преподавателях и студентах.
2. Учебный план по специальностям КОИБАС и ПиТЭВС.
3. Сайт проекта Free Dean's Office (Электронный деканат) [Электронный ресурс]. URL: http://www.deansoffice.ru/
4. Сообщество разработчиков Free Dean's Office [Электронный ресурс]. URL: http://www.infoco.ru/course/view.php?id=19
5. Документации по Free Dean's Office [Электронный ресурс]. URL: http://docs.deansoffice.ru/ru/Заглавная_страница

УСТАНОВКА ПЕРЕНОСА РИСУНКА НА ПЕЧАТНУЮ ПЛАТУ

К.И. Чугаевский, А.В. Леонидов, студенты каф. КИБЭВС
Научный руководитель Л.А. Торгонский, доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, seafores@gmail.com

Выполняемая работа посвящена созданию автоматизированной установки для переноса изображения на печатную плату (ПП) и подготовки ее для последующей обработки. Процесс работы установки включает следующие этапы:

– засветка слойного пакета в заданном режиме;

– задубливание фоторезиста термической обработкой (контроль температуры и времени воздействия).

Формирование слойного пакета происходит за пределами данной установки вручную.

На названных этапах принято решение контролировать температуру, интенсивность и время засветки и задубливания при помощи соответствующих датчиков. Для контроля процессов установка оснащается микропроцессорным контроллером [1, 2].

Упрощённая схема установки без средств управления представлена на рис. 1, где выделены две технологически зоны: зона экспонирования – *1* и зона задубливания – *2*.

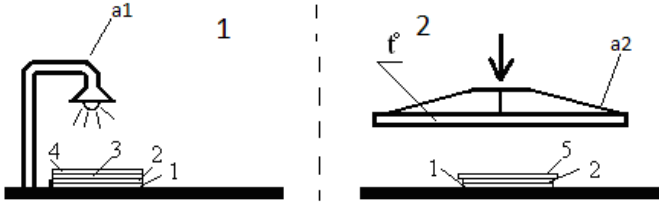


Рис. 1. Упрощенная схема установки

В зоне *1* выполняется облучение печатной платы в ультрафиолетовом диапазоне спектра. Подсветка осуществляется светильником *a*1. В зоне *2* выполняется подогрев печатной платы (ПП) с экспонированным фоторезистом через буферную тепловую прокладку (*5*), с контролем температуры прижимающей тепловой плиты *a*2 и времени прогрева.

Подготовка слойного пакета для экспозиции в зоне *1* выполняется за её пределами. Слойный пакет образуется из ПП (*1*) со слоем плёнки фоторезиста (*2*), подготовленной для облучения, напечатанным на прозрачной плёнке фотошаблоном (*3*), и прижимной оптически прозрачной прижимной пластины (*4*).

Время засветки устанавливается оператором с пульта. Интенсивность освещения регулируется в соответствии с алгоритмом управления светильником (циклическое включение-отключение лампы).

Аналогично в зоне *2* выполняется термообработка с установкой и контролем температуры и времени прогрева экспонированных пластин перед проявлением.

На рис. 2 показана схема управления установки. Установка включает в себя блоки управления светильником, нагревателем, датчики, исполнительные органы, пульт для ввода команд и отображения состояний.

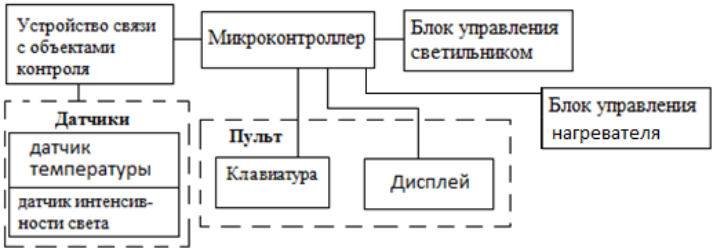


Рис. 2. Структура средств управления установкой

В текущее время выполняется проработка схем сопряжения устройства управления с датчиками и исполнительными органами, проработка конструкций модулей и программы управления от контроллера SDK 1.1 [3].

ЛИТЕРАТУРА

1. Бродин В.Б., Шагурин И.И. Микроконтроллеры. Архитектура, программирование, интерфейс. М.: Изд-во ЭКОМ, 1999. 401 с.

2. Дж. Смит. Сопряжение компьютеров с внешними устройствами. Уроки реализации. М.: Мир, 2000. 266 с.

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

РАЗРАБОТКА ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ НА СТЕНД-ТРЕНАЖЕР УЗЛОВ УЧЕТА ГАЗА

Д.А. Фаррахова, студентка каф. КИБЭВС

Научный руководитель О.В. Пехов, ассистент каф. КИБЭВС, аспирант

г. Томск, ТУСУР, Farrakhovad@gmail.com

Стенд-тренажер узла учета газа (далее стенд) отображает принцип работы узлов расхода газа. Узел учета газа – это комплекс средств измерений, предназначенных для измерения объемного, массового расхода, а также давления, температуры и других физических свойств природного газа по ГОСТ 5542, приведенных к стандартным условиям по ГОСТ 2939–63 по измерительным трубопроводам.

К работе на стенде допускается персонал, прошедший обучение по руководству на стенд, документации на комплектующие приборы, имеющий квалификационную группу по технике безопасности II согласно «Межотраслевым правилам по охране труда (правилам безопасности) при эксплуатации электроустановок» (ПОТ Р М-016–2001 РД 153-34.0– 03.150-00) и допущенный к работе с давлением. Техниче-

ское обслуживание средств измерения, входящих в узлы учета газа, производится специально обученным персоналом.

В связи с тем, что в учебном центре нет полного комплекта пакета документов, возникает проблема в ведении его в процесс обучения персонала.

Для решения проблемы необходимо разработать недостающие документы. В результате появится возможность провести переподготовку специалистов, что значительно повысит производительность труда на реальном объекте.

Принципиальная схема стенда представлена на рис. 1.

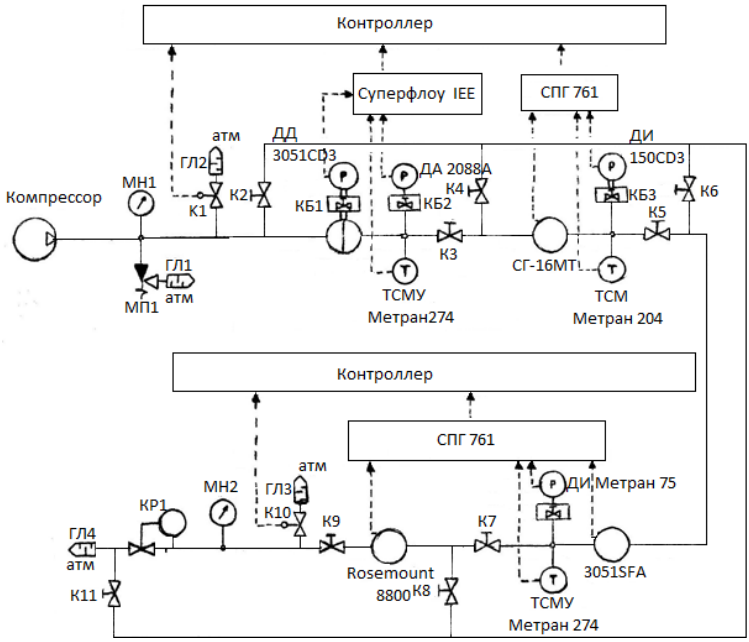


Рис. 1. Схема принципиальная стенда СТУ

Согласно паспорту стенд-тренажер предназначен для изучения принципов работы узлов расхода газа, а именно узлов на базе диафрагмы камерной стандартной (диафрагма ДКС), работающей совместно с датчиком разности давления Rosemount 3051 и вычислителем СПГ-761, турбинного счетчика газа СГ-16МТ, работающего совместно с вычислителем Суперфлоу 21В, расходомера серии Annubar PROBAR3051-SFA и расходомера – счетчика вихревого Rosemount 8800DR. Стенд состоит из каркаса стенда, системы трубопроводов и приборов.

При анализе нормативной документации на стенд в графическом конструкторском документе нет структурной схемы стенда-тренажера. В эксплуатационных документах отсутствуют инструкции по эксплуатации, по монтажу, пуску, регулированию и обкатке изделия, технике безопасности. В документах «Технические условия» отсутствуют технические требования, включающие в себя тактико-технические характеристики изделия, электрические и конструктивные параметры, допустимые условия эксплуатации, требования по надежности. Все документы разрабатываются в соответствии с ГОСТами. При внедрении документации в учебную деятельность проблема будет решена.

ЛИТЕРАТУРА

4. Стенд-тренажер СТУ. Руководство по эксплуатации. 16.0012.000.00 РЭ.
5. Стенд-тренажер СТУ. Паспорт. 16.0012.000.00 ПС.

РОБОТЫ-МАНИПУЛЯТОРЫ

Е.А. Федоскин, студент каф. КИБЭВС
Научный руководитель О.В. Пехов, ассистент каф. КИБЭВС
г. Томск, ТУСУР, Fedoskin_e@mail.ru

Целью данной работы является изучение роботов-манипуляторов, а также установка и настройка тестового стенда робота манипулятора.

Манипуляторы на основе пространственных механизмов платформенного типа обладают повышенной жесткостью, способны обеспечить достаточно высокие динамические характеристики при относительно небольшой металлоёмкости.

Манипулятор на основе пространственного механизма может использоваться для позиционирования инструмента, датчиков, приборов на мобильном информационном роботе, на гусеничном шасси, для поиска подземных электрических и коммуникационных кабелей, магистралей тепло- и водоснабжения, схемы прокладки которых утрачены и т.д. [1]. Другое актуальное направление использования мобильного информационного робота с манипулятором – это обследование состояния заброшенных ирригационных каналов сельскохозяйственных угодий или других мелиоративных сооружений на предмет обрушений, провалов, заиления, наличия зарослей кустарников, с целью последующего планирования восстановительных работ. Также манипулятор может управлять каким-либо инструментом либо перемещать деталь около него.

В составе робота есть механическая часть и система управления этой механической частью, которая в свою очередь получает сигналы

от сенсорной части. Механическая часть робота делится на манипуляционную систему и систему передвижения.

Манипулятор – это механизм для управления пространственным положением орудий и объектов труда.

Манипуляторы включают в себя подвижные звенья двух типов:

– звенья, обеспечивающие поступательные движения;

– звенья, обеспечивающие угловые перемещения.

Сочетание и взаимное расположение звеньев определяет степень подвижности, а также область действия манипуляционной системы робота. Для обеспечения движения в звеньях могут использоваться электрические, гидравлические и пневматические приводы. В последнее время все больше используются сервоприводы.

Программирование промышленных роботов делится на два вида:

– Online-программирование;

– Offline-программирование.

Online программированием называют программирование робота непосредственно на месте его установки с помощью самого робота. К данному способу относятся два метода: Teach-In (обучение) и Playback (проигрывание).

Offline – текстовой язык программирования и графическое программирование (3D-модели, CAD системы).

В ходе работы был установлен и настроен рабочий стенд-манипулятор (рис. 1). Данный манипулятор имеет пять степеней свободы, в которых робот-манипулятор может двигаться с помощью шести серводвигателей: база, плечо, локоть, запястье, щуп (рука), и сцепление.

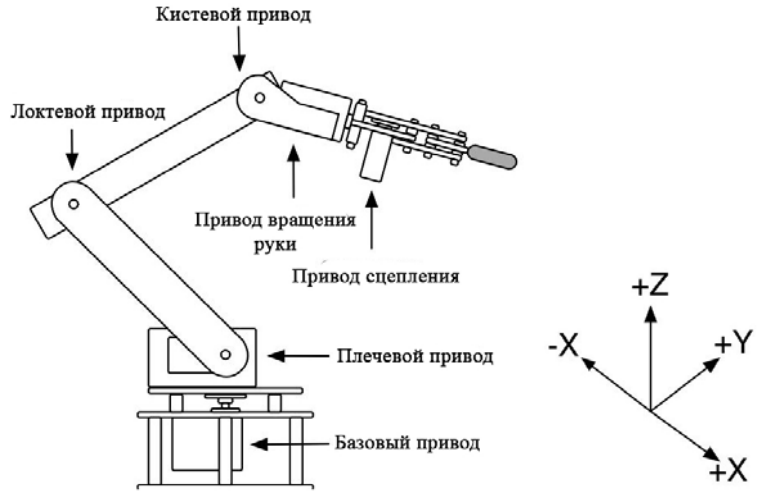


Рис. 1. Манипулятор

Для решения задачи позиционирования манипулятора в пространстве были определены начальные значения, рабочие области, начало координат и т.д. Координаты в пространстве для манипулятора определяются следующим образом:

– база манипулятора располагается на горизонтальной плоскости x, y;

– вертикальная ось z перпендикулярна плоскости x, y;

– центр основания принимается за начало координат x, y, z = 0, 0, 0.

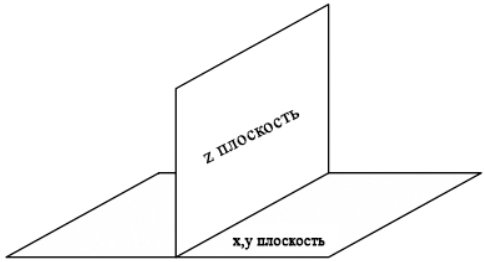


Рис. 2. Плоскости в пространстве

Серводвигатели контролируются широтно-импульсной модуляцией сигнала, в зависимости от которой изменяется положение сервопривода. Управляющая ширина импульсов варьируется от 500 до 2500 мкс, что соответствует углу поворота сервопривода от 0 до 180°. Для удержания позиции манипулятор должен получать постоянно сигнал на ШИМ с частотой не менее 1 раза в 20 мкс.

Для управления манипулятором была использована аппаратная платформа Arduino Uno. Реализована программа для контроллера, с помощью которой контроллер при получении определенного пакета данных разбирает его в соответствующие положения сервоприводов манипулятора. Формат пакета состоит из 18 цифр, по три на каждый мотор, и знака «!» для идентификации окончания пакета данных. Таким образом, если на порт контроллера послать данные вида «090090090090090090!», то каждый сервопривод встанет в нейтральное положение, равное 90 градусов, или длиной импульса 1500 мкс.

В дальнейшем следует реализовать обратную кинематику, при которой, задавая 4 входные координаты, контроллер преобразует эти данные в углы всех 6 сервоприводов.

ЛИТЕРАТУРА

1. Павловский В.Е., Евграфов В.В., Забегаев А.Н., Калиниченко и др. Экстремальная робототехника // Труды XXI Междунар. науч.-практ. конф. СПб.: Политехника-сервис, 2010. С. 103–108.

АСУ ТП ЭНЕРГОКОМПЛЕКСА НА ОСНОВЕ ПУШКИ С ПЛАЗМЕННЫМ КАТОДОМ

А.В. Крючков, научный сотрудник ООО «АСУ-ЭКСПЕРТ»,
В.В. Филатов, студент ФБ
г. Томск, ТУСУР, kaw@iao.ru

Современный этап развития АСУТП характеризуется применением индустриальных технологий создания и внедрения АСУТП на базе серийно выпускаемых промышленных контроллеров, совместимых с персональными компьютерами, и мощных программно-техничесих комплексов (ПТК) поддержки программирования АСУТП – SCADA-систем, а также развития и стандартизации сетевых технологий. Построение АСУТП на основе концепции открытых систем позволяет аппаратно-программные средства различных производителей совмещать снизу доверху и обеспечивать проверку всей системы. При таком подходе значительно уменьшается общая стоимость системы в результате применения более дешевого оборудования (при аналогичных функциональных характеристиках), частичной и поэтапной замене имеющихся на предприятии аппаратно-программных средств или даже сохранении некоторого старого оборудования [1].

Автоматизированная система управления технологическими процессами (АСУТП) – совокупность аппаратно-программных средств, осуществляющих контроль и управление производственными и технологическими процессами; поддерживающих обратную связь и активно воздействующих на ход процесса при отклонении его от заданных параметров; обеспечивающих регулирование и оптимизацию управляемого процесса.

Цели:

- повышение эффективности производственного процесса;
- повышение безопасности;
- повышение экономичности.

Задачи:

- автоматизированный сбор и обработка информации;
- визуализация информации в удобном для оперативного персонала виде;
- ручной ввод информации в систему с использованием пульта оператора или клавиатуры;
- снижение трудоемкости управления технологическими процессами;
- организация автономности управления (без помощи компьютера);
- контроль технологических параметров на физическую достоверность, на соответствие технологическому регламенту, на достижение аварийных границ.

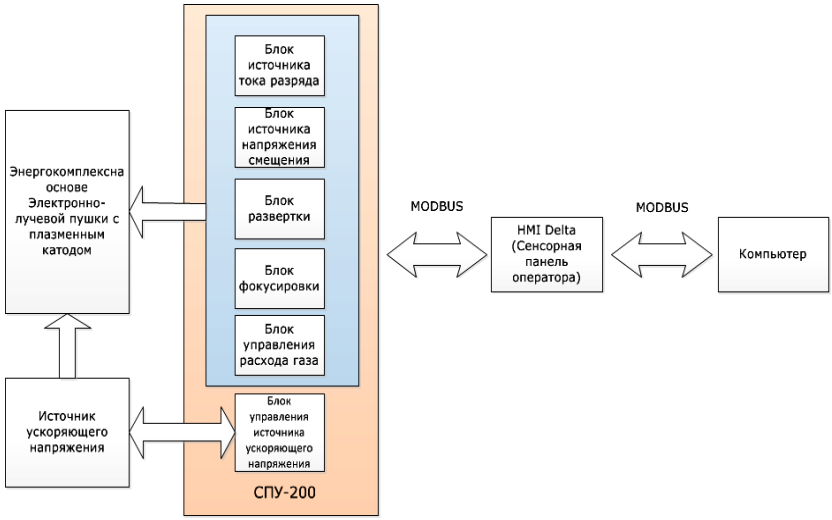


Рис. 1. Структура АСУ ТП для управления энергокомплексом [2, 3]

На рис. 1 представлена структура АСУ ТП, в которой главным звеном является сенсорная панель оператора HMI Delta, которая выступает в роли главного устройства сети. HMI Delta управляет всеми подчиненными элементами АСУ и берет на себя всю работу по обработке ввода и вывода информации на себя.

Заключение. Особенностью данной АСУ ТП являются автономность и законченность. Особенностью работы энергокомплекса являются постоянно возникающие высоковольтные пробои в вакуумной камере, сопровождающиеся электромагнитными помехами, приводящими к потере связи с компьютером. При отсутствии связи с системой верхнего уровня система АСУ ТП способна работать автономно в необслуживаемом режиме без потери информации, а при необходимости – осуществлять автономное дополнительное управление процессом, протекающим на энергокомплексе.

ЛИТЕРАТУРА

1. Втюрин В.А. Автоматизированные системы управления технологическими процессами. Основы АСУТП: учеб. пособие для студентов специальности 220301 «автоматизация технологических процессов и производств». СПб.: СПбГЛТА. 2006. 152 с.

2. Электронно-лучевой энергокомплекс на основе пушки с плазменным катодом [Электронный ресурс] // Официальный информационный портал университета. URL: http:// www.tusur.ru/ru/science/elaborations/elaborations/subjects/03/elekppk/info.html (дата обращения: 1.07.2013).

3. Электронная пушка с плазменным катодом [Электронный ресурс] // ЭЛИОН. URL: http://elion-tomsk.ru/ru/prod1.html (дата обращения: 11.11.2013).

ПОЗИЦИОНИРОВАНИЕ ЛУЧА ПРИ ЭЛЕКТРОННО-ЛУЧЕВОЙ СВАРКЕ

Т.Г. Вейсвер, ст. преподаватель, М.Ю. Морозов, аспирант
Научный руководитель В.Я. Браверман, профессор каф. САУ, д.т.н.
г. Красноярск, СибГАУ, каф. САУ, veisver@mail.ru

Установка для электронно-лучевой сварки (ЭЛС) как объект автоматизации представляет собой сложный комплекс, в который входит высокопроизводительное вакуумное и мощное энергетическое оборудование. Высокая скорость сварки и ограниченные возможности визуального наблюдения создают трудности оператору даже высокой квалификации в управлении процессом сварки. Поэтому стремление к максимальной автоматизации процесса закономерно. В настоящее время работы по автоматизации ЭЛС ведутся в направлении комплексной автоматизации с применением средств вычислительной техники [1].

Вторично-эмиссионные и видеосистемы управления ЭЛС, разработанные в 60–80-х годах прошлого столетия, не соответствуют критериям, предъявляемым к современному технологическому оборудованию. Большинство этих систем управления выполнено по децентрализованной двухкомпьютерной схеме, где один компьютер управляет взаимным перемещением свариваемых заготовок и электронно-лучевой пушки (ЭЛП) относительно друг друга, а второй – параметрами электронного луча. Для управления взаимным перемещением свариваемых деталей и ЭЛП, как правило, используются программы, написанные на едином стандартизованном языке ISO-7bit, а для управления электронным лучом – электронные таблицы либо программы на нестандартном языке программирования, как правило, собственной разработки. Синхронизация необходимых перемещений и изменения параметров электронного луча производятся оператором в ручном режиме. Такая схема построения системы управления устарела. Основные ее недостатки заключаются в отсутствии единой концепции построения систем управления для данного типа технологического оборудования и в необходимости совместной работы специалистов по электронно-лучевой сварке и по автоматизации технологического оборудования [3].

Важнейшим элементом системы наведения является датчик положения луча относительно стыка. От его выбора зависит точность совмещения луча со стыком свариваемых деталей, и, как следствие, качество сварного соединения. В качестве датчика возможно использовать систему автоматического наведения луча на стык с ПЗС-матрицей, регистрирующей излучения рентгеновского диапазона. ПЗС-

матрица (сокр. от «прибор с зарядовой связью») – специализированная аналоговая интегральная микросхема, состоящая из фотодиодов, выполненная на основе кремния, использующая технологию ПЗС-приборов с зарядовой связью [3].

Возможности ПЗС в части регистрации изображений ограничиваются шумами, основными из которых являются шумы считывания. Время передачи заряда из пикселя в пиксель характеризуется тактовой частотой, максимальное значение которой обусловливает допустимое время передачи зарядового сигнала из одного пикселя в другой. ПЗС-матрица – это безынерционный прибор, поэтому идеально подходит для высоконадежных цифровых технологий, в том числе и для регистрации рентгеновского излучения в процессах ЭЛС. Кроме того, известно, что величина рентгеновского излучения из сварочной ванны зависит от точности совмещения луча со стыком и тока луча [4].

ПЗС-матрицы выпускаются и активно используются компаниями Nikon, Canon, Kodak, Matsushita, Philips и многими другими. В России ПЗС-матрицы сегодня разрабатывают и выпускают: ОАО «ЦНИИ Электрон» (Санкт-Петербург) и его дочернее предприятие ЗАО «НПП Элар» (Санкт-Петербург).

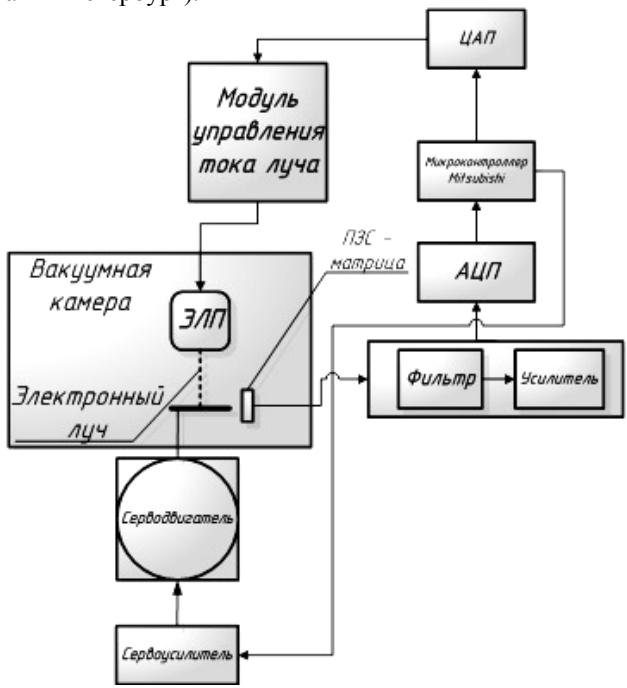


Рис. 1. Функциональная схема системы управления с ПЗС-матрицей

Работа системы с ПЗС-матрицей приведена на рис. 1. В вакуумной камере происходит процесс ЭЛС с инициацией рентгеновского излучения. На входе ПЗС-матрицы происходит фиксация рентгеновского излучения (сигнала), на выходе аналоговый сигнал попадает на фильтр и усилитель, далее аналого-цифровой преобразователь преобразует входной аналоговый сигнал в цифровой (дискретный код). После обработки микроконтроллер подает сигнал на сервоусилитель, далее – на сервопривод в вакуумной камере, тем самым осуществляя позиционирование пушки или изделия. Одновременно с этим сигналом микроконтроллера через канал управления можно изменять ток луча, а соответственно и глубину проплавления.

ЛИТЕРАТУРА

1. Управление процессом электронно-лучевой сварки с использованием информационных свойств плотности распределения электронного пучка. Режим доступа: http://www.dslib.net/avtomatizacia-upravlenia/upravlenie-processom-jelektronno-luchevoj-svarki-s-ispolzovaniem-informacionnyh.html

2. Расширение функциональных возможностей системы ЧПУ для управления установкой электронно-лучевой сваркой [Электронный документ]. Режим доступа: http://www.cniim.com/files/technology_svarka_2008.pdf

3. ПЗС-матрица. Режим доступа: http://ru.wikipedia.org/wiki/%CF%C7%D1-%EC%E0%F2%F0%E8%F6%E0

4. Браверман В.Я. Контроль глубины проплавления по интенсивности рентгеновского излучения при электронно-лучевой сварке / В.Я. Браверман, Т.Г. Вейсвер, В.С. Белозерцев // Вестник СибГАУ: сб. науч. тр. Красноярск, 2010. Вып. 6(32). С. 116–119 .

РАЗРАБОТКА МНОГОФУНКЦИОНАЛЬНОГО ИНФОРМАЦИОННОГО ТАБЛО ДЛЯ ВЫВОДА И ОБРАБОТКИ ИНФОРМАЦИИ

Е.В. Воронко, Р.В. Коновалов, студенты 4-го курса

Научный руководитель Д.В. Кручинин, ассистент каф. КИБЭВС

г. Томск, ТУСУР, каф. КИБЭВС, linha1992@mail.ru

Проект ГПО-1204 – «Разработка информационного табло для ввода и обработки информации на примере работы секретариата соревнований»

В современном мире донесение актуальной информации с места событий до широкой аудитории зрителей является неотъемлемой частью проведения соревнования любого вида спорта. Однако, как показал анализ рынка подобных устройств, они достаточно дороги, и ассортимент их не велик. Именно поэтому создание информационного

табло, отображающего всю необходимую информацию о данном состязании, является актуальной задачей.

В результате разработки многофункционального табло была спроектирована главная схема управления табло. Управление осуществляется микроконтроллером Atmega с дальнейшим выводом информации через сдвиговые регистры (рис. 1 – управляющая плата, рис. 2 – схема управляющей платы).

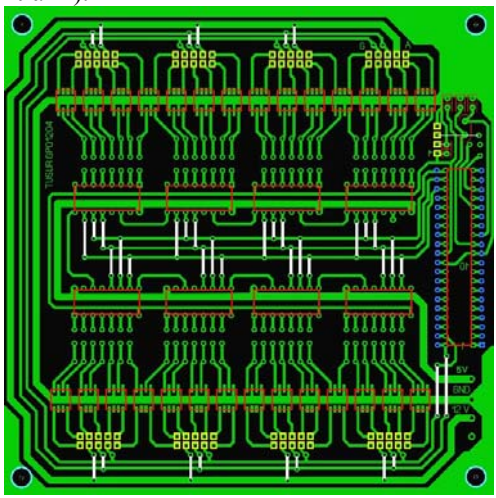


Рис. 1. Управляющая плата

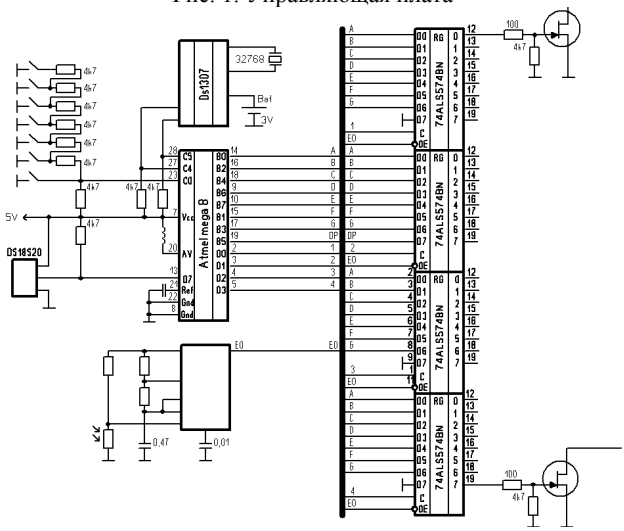


Рис. 2. Схема управляющей платы

Каждый сдвиговый регистр относится к своему семисигментному индикатору (рис. 3 – светодиодная плата).

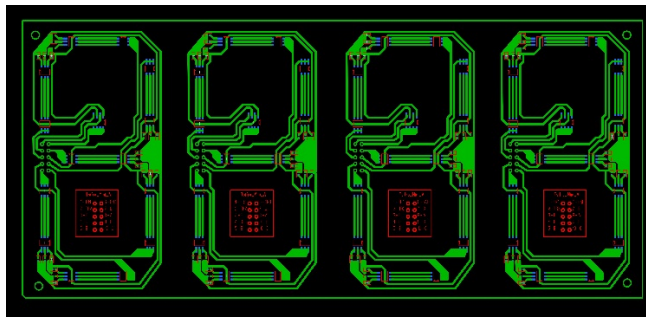


Рис. 3. Светодиодная плата

В зависимости от режима работы потребление электроэнергии различное. Так, например, в режиме полной функциональности каждый светодиод SMD5050 работает на полную мощность, потребляя значительное количество электроэнергии. Но при включении в режим минимального электропотребления светодиод светится значительно меньше, но и потребление также уменьшается (переключение осуществляется за счет того, что светодиод SMD5050 имеет три кристалла, тем самым происходит управление мощностью свечения). Управление режимами осуществляется микроконтроллером, который переключается mosfeet.

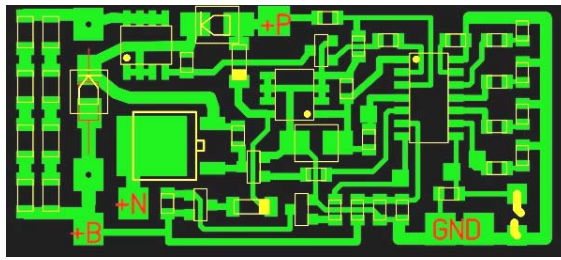


Рис. 4. Плата управления питанием

Питание табло также является немаловажным фактором. На рис. 4 изображена управляющая плата питания информационного табло. При подключении табло к розетке 220 В производится зарядка аккумулятора. После того как аккумулятор заряжен, зарядка прекращается и работа табло продолжается от сети. При отключении табло от питающей сети плата управления питанием автоматически переключается на резервное питание – аккумулятор.

Помимо самого табло, была реализована приемная (рис. 6) и передающая (рис. 5) части. Передающая часть (пульт ДУ) состоит из передатчика MAX1479 и шифратора команд ATMEGA8L, приемная часть состоит из MAX1473 – является супергетеродинным и может работать на частоте 315–433 МГц (подключается напрямую к основной схеме табло).

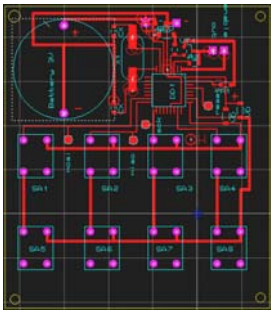


Рис. 5. Передатчик

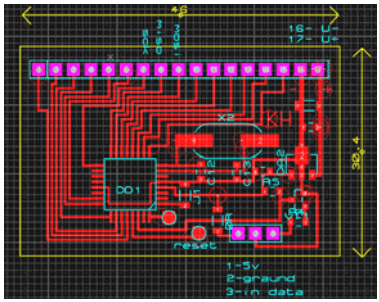


Рис. 6. Приемник

ЛИТЕРАТУРА

1. Джон Мортон. Микроконтроллеры AVR. Вводный курс. М.: Изд. дом «Додэка-XXI», 2006. 274 с.

2. Шустов М.А. Практическая схемотехника (1–3 ч.). М.: Альтекс-А, 2003.

СТРУКТУРНАЯ МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ В СФЕРЕ МОЛОДЕЖНОЙ ПОЛИТИКИ

Р.Р. Галин, м.н.с. ИСИБ

г. Томск, ТУСУР, ppos.grr@gmail.com

Рассматриваются структурная модель и показатели оценки эффективности государственного управления в сфере молодежной политики. Приводится сравнение оценки эффективности деятельности органов исполнительной власти субъектов РФ с предлагаемой авторской методикой.

На сегодняшний день вопрос эффективности государственной деятельности является направлением совершенствования системы государственного управления, и оценка данной эффективности объективно необходима, так как неэффективное государственное управление может привести к дестабилизации социально-экономической ситуации в обществе.

Важным направлением государственного развития является реализация молодежной политики. В Российской Федерации с момента проведения административной реформы [1] только в 2007 г. был создан федеральный орган исполнительной власти по делам молодежи с функционалом выработки и реализации государственной молодежной политики, а также по созданию условия для обеспечения здорового образа жизни, нравственного и патриотического воспитания молодежи, ныне данное направление курирует Министерство образования и науки РФ [2].

Методические подходы к оценке эффективности государственного управления в сфере молодежной политики. В целях повышения эффективности регионального управления были приняты Указ Президента РФ «Об оценки эффективности…» [3, 4], согласно которым рассматривается индикативный подход к оценке эффективности деятельности органов исполнительной власти по десяти разделам и 43 индивидуальным показателям. В рамках данного подхода представлен перечень из 12 показателей для оценки эффективности деятельности органов исполнительной власти субъектов РФ, характеризующих демографическую и финансово-экономическую стороны деятельности государственного управления.

Стоит отметить, что молодежная политика как обособленное направление государственного управления на всех уровнях не рассматривается в рамках оценки эффективности исполнительной деятельности органов государственной власти, при этом прорабатывается нормативная база, регулирующая развитие молодежи [5–7]. В свою очередь, молодежь является неотъемлемой частью формирования и воспроизводства общества [8–12], в рамках государственного управления которого необходимо принимать своевременные и грамотно выстроенные управленческие решения по развитию данного сектора.

Предлагается методика оценки эффективности государственного управления в сфере молодежной политики по трем направлениям, наиболее комплексно отражающим развитие, представленная в виде структурной модели (рис. 1).

Структура оценки государственного управления в сфере молодежной политики формируется на основе агрегирования оценок, полученных по основным направлениям оценивания деятельности органов исполнительной власти: «Оценка качества государственных и муниципальных услуг», «Оценка социально-экономического потенциала развития молодежной политики», «Оценка инфраструктуры молодежной политики».

Рис. 1. Структурная модель оценки эффективности государственного управления в сфере молодежной политики

Выводы. Как показывает исследование, подходы к оценке эффективности государственного управления в сферах жизнедеятельности человека не являются универсальными. Сложность адаптации методов оценки проявляется во взаимной зависимости качества и эффективности политики государства, т.е. качество не всегда может выступать положительным аспектом эффективности реализации политики, но также может повлиять и на конечный результат. Данное суждение показывает необходимость проведения интегральной оценки эффективности государственного управления, которая позволит оценить как среднесрочные результаты за отчетный период, так и конечные.

ЛИТЕРАТУРА

1. Указ Президента Российской Федерации от 23 июля 2003 г. № 824 «О мерах по проведению административной реформы в 2003–2004 гг.».

2. Указ Президента Российской Федерации от 21 мая 2012 г. № 636 «О структуре федеральных органов исполнительной власти».

3. Указ Президента Российской Федерации от 28 июля 2007 г. № 825 «Об оценке эффективности деятельности органов исполнительной власти субъектов Российской Федерации».

4. Указ Президента Российской Федерации от 01 ноября 2012 г. № 1142 «О мерах по реализации Указа Президента Российской Федерации от 21 августа 2012 г. № 1199 «Об оценке эффективности деятельности органов исполнительной власти субъектов Российской Федерации».

5. Концепция государственной молодежной политики в Российской Федерации. Одобрена протоколом заседания Правительственной комиссии по делам молодежи от 5 декабря 2001 г. №4.

6. Стратегия государственной молодежной политики в Российской Федерации. М., 2005.

7. Рудаков А.В. Механизм формирования и технологии реализации государственной молодежной политики РФ: дис. … канд. полит. наук: 23.00.02. Н.Новгород: РГБ, 2006. Режим доступа http://diss.rsl.ru/diss/06/0229/060229002.pdf, ограниченный.

8. Родионова В.А., Колмогорцева С.Т. Молодежь и общество: Проблемы разработки и реализации молодежной политики. М., 2001. С. 35.

9. Беспаленко П.Н. Проектирование государственной молодежной политики в практике муниципального управления: автореф. дис. … канд. социол. наук. Белгород, 2001. С. 1–12.

10. Галин Р.Р., Мещеряков Р.В. Методика оценки качества государственных услуг в сфере молодёжной политики // Качество. Инновации. Образование. 2013. № 10. С. 61–65.

11. Алескеров Ф.Т., Головщинский К.И., Клименко А.В. Оценки качества государственного управления. М.: ГУ ВШЭ, 2006. 36 с.

12. Глухова М.Ф. Инфраструктура региональной молодежной политики: основные признаки и типологии // Регионология. 2011. № 2 [Электронный ресурс]. Режим доступа: http://regionsar.ru/node/684.

ПРИМЕНЕНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ НАХОЖДЕНИЯ ОПТИМАЛЬНЫХ ПАРАМЕТРОВ НАСТРОЙКИ АСР ТЕМПЕРАТУРЫ ОСТРОГО ПАРА КОТЛОАГРЕГАТА ТПЕ-214

В.В. Глезер, студент

Научный руководитель А.В. Сафронов, ассистент каф. ТЭС

г. Новосибирск, НГТУ, glezer.v.v@gmail.com

Энергетика – это отрасль с большим объемом автоматизации. Если в конце XX в. теплоэнергетические процессы были автоматизированы на 70–80%, то уже в начале XXI в. объем автоматизации стал достигать 90–95%. При этом если раньше затраты на автоматизацию составляли порядка 4–5% от стоимости основного оборудования, то сейчас эта цифра увеличилась до 15–20% [1].

Развитие микропроцессорной техники позволило реализовать более сложные законы регулирования основных параметров. Так, доля применения ПИД закона регулирования составляет в одноконтурных системах 64%, а в двухконтурных – 36% [2].

В связи с более сложными структурами регуляторов на сегодняшний день актуальным вопросом является моделирование технологических объектов регулирования с целью предварительной настройки АСР перед монтажом ПТК на объекте.

При этом в качестве регулятора используется программируемый логический контроллер (ПЛК) с реализованным в нем алгоритмом работы регулятора (рис. 1).

«Р» – регулятор, выполненный конкретным производителем и реализующий тот или иной закон регулирования; «ОР» – математическая модель объекта регулирования, достаточно полно и точно описывающая реальную систему, в которой предполагается использовать данный регулятор.

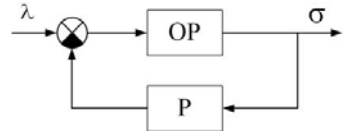


Рис. 1. Структураная схема одноконтурной АСР

После создания математической модели объекта регулирования поднимается задача о связи модели с ПЛК. Существует три пути решения данной задачи (рис. 2):

1) выходные данные из математической модели поступают на вход цифроаналогового преобразователя (ЦАП). После этого они заводятся во входы ПЛК. Выходные сигналы с ПЛК поступают обратно в персональный компьютер (ПК) через аналогово-цифровой преобразователь (АЦП);

2) коммутация двух систем происходит через технологию OPC (OLE for Process Control);

3) прямое обращение к входам/выходам ПЛК через драйверы.

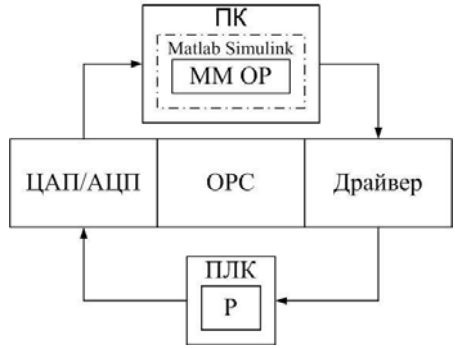


Рис. 2. Схема возможных решений реализации связи

Наиболее простым и в то же время самым эффективным путём является применение OPC-сервера [3]. Использование открытого коммутационного протокола позволяет использовать единую математическую модель для ПЛК различных производителей.

Данная система была апробирована на модели тракта острого пара котла ТПЕ-214, реализованной в среде «MATLAB SIMULINK», и регулятора в контроллере «ОВЕН ПЛК 150», обменивающихся данными через OPC-сервер «CoDeSys OPC».

По параметрам переходного процесса, снятых с котлоагрегата ТПЕ-214, была проведена аппроксимация. Полученная математическая модель была реализована в «MATLAB SIMULINK», (рис. 3). Далее был реализован блок регулятора в контроллере «ОВЕН ПЛК 150». Проведено сопряжение математической модели и ПЛК, используя

ОРС-сервер. Определены оптимальные настройки регулятора и проверено, что полученная система удовлетворяет заданным требованиям показателей качества переходного процесса.

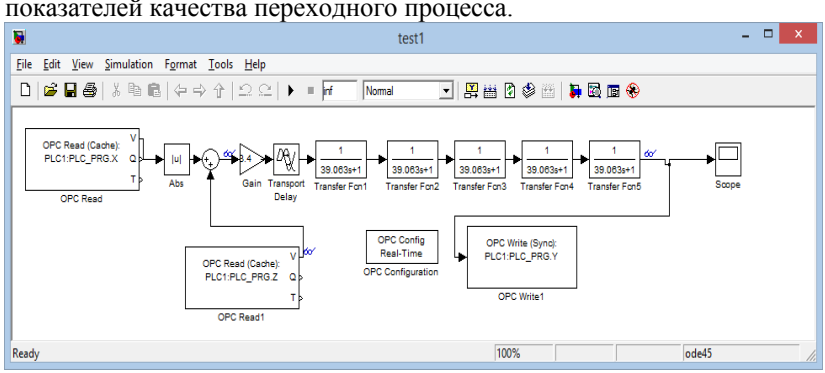


Рис. 3. Математическая модель в среде «Matlab Simulink»

Использованный подход хорошо себя зарекомендовал. Используя высокие вычислительные мощности современных ЭВМ, можно разрабатывать модели с достаточно высокой точностью, большой информативностью и возможностью расчета в режиме мягкого реального времени.

ЛИТЕРАТУРА

1. Новиков С.И. Оптимизация систем автоматизации теплоэнергетических процессов. Ч. 1. Автоматические системы регулирования теплоэнергетических процессов с аналоговыми регуляторами: учебник. Новосибирск : Изд-во НГТУ, 2011. 284 с.

2. Новиков С.И., Сафронов А.В. Метод экспериментального определения Д-составляющей ПИД-регулятора // Энергетика и теплотехника: сб. науч. трудов / Под ред. В.Е. Накорякова. Новосибирск : Изд-во НГТУ,2010. Вып. 15. С. 127–136.

3. Глебов Р.С. Моделирование системы управления в реальном времени // Автоматизация в промышленности. 2014. №1. С. 57–59.

ПРИМЕНЕНИЕ МЕТОДА СТЯГИВАНИЯ ОКНА В КОРРЕЛЯЦИОННО-СПЕКТРАЛЬНОМ АНАЛИЗЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ЭКСТРУЗИИ

В.С. Головко, С.А. Федосеева, магистранты 1-го курса
каф. автоматики и управления в технических системах
г. Самара, Самарский государственный технический университет
adamantv@mail.ru

Традиционные оптимальные по типовым критериям системы управления не могут быть использованы применительно к задачам

управления производством кабелей связи, поскольку они не учитывают частотную структуру возмущений [1]. Для исследования и оптимизации таких систем предпочтительно использовать аппарат корреляционно-спектрального анализа.

В ходе статистического обследования случайных процессов при построении оценок спектральных плотностей исследуемых параметров часто возникает необходимость в их сглаживании. Оценка спектральной плотности должна быть положительной на всех частотах, что обусловлено физическим смыслом – мощность сигнала не может быть отрицательной [2]. На практике это условие не всегда выполняется из-за влияния случайных ошибок.

На рис. 1 представлен график оценки спектральной плотности, построенный с использованием экспериментальных данных реального объекта – реализации диаметра изоляции, полученной на экструзионной линии в ходе изготовления LAN-кабеля на Самарском кабельном заводе. Наглядность графика обеспечивается логарифмическим масштабом по оси абсцисс. Для построения оценки спектральной плотности диаметра изоляции использовалась формула (1):

$$S(f) = \int_{+\infty}^{-\infty} R(\tau) \cdot \cos 2\pi f \tau d\tau, \quad f \in (-\infty; +\infty), \tag{1}$$

где $R(\tau)$ – корреляционная функция исследуемого процесса.

Из рис. 1 видно, что данная оценка спектральной плотности не удовлетворяет условию положительности на всех частотах. Для ее сглаживания удобно использовать процедуру стягивания корреляционного окна, которая используется для уменьшения дисперсии случайной ошибки оценки спектральной плотности [3].

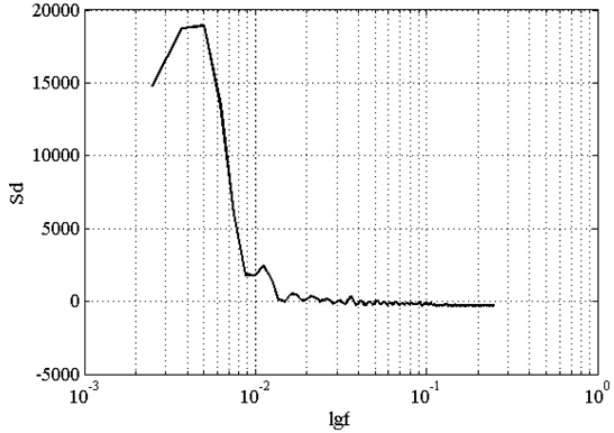


Рис. 1. Оценка спектральной плотности диаметра изоляции

Допустим, случайный процесс представлен реализацией размерностью N отсчетов. Может быть рассмотрена ее часть, видимая через так называемое окно, причем число отсчетов рассматриваемой части будет равно ширине окна m. Полагается, что ненаблюдаемые $N-m$ отсчетов равны нулю – производится стягивание окна.

Сглаженная оценка спектральной плотности находится по формуле (2):

$$S(f)=\int_{0}^{\tau_{max}} R(\tau)\cdot k(\tau)\cdot\cos 2\pi f\tau d\tau;\ f\in[0,f_{в}], \qquad (2)$$

где $\tau_{max}=mT_0$; $k(\tau)$ – функция корреляционного окна; T_0 – интервал дискретизации.

Если $k(\tau)=1$, то окно является прямоугольным. Такое окно обладает худшими свойствами. Предпочтительно использование корреляционных окон разной формы: Бартлетта (треугольное окно), Хэмминга (приподнятый косинус), Тьюки [4].

На рис. 2 показаны сглаженные оценки спектральной плотности диаметра изоляции, полученные с применением вышеперечисленных окон. Действительно, применение окон Бартлетта, Хэмминга и Тьюки является предпочтительным – сглаженные оценки спектральной плотности положительны на всех частотах. Прямоугольное окно, которое, по сути, является просто обрыванием корреляционной функции, действительно не обладает сглаживающими свойствами. Однако оно обладает наибольшей разрешающей способностью, острый пик спектральной плотности не «заваливается» на нижних частотах.

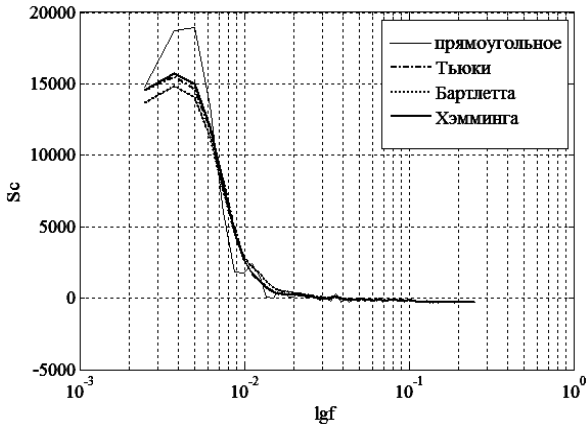


Рис. 2. Сглаженная оценка спектральной плотности

Варьируя ширину корреляционного окна, можно добиться оптимального результата. Чем меньше ширина, тем более сглаженной бу-

дет оценка. Однако важно соблюдать баланс, чтобы избежать потери данных. Обычно предпочтительная ширина окна составляет $m = 0{,}05 \div 0{,}1 \cdot N$.

В рассматриваемом примере длина число отсчетов реализации – 1800, а оптимальная ширина корреляционного окна составила 200 отсчетов.

Сглаженные оценки спектральной плотности мощности могут быть использованы для получения исходных данных для оптимизации управления технологическим объектом.

Например, в рассматриваемом примере это может быть управление частными параметрами качества изготовляемого кабеля – диаметром изоляции и погонной емкостью [1]. Возможна аппроксимация полученных сглаженных оценок спектральной плотности с целью синтеза моделей формирующих фильтров, что позволит получить параметрическую модель возмущающего воздействия.

ЛИТЕРАТУРА

1. Чостковский Б.К. Методы и системы оптимального управления технологическими процессами производства кабелей связи. М.: Машиностроение, 2009. 190 с.

2. Бендат Д., Пирсол А. Прикладной анализ случайных данных. М.: Мир, 1989. 540 с.

3. Чостковский Б.К. Моделирование и алгоритмизация процессов управления в стохастических системах с цифровыми регуляторами: учеб. пособие. Самара: СамГТУ, 2005. 134 с.

4. Дженкинс Г., Ваттс Д. Спектральный анализ и его приложения. Вып. 1 / Пер. с англ. М.: Мир, 1971. 316 с.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО СЕКРЕТАРИАТА СОРЕВНОВАНИЙ

Р.В. Коновалов, студент каф. КИБЭВС

Научный руководитель Д.В. Кручинин, ассистент каф. КИБЭВС

г. Томск, ТУСУР, archangel0804@mail.ru

Проект ГПО ФВС-1204 – «Инженерия баз данных»

Организация спортивных соревнований является трудоемкой работой. Все данные (о предстоящем соревновании, о его участниках и итогах проведения соревнования) необходимо где-то хранить и обрабатывать и, что является немаловажным, поднимать данные о прошедшем соревновании. Чтобы выполнить такие задачи, необходим не малый рабочий персонал, что является неэкономичным и неэффективным. Но сейчас в современном мире, где господствуют высокопроиз-

водительные вычислительные машины, они стали неотъемлемой частью нашей жизни. Поэтому разработка базы данных значительно упрощает как организацию, так обработку и хранение данных. Стоит заметить, что управление БД не требует большого персонала.

Создание программного комплекса по автоматизации ввода, вывода и обработки информации на примере работы секретариата соревнований производится поэтапно: реализация базы данных и разработка интерфейса.

Цель данной работы – разработка программного комплекса по автоматизации ввода, вывода и обработки информации на примере работы секретариата соревнований.

Первая этап – разработка базы данных – состоит из двух этапов: проектирования БД и создания БД. Проектирование включает в себя:

– системный анализ предметной области;

– анализ данных и построение модели данных.

Создание БД в памяти ЭВМ происходит в среде определенной СУБД и состоит из:

– создания структуры базы данных;

– заполнения базы данными.

Один из этапов – разработка реляционной модели. Модель данных описывает некоторый набор родовых понятий и признаков, которыми должны обладать все конкретные СУБД и управляемые ими базы данных, если они основываются на этой модели. Наличие модели данных позволяет сравнивать конкретные реализации, используя один общий язык.

После выполнения двух этапов нормализации была получена реляционная модель (рис. 1).

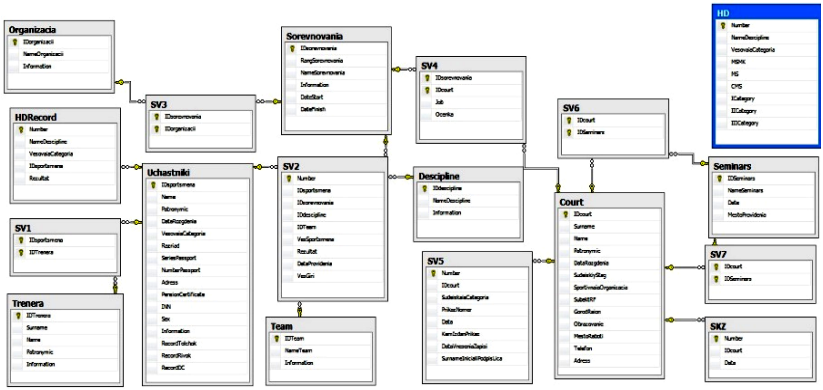


Рис. 1. Реляционная модель

Данная БД была реализована при помощи СУБД Microsoft SQL Server 2012.

На втором шаге рассматривается создание авторизации пользователя, простого графического интерфейса пользователя и добавление к нему несложной серверной функциональности (рис. 3) для более легкого учета соревнования, а также и возможность самим участникам просматривать данные о соревнованиях в сети при помощи авторизации (см. рис. 2).

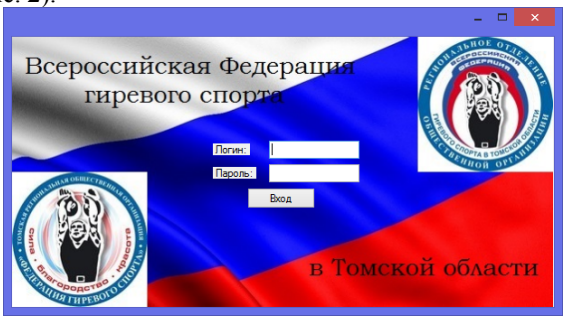


Рис. 2. Авторизация пользователя

В самой программе реализован подсчет данных о проведении соревнований согласно регламенту соревнований. А также к самой базе данных применимы определенные бизнес-процессы (например, ограничение возраста, масса тела). Согласно установленным нормам по получению разряда программа автоматически сравнивает эти данные, и если участник достигает этого результата, ему присваивается очередной разряд.

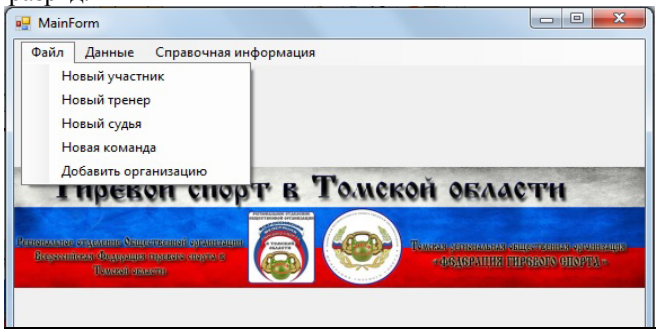


Рис. 3. Главная страница программы

Эта работа уже является продолжением работы ГПО, в программе реализован протокол ведения соревнований (рис. 4) согласно регламенту Федерации гиревого спорта. Была добавлена возможность вы-

вода на печать карточки участника, а также протокола соревнований. Были устранены ошибки относительно работоспособности триггеров, применяемых к таблицам добавления. Были переработаны графический интерфейс в более удобный, визуальное оформление (в связи со сменой символик Федерации).

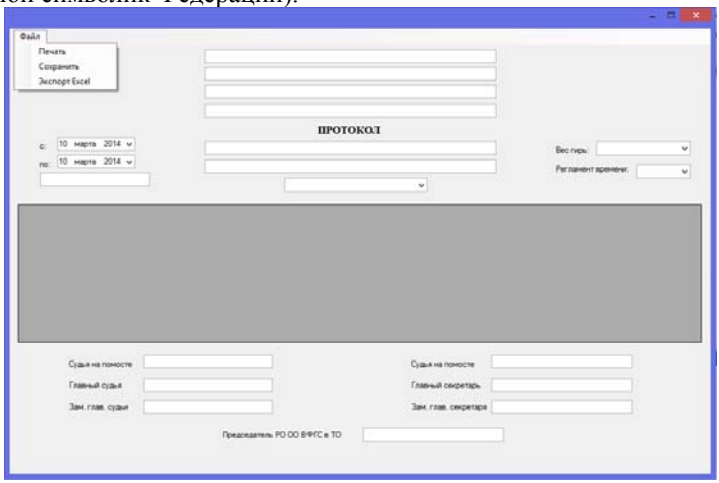


Рис. 4. Протокол соревнований

Заключение. На основе написанной программы данные, которые хранились в картотеках и имели большие объемы (как места хранения, так и объем информации), теперь в большом объеме хранятся в базе данных, и практически не занимают места хранения. А также при помощи автоматизации данных, подсчет всех данных лежит на программном обеспечении, где освобождает судейскую коллегию от подсчетов и экономит время на выявления победителя.

ЛИТЕРАТУРА

1. Новгородова Н.А. Лабораторный практикум по базам данных в Visual Studio (СУБД MICROSOFT ACCESS, MICROSOFT SQL SERVER). 2010. 265 с.

2. Библиотека MSDN. Справочник [Электронный ресурс]. URL: http://msdn.microsoft.com/ru-ru/library/ (дата обращения: 21.07.2013).

3. Методология проектирования БД [Электронный ресурс]. URL: http://database.ucoz.com/index/0-8 (Дата обращения: 16.09.2013).

4. C# и базы данных, ADO.NET [Электронный ресурс]. URL: http://www.cyberforum.ru/ado-net/ (дата обращения: 10.10.2013).

5. Вийера Роберт. Программирование баз данных Microsoft SQL Server 2008. Базовый курс.2008. 816 с.

6. Нильсон Пол. SQL Server 2005 Библия пользователя. 2008. 1228 с.

7. Учебные программы и курсы повышения квалификации MicrosoftInnovationCenter.

РОБОТ-СОРТИРОВЩИК

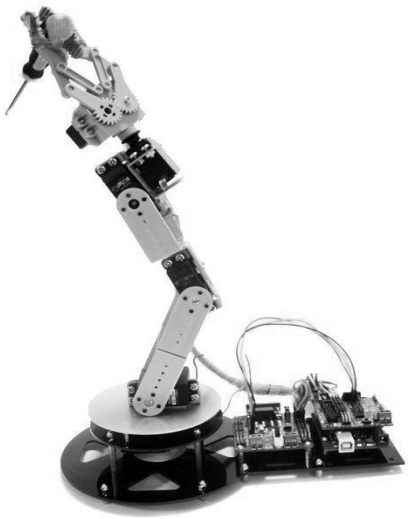
К.В. Левин, студент каф. КИБЭВС
г. Томск, ТУСУР, Konstantin_Levin@inbox.ru
Проект ГПО КИБЭВС-1202 – «Робототехника»

В современном быстро меняющемся мире единственный путь к сохранению рентабельности производства – постоянное внедрение новых технологий. Ввиду бурного развития автоматизации производства ведется большое количество разработок в области робототехники. Роботы позволяют решать огромный спектр различных задач, начиная от самых простейших и заканчивая задачами высочайшей сложности. При этом автоматизации может быть подвержен практически любой этап производства. Использование автоматизированных производств значительно уменьшает стоимость продукции за счет уменьшения количества человеческого труда. Промышленные роботы позволяют уменьшить количество персонала на предприятиях, увеличить объем производства, тем самым возрастает технологичность производства.

Сортировка продукции является задачей широкого применения. Сортировка осуществляется повсеместно: начиная с аппаратов по продаже напитков (сортировка полученных купюр по номиналу) и заканчивая массовыми производствами, например сортировка резисторов по номиналу. Примерами использования автоматизированных систем сортировки могут служить сортировка продукции в пищевой и фармацевтической отраслях [1]. Область применения робота-сортировщика не ограничена простой сортировкой. К примеру, его можно использовать с целью разбраковки производимой продукции или проверки содержимого упаковки.

В рамках разрабатываемого проекта планируется создать робота-сортировщика, способного сортировать продукцию по ряду необходимых критериев. Таким критериями, например, могут служить цвет, температура, размер. На основании данных критериев робот принимает решение о переносе продукта в ту или иную область. В ходе работы планируется создать одну из возможных моделей робота-сортировщика на основе аппаратной вычислительной платформы Arduino.

Разрабатываемый робот-сортировщик имеет шесть степеней свободы, обеспеченных шестью сервомоторами. Конструкция манипулятора изображена на рис. 1. Каждый сервомотор может поворачиваться на градус в диапазоне от 0 до 180 [2]. При этом управление сервомоторами осуществляется с аппаратной вычислительной платформы Arduino. Управление сервомоторами осуществляется на основе поступивших с датчиков данных. При этом для определения захвата пред-



мета будет использоваться тензодатчик, остальные датчики могут варьироваться в зависимости от сортируемых объектов. Изначально для сортировки предметов планируется использовать такие параметры, как цвет и размер. Для этого будут использоваться цветовой и ультразвуковой датчики соответственно.

Рис. 1. Конструкция манипулятора

В результате проделанной работы планируется создать робота-сортировщика, способного выполнять сортировку предметов по нескольким параметрам.

ЛИТЕРАТУРА

1. МКОИ – Автоматизация сортировки и отбраковки // Матер. сайта [Электронный ресурс]. URL: http://www.mkoi.org/366/367/373/ (дата обращения: 27.02.2014).

2. AS-6DOF Aluminium Robotic Arm Metal Arduino Robot Teaching Platform – Free Shipping – ThanksBuyer // материалы сайта [Электронный ресурс]. URL: http://www.thanksbuyer.com/as-6dof-aluminium-robotic-arm-metal-arduino-robot-teaching-platform-21716 (дата обращения: 27.02.2014).

ПРОЕКТИРОВАНИЕ СИСТЕМЫ МОНИТОРИНГА РЕЗЕРВУАРНОГО ПЛАНА

В.И. Маковкин, студент каф. АОИ

Научный руководитель Н.В. Замятин, профессор каф. АОИ, д.т.н.

В настоящее время активное развитие и увеличение в масштабе промышленных предприятий вызывает необходимость разработки различных специализированных систем сбора, обработки и отображения информации об их технических объектах. Подобные системы помогают удаленно и непрерывно наблюдать за работой любых устройств и, таким образом, получать от них необходимую информацию и оперативно реагировать на нее.

Большая часть предприятий самых разных отраслей и специализаций нуждается в системах наблюдения за объемом используемого сырья. Измерение уровня сырья требуется в большинстве производственных процессов; в системах экологического мониторинга и безопасности; для учета массы, расхода жидких продуктов при их хранении и транспортировке. Актуальность измерения уровня жидкостей возрастает по мере повышения степени автоматизации производственных процессов, систем контроля и учета.

Основными проблемами при разработке подобных систем являются:

- выбор типов устройств для измерения уровня сырья;
- проектирование схемы работы приборов, особенно в сложных и больших системах;
- разработка приложений для обработки и вывода данных, поступающих с устройств.

Существует широкая номенклатура средств контроля и измерения уровня, использующих различные физические методы. Эти методы и средства позволяют контролировать уровень различных сред: жидких (чистых, загрязненных), пульп, нефтепродуктов, сыпучих твердых различной дисперсности.

При выборе основного устройства для измерения уровня учитывались физические и химические свойства измеряемых веществ, таких как цемент, различные сыпучие вещества и смеси и нефтепродукты.

Для измерения уровня устройства можно разделить на подкатегории:

1) визуальные;

2) поплавковые – используется поплавок или другое тело, находящееся на поверхности жидкости;

3) буйковые – для измерения используется массивное тело (буек), частично погружаемое в жидкость;

4) гидростатические, основанные на измерении, и визуальные;

5) поплавковые – используется поплавок или другое тело, находящееся на поверхности жидкости;

6) и т.д.

Наиболее эффективными в данных средах оказались уровнемеры, использующие технологию на основе лазера импульсного действия. Подобные устройства состоят из импульсного лазера и детектора излучения. Измеряя время, которое затрачивает луч на путь до отражателя и обратно, и зная значение скорости света, можно рассчитывать расстояние между лазером и отражающим объектом. Способность электромагнитного излучения распространяться с постоянной скоростью дает возможность определять дальность до объекта. Такие датчи-

ки позволяют измерять уровень веществ даже в жестких индустриальных условиях при наличии пыли и пара.

Крупные предприятия обычно имеют много резервуаров и отдельно под них выделяют большие площади. Чтобы оптимизировать затраты и облегчить установку и работу системы, было решено использовать GSM/GPRS модемы ОВЕН ПМ01 для передачи данных. Таким образом, информация с уровнемеров будет передаваться по беспроводной сети со скоростью 42800 бит/с к модулю сбора данных (МСД), ОВЕН МСД200. Модуль сбора данных ОВЕН МСД200 применяется для опроса/прослушивания приборов, модулей ввода, контроллеров, имеющих возможность передавать данные в сеть RS-485. Обмен данных между МСД и рабочей станцией будет осуществляться по интерфейсу RS-485 с использованием протокола ModBus RTU.

На рабочей станции данные обрабатываются и записываются в базу данных на MySQL. MySQL – это свободная реляционная система управления базами данных, которая может распространяться в соответствии с условиями лицензии GPL. После обработки данные отображаются пользователю через прикладное приложение.

Приложение планируется разрабатывать на языке программирования Ruby, с использованием менеджера пакетов RubyGems и JRuby. Ruby – это динамический, рефлективный, интерпретируемый высокоуровневый язык программирования для быстрого и удобного объектно-ориентированного программирования. Кроссплатформенная реализация интерпретатора языка является полностью свободной. RubyGems – менеджер пакетов для языка программирования Руби, который предоставляет стандартный формат для программ и библиотек Руби, инструменты, предназначенные для простого управления установкой «gems», и сервер для их распространения. JRuby – интерпретатор языка программирования Ruby, написанный целиком на Java. Из Ruby-кода в JRuby можно вызывать классы Java, таким образом, можно получить доступ ко всем библиотекам, инфраструктурам и инструментам платформы Java.

Основное назначение JRuby в текущем приложении – написание GUI с помощью Java-библиотеки для создания графического интерфейса Swing.

С помощью приложения пользователь имеет возможность:

1) наблюдать за уровнями всех резервуаров;

2) просматривать все характеристики каждого резервуара (тип содержащегося вещества, плотность вещества, параметры резервуара и пр.);

3) редактировать характеристики резервуаров;

4) наблюдать статус работы каждого прибора (вкл/выкл/неисправен);

5) просматривать информацию о состоянии внешней среды (время, температура, влажность).

В дальнейшем планируется разработка прикладного приложения для работы с данными и поиск потенциальных заказчиков.

ЛИТЕРАТУРА

1. ОВЕН // Модуль сбора данных ОВЕН МСД200 [Электронный ресурс]. 2009. http://www.owen.ru/catalog/31257702 (дата обращения: 1.03.2014).

2. ОВЕН // GSM/GPRS модем ОВЕН ПМ01 [Электронный ресурс]. 2009. http://www.owen.ru/catalog/19726803 (дата обращения: 1.03.2014).

3. Ruby [Электронный ресурс]. 2006. https://www.ruby-lang.org/ru/ (Дата обращения: 1.03.2014).

4. Wikipedia // Swing (Java) [Электронный ресурс]. 2009. http://en.wikipedia.org/wiki/Swing_(Java) (дата обращения: 1.03.2014).

5. JRuby // The Ruby Programming Language on the JVM [электронный ресурс]. 2009. http://jruby.org/ (дата обращения: 1.03.2014).

КЛАССИФИКАЦИЯ И МОДЕЛИРОВАНИЕ МАНИПУЛЯТОРОВ ПРОМЫШЛЕННЫХ РОБОТОВ

Г.С. Маликова, студентка, Ю.О. Лобода, доцент, магистрант ФИТ

Научный руководитель Ю.О. Лобода, доцент

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

Промышленный робот (далее ПР) – это автономное устройство, состоящее из механического манипулятора и системы управления, позволяющее перепрограммировать в широких пределах движения исполнительных органов манипулятора. Промышленный робот состоит из исполнительного устройства в виде манипулятора и устройства программного управления. Манипулятор ПР предназначен для выполнения двигательных функций при перемещении объектов в пространстве. Это механизм для управления пространственным положением орудий, объектов труда и конструкционных узлов и элементов [1].

В данной работе была поставлена задача составления классификации промышленных роботов, оснащенных манипуляторами, и описание моделей манипуляторов на базе EV3, NXT 2.0 и Arduino.

В данной работе приведена классификация промышленных роботов, оснащенных манипуляторами, по десяти основным признакам. По характеру выполняемых операций существуют производственные ПР, подъемно-транспортные, универсальные. По специализации: специ-

альные, специализированные, универсальные. По назначению: литейные, сварочные, прессовые, для механической обработки, сборочные. По числу степеней подвижности: с тремя степенями подвижности, с четырьмя степенями подвижности, с пятью степенями подвижности, с шестью степенями подвижности и ПР, имеющие более шести степеней подвижности. По грузоподъемности: сверхлёгкие, лёгкие, средние, тяжёлые, сверхтяжёлые. По способу размещения: напольные, подвесные и встраиваемые. По типу привода: электрические, гидравлические, пневматические, комбинированные. По количеству манипуляторов: одноманипуляторные (однорукие), двурукие, трехрукие, четырехрукие. По типу систем управления: программные, адаптивные и интеллектуальные. По типу координатных перемещений: декартовы, с избирательной гибкостью, параллельные, шарнирные.

Робототехнический набор Lego Mindstorms NXT 2.0 включает в себя модуль NXT 2.0, датчик света, датчик нажатия, датчик звука, ультразвуковой датчик, три больших сервомотора. Робототехнический набор Lego Mindstorms EV3 включает в себя модуль EV3, датчик цвета, датчик касания, инфракрасный датчик, два больших и один средний сервомотор. Манипуляторы ПР базируются на сервомоторах. Сервомотор – это регулируемый редукторный электродвигатель. Он состоит из приводного механизма с электродвигателем постоянного тока, платы управления и потенциометра, который обеспечивает обратную связь. Три больших сервомотора NXT 2.0 дают роботу возможность двигаться. В каждый мотор NXT 2.0 встроен датчик вращения. Он позволяет точнее вести управление движениями робота. Lego Mindstorms EV3 имеет два больших сервомотора и один средний. Средний мотор EV3 также имеет встроенный датчик вращения, но он меньше и легче, чем большой мотор. Это означает, что он способен реагировать быстрее, чем большой мотор. Robotic Arm 6dof является манипулятором, оборудованным шестью сервомоторами.

В комплект поставки входят специализированный контроллер и программное обеспечение. Манипулятор имеет шесть сервомоторов, из них два мотора Hitec Servo 311, управляющих «запястьем», два мотора DF15MG Servo, отвечающих за подъем и поворот руки, один мотор DF05BB Servo, управляющий захватом, и один мотор HS422 Servo, отвечающий за поворот платформы [2]. Сервомотору необходимо указывать направление вращения. Это происходит с помощью импульсов. При поступлении импульса в управляющую схему, имеющийся в ней генератор импульсов производит импульс, длительность которого определяется через потенциометр. Другая часть схемы сравнивает длительность двух импульсов. Если длительность разная, включается электродвигатель. Рассмотрим пример программы, с помощью кото-

рой задаем три угла поворота выходного вала сервомотора, используя управление изменением непосредственно значения ширины импульса:

```
#include <Servo.h> //добавление библиотеки для работы с сервомоторами;
#define servoPin 9// 9 пин является servoPin – ом;
#define servoMinImp 544 //стандартная длина импульса при которой сервомотор должен принять положение 0° составляет 544 мкс;
#define servoMaxImp 2400 //стандартная длина импульса при которой сервомотор должен принять положение 180° составляет 2400 мкс;
Servo myServo;
void setup()
{
myServo.attach (servoPin, servoMinImp, servoMaxImp);
//установка пина, как вывода для управления сервомотором;
//задание минимального и максимального значения импульсов;
//импульсы с большей или меньшей длиной восприниматься не будут;
}
void loop()
{
myServo.writeMicroseconds(servoMinImp); //установка сервомотора в положение 0°;
delay(2000);
myServo.writeMicroseconds(1520); //установка сервомотора в положение 90°, что соответствует длине импульса равной 1520мкс;
delay(2000);
myServo.writeMicroseconds(servoMaxImp); //установка сервомотора в положение 180°, что соответствует длине импульса равной 2400 мкс;
delay(2000);
} [3]
```

В заключение можно провести сравнительный анализ манипуляторов на базе NXT 2.0, EV3 и Robotic Arm 6dof. Манипулятор на базе NXT 2.0 является громоздким и наименее точным, но при этом обладает лучшей грузоподъемностью. Манипулятор на базе EV3, благодаря наличию среднего сервомотора, является менее громоздким, обладает более высокой степенью точности, но при этом меньшей грузоподъемностью. Манипулятор Robotic Arm 6 dof обладает шестью сервомоторами, благодаря чему является более подвижным. У основания мани-

пулятора Robotic Arm 6 dof расположен более мощный сервомотор. Таким образом, делаем вывод, что манипулятор Robotic Arm 6 dof является более универсальным, в дальнейшем планируется разработка комплекса лабораторных работ на его базе.

ЛИТЕРАТУРА

1. Манипулятор (механизм) [Электронный ресурс]. Режим доступа:http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D0%BD%D0%B8%D0%BF%D1%83%D0%BB%D1%8F%D1%82%D0%BE%D1%80(%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D0%B8%D0%B7%D0%BC) (дата обращения: 28.01.2014).

2. Рука манипулятор 6 dof. [Электронный ресурс]. – Режим доступа:http://www.hobbylab.ru/catalog/comps/handles_and_grips/rob0036/ (дата обращения: 18.01.2014).

3. Сервоприводы [Электронный ресурс]. Режим доступа: http://wiki.amperka.ru/робототехника:сервоприводы (дата обращения: 20.02.2014).

ИССЛЕДОВАНИЕ ОСНОВНЫХ ХАРАКТЕРИСТИК ДАТЧИКА ЦВЕТА

Ю.О. Лобода, доцент каф. КИБЭВС, магистрант ОКЮ,
Ю.К. Малофий, студент ФБ
г. Томск, ТУСУР, akcia@mail.ru

Целью данной работы является изучение основных характеристик датчика цвета в конструкторе LEGO MINDSTORMS NXT.

Датчик цвета – это понятие в системах управления, первичный преобразователь, элемент измерительного, сигнального, регулирующего или управляющего устройства системы, преобразующий контролируемую величину в удобный для использования сигнал, позволяющий регистрировать видимый спектр излучения.

Существуют 2 вида датчиков цвета, которые основаны на различных принципах работы и могут быть использованы для моделей роботов на базе LEGO MINDSTORMS. Датчик LEGO использует светодиод RGB. Отраженный свет улавливается световым датчиком, чувствительным к волнам разной длины.

Датчик HiTechnic имеет белый светодиод и специализированный цветочувствительный чип. Этот чип имеет три чувствительные области, покрытые красным, зеленым и синим светофильтрами. Дополнительное преимущество метода HiTechnic состоит в том, что он может обнаружить цвет света, посланного на него (в пассивном режиме, с отключенным белым светодиодом).

Рис. 1. Датчик LEGO

Рис. 2. Датчик HiTechnic

Каждый датчик имеет сильные стороны и будет лучшим в различных ситуациях. Датчик цвета LEGO лучше всего покажет себя в случае, когда важна скорость определения цвета, например в случае продвижения по цветной линии. Датчик HiTechnic будет полезен, когда трудно осветить экран датчика или когда необходимо распознавание большего количества цветовых оттенков.

Цветовой датчик работает в трех режимах:

1) Различает цвета предметов в режиме Color Sensor. Каждому цвету соответствует число, возвращаемое функцией, различаются шесть цветов (стандартные цвета LEGO-деталей).

2) Фиксирует внешнее освещение и выдает результат в условных единицах. В режиме измерения окружающей освещенности количество света, попавшее на светочувствительный элемент, преобразуется в цифровое значение, которое уже используется в программе. Например, с датчиком, работающим в этом режиме, можно собрать робота, который ищет самое освещенное место в комнате.

3) Фиксирует отраженный свет, созданный собственным излучателем, и выдает результат в условных единицах. В режиме измерения отраженного цвета, помимо светочувствительного элемента, активируется светодиод. Свет, выпущенный этим элементом, отражается от какой-нибудь поверхности и попадает обратно в светочувствительный элемент.

В светочувствительный элемент приходит определенное количество света, измеряемое в условных единицах, которое преобразуется в цифровое значение и передается в программу. Чем темнее поверхность, тем меньшие значения приходят в программу; если поверхность светлее, программа оперирует с большими значениями.

В режиме Light Sensor датчик может работать с тремя различными типами подсветки – красным, синим или зеленым. Это может быть полезно для лучшего детектирования объектов различных цветов и в разных условиях освещенности.

Было решено провести эксперимент, в котором будет определяться максимальное расстояние, на котором датчик цвета способен разли-

чать цвета. Эксперимент проводился с использованием компьютерной среды LEGO MINDSTORMS NXT 2.0.

В ходе проведения эксперимента, основанного на способности датчика LEGO определять различные цвета на максимальном расстоянии от него, было выяснено, что датчик определяет все заявленные в конструкторской документации цвета. Любые темные или слабоосвещенные цвета датчик определяет как черный цвет. Измеренные цвета датчик определяет как черный, если их отодвинуть от датчика дальше. Таким образом, не удается определить точное максимальное расстояние, с которого датчик начинает обнаруживать черный цвет. Средние значения для определения максимальных расстояний: красный – 0,154 м, желтый – 0,157 м, светло-зелёный – 176 м, тёмно-зелёный – 0,198 м, синий – 0,149 м, белый – 0,174 м.

В результате проведения эксперимента выяснилось, что датчик определяет бордовый, оранжевый, коричневый и розовый как красный цвет, а фиолетовый и голубой – как синий цвет.

Датчики цвета могут быть использованы в самых разнообразных отраслях промышленности, например для контроля сортировки изделий по цвету.

ЛИТЕРАТУРА

1. Сравнение датчиков цвета [Электронный ресурс]. Образовательные инициативы от ХОЛИТ Дэйта Системс. URL: http://edu.holit.ua/index.php?option=com_content&view=article&id=235%3A2010-02-18-09-46-10&catid=64%3A2008-08-12-08-18-39&Itemid=74&lang=ru (дата обращения: 27.03.2013).

2. Разработка и исследование метода контроля цвета продукции с помощью датчиков на светодиодах и волоконной оптике [Электронный ресурс]. Радиотехнические и телевизионные системы и устройства. URL: http://tekhnosfera.com/razrabotka-i-issledovanie-metoda-kontrolya-tsveta-produktsii-s-pomoschyu-datchikov-na-svetodiodah-i-volokonnoy-optike (дата обращения: 22.10.2012).

3. Программирование LEGO Mindstorms NXT на языке NXC [Электронный ресурс] // МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ.URL: http://ed.tusur.ru/lit/edu/robotics/BricxCC.pdf / (дата обращения: 22.10.2012).

4. Разработка и исследование методов контроля цветовых характеристик объектов в производственных условиях [Электронный ресурс] // Радиотехнические и телевизионные системы и устройства. URL: http://www.dissercat.com/content/razrabotka-i-issledovanie-metodov-kontrolya-tsvetovykh-kharakteristik-obektov-v-proizvodstve (дата обращения: 22.10.2012).

РАЗРАБОТКА ВИРТУАЛЬНОЙ МОДЕЛИ СТЕНДА-ТРЕНАЖЕРА УЗЛОВ УЧЕТА ГАЗА

О.С. Марченко, студент каф. КИБЭВС

Научный руководитель О.В. Пехов, ассистент каф. КИБЭВС, аспирант

г. Томск, ТУСУР, marchenca@mail.ru

Узлы учета расхода газа – комплекс средств измерений, предназначенных для определения объемного, массового расхода, а также давления, температуры и других физических свойств газа.

Техническое обслуживание средств измерения, входящих в узлы учета газа, производится специально обученным персоналом. Обучение производится на имитационном оборудовании – стенде-тренажере узлов учета газа (СТУ). По причине его высокой стоимости в учебно-производственном центре стенд-тренажер присутствует в единственном экземпляре. При введении стенда СТУ в учебный процесс возникает проблема распределения времени индивидуального обучения на нем. Это объясняется тем, что обучение производится группами и время занятий ограничено.

Одно из возможных решений этой проблемы заключается в разработке виртуальной модели тренажера. Такая модель предоставит каждому специалисту возможность получения индивидуального «практического» опыта работы на стенде СТУ и снизит вероятность поломки реального стенда, связанную с некомпетентностью или неподготовленностью специалиста, а также позволит осуществлять дистанционное обучение.

Стенд СТУ [1, 2] состоит из каркаса стенда, системы трубопроводов и приборов. Схема принципиальная стенда представлена на рис. 1. При включении компрессора газ под давлением поступает на вход установки, где с помощью регулятора давления прямого действия устанавливается рабочее давление установки (0,2 МПа).

В рабочем режиме осуществляется считывание показаний измерительного оборудования путем преобразования параметров газа в аналоговый сигнал, который передается на корректор (вычислитель) для преобразования в цифровое значение и отображения на его дисплее.

Так как стенд СТУ представляет собой «дублирующую» систему, то показания средств измерения соответствующего параметра должны быть одинаковы. Если разница показаний соответствующих параметров газа превышает заданную погрешность, то необходимо провести настройку данного средства измерения с помощью корректора или с помощью специального оборудования.

По принципу действия все измерительные средства, расположенные на трубопроводе, условно можно разделить на следующие группы:

преобразователи расхода (счетчики газа), корректоры (вычислители) параметров газа, датчики давления и термопреобразователи сопротивления. В ходе преддипломной практики для каждой из этих групп были выбраны зависимости входных параметров от выходных.

Виртуальная модель разрабатывается с целью обучения специалистов особенностям работы с узлами учета газа на базе стенда СТУ. Основными задачами разработки являются моделирование интерфейса пользователя и основных режимов работы стенда (основного и байпасного), моделирование процессов измерения параметров газа и настройки средств измерения, а также непредвиденных ситуаций (обрыв датчиков и пробой трубопровода).

Модель подлежит разработке в среде Visio Studio C# [3] с применением форм создания Windows-подобных приложений. После анализа поставленных задач было решено, что виртуальная модель должна содержать окно выбора режима работы модели, окна для отображения режима работы стенда, визуальной модели стенда (основное окно), окно для настройки взаимодействия узлов учета газа и вычислителя (корректора), окно подсказки и окно настройки датчиков с помощью специализированного оборудования.

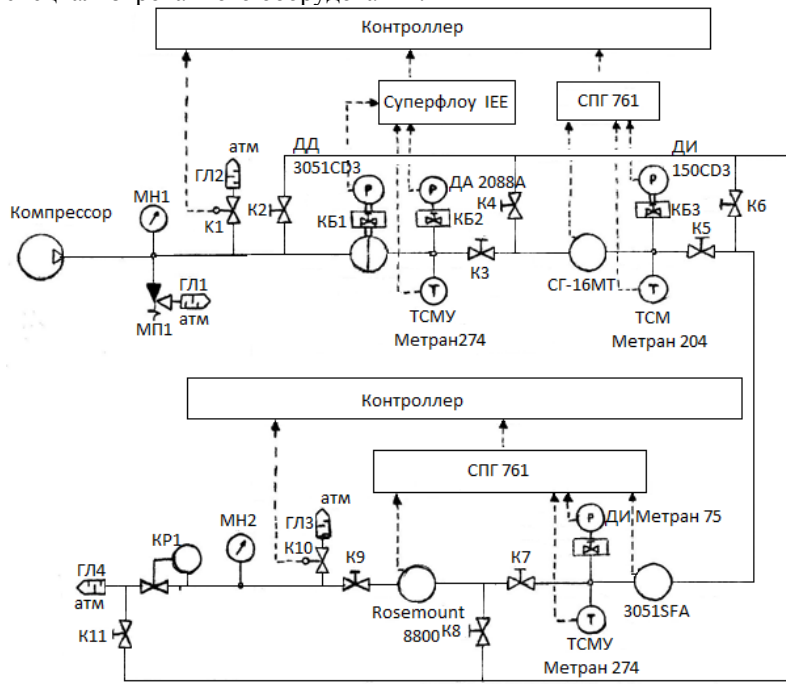


Рис. 1. Схема принципиальная стенда СТУ

Макет виртуальной модели представлен на рис. 2.

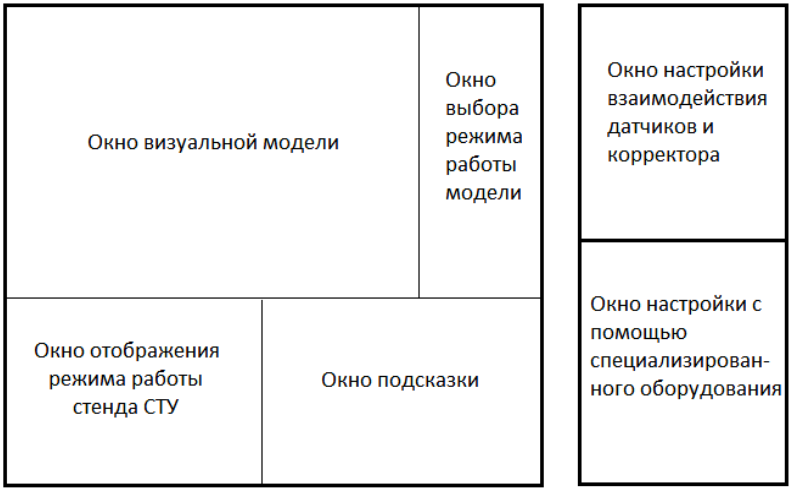


Рис. 2. Макет виртуальной модели стенда СТУ

Виртуальная модель должна содержать окно выбора режима работы, чтобы пользователь мог выбрать режим, подлежащий имитации, – симуляция непредвиденной ситуации или работа в стандартных условиях. Окно визуальной модели предполагается для наглядности процесса измерения параметров газа, а также для возможности управления при помощи виртуальной системы кранов маршрутом потока газа, для отражения которого необходимо окно отображения режима работы стенда. Чтобы выполнять лабораторные работы на стенде СТУ, должны быть предусмотрены окно для настройки взаимодействия датчиков и корректора и окно для настройки датчиков с помощью специализированого оборудования. Для того чтобы пользователь мог использовать все функциональные возможности разрабатываемой модели, было решено добавить макет приложения окно подсказки.

ЛИТЕРАТУРА

1. Стенд-тренажер СТУ. Руководство по эксплуатации. 16.0012.000.00 РЭ.
2. Стенд-тренажер СТУ. Паспорт. 16.0012.000.00 ПС.
3. Бишоп Дж. C# в кратком изложении / Дж. Бишоп, Н. Хорспул / Пер. с англ. М.: БИНОМ. Лаборатория знаний, 2005. 472 с.

ЭЛЕКТРИЧЕСКАЯ СХЕМА АУДИОМЕТРА

М.В. Горбунов, П.К. Звеглянич, И.А. Лысенко,
М.А. Михеев, Л.А. Патрашану, студенты 4-го курса каф. КИБЭВС
Научный руководитель Р.В. Мещеряков, доцент, д.т.н
г. Томск, ТУСУР, Konfetka-921@mail.ru
Проект ГПО КИБЭВС-1209 – «Исследование речевого сигнала»

Целью проекта является создание электроакустического прибора для измерения остроты слуха – аудиометра, основанного на воздушной и костной проводимости. Аудиометры предназначены для оценки функционального состояния слухового анализатора человека путем определения порогов слышимости по воздушному и костному звукопроведению путем сравнения слуха обследуемого с характеристиками, эквивалентными порогу слышимости нормального человека.

Актуальность проблемы обусловлена, прежде всего, необходимостью оказания специализированной помощи пациентам с ушной патологией. По данным статистики Всемирной организации здравоохранения, 7% населения страдают нарушением слуховой функции. По данным Минздрава России, нарушениями слуха в нашей стране страдают примерно 6% населения. В России насчитывается 12 миллионов больных с нарушением слуха, в том числе детей и подростков более 600 тысяч [1].

Исследуя рынок аудиометрии, можно увидеть массу дорогих аудиометров отечественного и зарубежного производства. Крупнейшими производителями аудиометров в мире являются компании «Entomed» (Швеция), «WelchAllyn» (США), «Interacoustics» (Дания) и компания «Maico» (Германия), из отечественных производителей найдена только одна компания «Биомедилен», выпускающая одну марку поликлинического аудиометра АА-2.

Проведен патентный поиск, объектом исследования стала аудиометрия как область измерений для диагностических целей. Ретроспектива поиска составила 15 лет. Классификационный индекс МПК A61B5/12. Согласно патентному поиску было найдено 72 патента. Аналогичных патентов предлагаемой разработки не было найдено [2].

К данному моменту разработки аудиометра были составлены функциональная и электрическая схемы.

Функциональная схема предназначена для разъяснения процессов, происходящих в отдельных функциональных цепях изделия или изделии в целом. На схеме изображают функциональные части изделия (элементы, устройства, функциональные группы) и связи межу ними. Функциональная схема представлена на рис. 1.

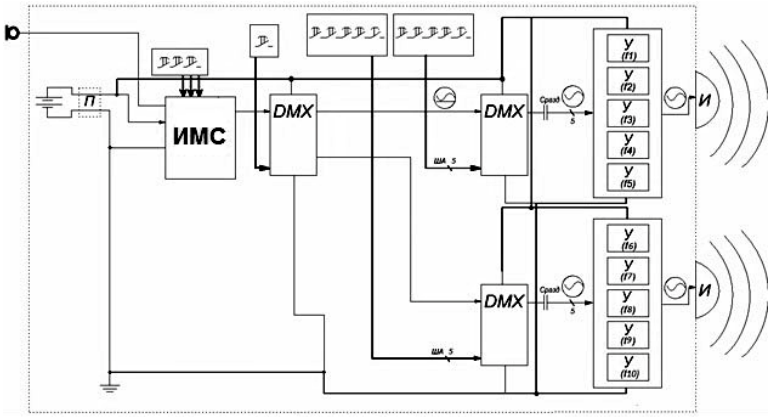


Рис. 1. Функциональная схема аудиометра: П – преобразователь напряжения питания; ИМС – интегральная микросхема ISD1416; У – усилительный каскад; И – излучатель вибрации; DMX – демультиплексор; ША – шина адреса

Опираясь на функциональную схему, была разработана электрическая схема аудиометра, представленная на рис. 2.

Электрическая схема – это чертеж, на котором показано упрощенное и наглядное изображение связи между отдельными элементами электрической цепи, выполненной с применением условных графических обозначений и позволяющей понять принцип действия устройства.

Данные схемы соответствуют ГОСТ 27072–86 «Генераторы сигналов диагностические звуковые. Аудиометры. Общие технические требования и методы испытаний» [3].

Алгоритм работы устройства будет заключаться в следующем:

1. Выбор вида проводимости с помощью переключателя – костной или воздушной.

2. Пользователь при помощи кнопок управления выбирает необходимые вид и интенсивность сигнала.

3. Микроконтроллер на встроенном ЦАП выдает сигнал с неоткалиброванным размахом напряжения.

4. На демультиплексоре сигнал направляется на калибровочные усилители (в зависимости от частоты). Демультиплексором управляет контроллер, задавая необходимый адрес.

5. На калибровочных усилителях реализуется необходимый размах напряжения.

6. Частота и уровень выбранного сигнала отображаются на индикационной панели, состоящей из 12 светодиодов.

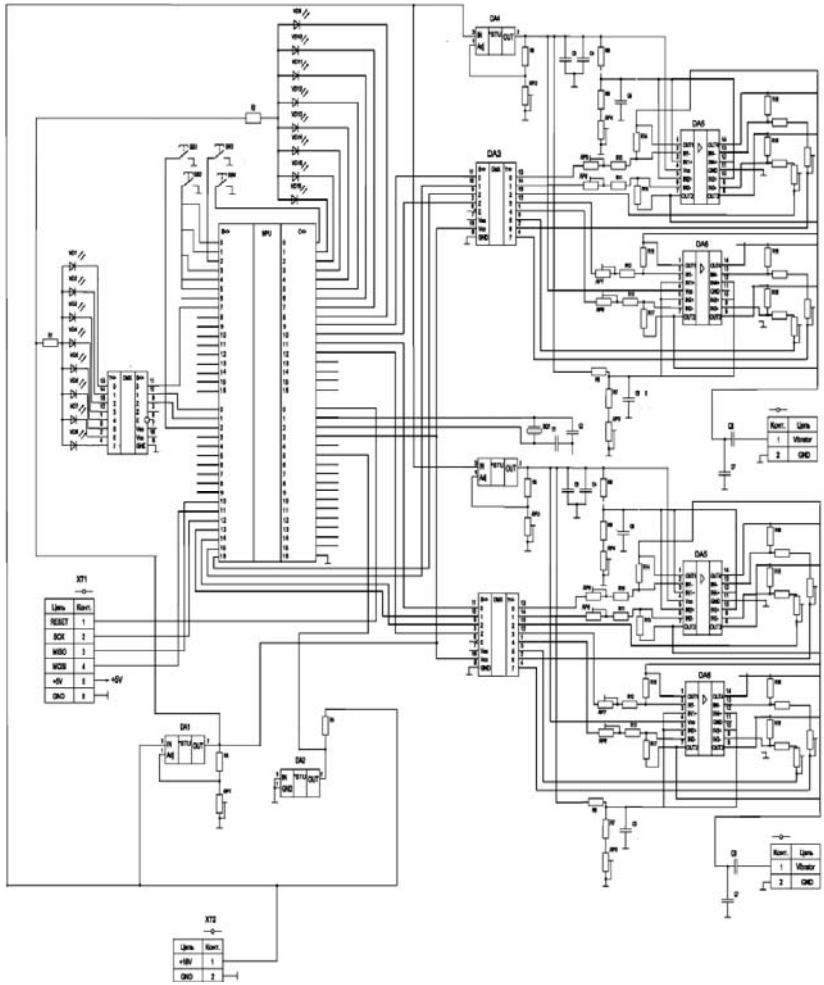


Рис. 2. Электрическая схема разрабатываемого устройства:
DA1,2,4 – стабилизатор напряжения; DA3,5,6 – микросхемы усилителей;
BQ1 – кристалл, задающий «вибрации»; SB1,2 – кнопки «вверх» и «вниз»;
XT1 – шлейф управления микросхемой (доп. питание, управление
и программирование схемы)

Ядром проектируемого аудиометра будет являться микроконтроллер. Предполагается, что он будет генерировать необходимые сигналов для костного и воздушного вибраторов: шести синусоид разной частоты, шума и голоса.

Вид сигнала и частота будут выбираться с помощью переключателей. Светодиоды будут использоваться для индикации выбранного сигнала. Использование светодиодов позволит сэкономить как на себестоимости прибора, так и на энергии.

Следующим этапом разработки предполагается сборка прибора и проведение испытаний. Также по возможности планируется уменьшить размеры прибора по сравнению с аналогами.

ЛИТЕРАТУРА

1. Альтман Я.А., Тавартkиладзе Г.А. Руководство по аудиологии. М.: ДМК Пресс, 2003. 360 с.

2. Дипломный проект «Аудиометр портативный, основанный на костной проводимости» / Том. ун-т систем управления и радиоэлектроники; разработчик: Нигматуллин Р.Ф. ФВС. Томск, 2010. 94 с.

3. ГОСТ 27072-86 Генераторы сигналов диагностические звуковые. Аудиометры. Общие технические требования и методы испытаний. М.: Гос. комитет СССР по стандартам, 1986. 35 с.

ПЕЧАТНАЯ ПЛАТА ПОРТАТИВНОГО АУДИОМЕТРА

М.В. Горбунов, П.К. Звеглянич, И.А. Лысенко, М.А. Михеев, Л.А. Патрашану, студенты каф. КИБЭВС

Научный руководитель Р.В. Мещеряков, доцент, д.т.н.

г. Томск, ТУСУР, Konfetka-921@mail.ru

Проект ГПО КИБЭВС-1209 – «Исследование речевого сигнала»

В данном проекте рассматривается создание аудиометра – прибора для измерения остроты слуха. Аудиометрия – это измерение остроты слуха, определение слуховой чувствительности к звуковым волнам различной частоты. Она позволяет исследовать как костную, так и воздушную проводимость.

Применение портативного скринингового аудиометра позволит врачам-отоларингологам своевременно направлять пациентов на хирургическое лечение. Также портативный прибор легко перевозить, а значит, можно использовать на выезде, в телеметрической медицине. В перспективе портативный аудиометр может быть у каждого отоларинголога в кабинете. Таким образом, для практического здравоохранения крайне актуальным является вопрос создания недорогого портативного диагностического устройства, позволяющего провести полное исследование слуха у пациента, своевременно назначить лечение и предотвратить стойкую тугоухость и инвалидность больных [1]. По данным Минздрава, в России насчитывается 12 миллионов больных с нарушением слуха, в том числе детей и подростков более 600 тысяч.

Разработка данного устройства является актуальной из-за необходимости оказания специализированной помощи пациентам с ушной патологией [2].

За эти 15 лет наблюдается стабильный рост интереса к объекту исследования, появляются новые виды аудиометров, в разработку вкладываются финансовые средства, что говорит о том, что выбранная область весьма перспективна.

На данный момент разработки аудиометра были составлены функциональная и электрическая схемы. Также был произведен расчет числовых характеристик элементов электрической схемы (элементов управления, питания, усиления, фильтрации, индикации) и размещение их с последующей трассировкой с использованием системы автоматизированного проектирования PCAD. Трассировка электрической схемы представлена на рис. 1.

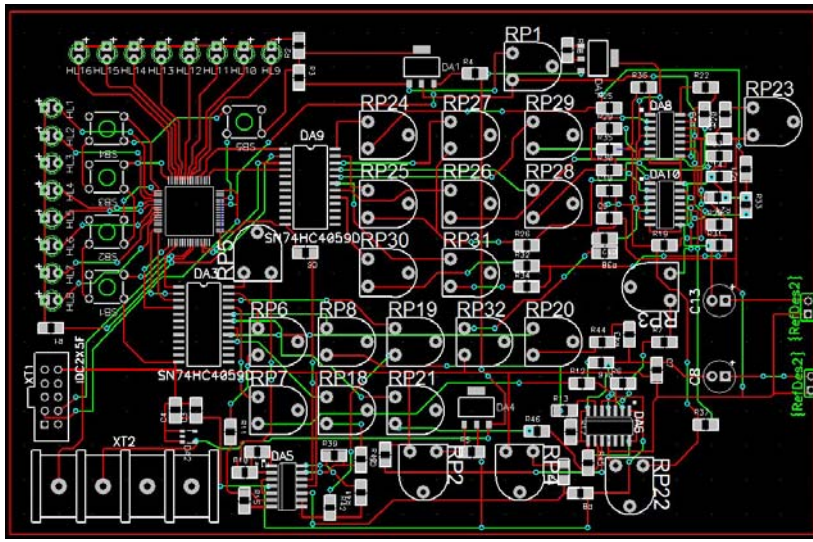


Рис. 1. Трассировка печатной платы

Была рассмотрена элементная база, подходящая для создания разрабатываемого прибора. Микроконтроллер STM32F405RGT6 будет являться ядром проектируемого аудиометра. Он будет отвечать за генерацию необходимых сигналов для костного и воздушного вибраторов: шести синусоид разной частоты, шума и голоса. В качестве тестовых фраз для проверки остроты слуха были выбраны фразы из ГОСТ Р 51061–97 «Системы низкоскоростной передачи речи по цифровым

каналам. Параметры качества речи и методы измерений». Слова, употребляемые для исследования, состоят из слов басовой группы (низкие звуки) и из слов дискантовой группы (высокие звуки).

Сигнал будет подаваться в ухо пациента либо через наушник (исследование воздушной проводимости), либо через костный вибратор (исследование костной проводимости). Пациенту будут предъявлены звуки различных частот с разной интенсивностью. Когда пациент услышит звук, он сообщит об этом, нажимая сигнальную кнопку. По результатам измерений будет построена аудиограмма, которая необходима для правильного выбора и настройки слуховых аппаратов.

На данном этапе проектирования был исследован воздушный излучатель (наушник) для проведения исследования воздушной проводимости. Был выбран излучатель типа ТДС-6. Также был изучен костный вибратор В-71.

Дальнейшим этапом разработки предполагается монтаж элементов на печатную плату и проведение испытаний. Также планируется уменьшение габаритов прибора по сравнению с аналогами. Себестоимость разрабатываемого прибора обещает быть несколько ниже, чем у существующих устройств.

ЛИТЕРАТУРА

1. Базаров В. Г., Лисовский В. А., Мороз Б. С., Токарев О. П. Основы аудиологии и слухопротезирования. М.: Медицина, 1984. 256 с.

2. Альтман Я.А., Таварткиладзе Г.А. Руководство по аудиологии. М.: ДМК Пресс, 2003. 360 с.

3. ГОСТ 27072–86. Генераторы сигналов диагностические звуковые. Аудиометры. Общие технические требования и методы испытаний. М.: Гос. комитет СССР по стандартам, 1986. 35 с.

ПОДГОТОВКА УПРАВЛЯЮЩИХ ПРОГРАММ НА ОБТЯЖНЫЕ СТАНКИ С ЧИСЛОВЫМ ПРОГРАММНЫМ УПРАВЛЕНИЕМ В АВИАЦИОННОЙ ПРОМЫШЛЕННОСТИ

В.А. Мишагин, аспирант каф. ТС

Научный руководитель С.В. Белых, доцент каф. ТС, к.т.н.

г. Комсомольск-на-Амуре, КнАГТУ, belykh.sergey@list.ru

Для авиационных предприятий является стратегической задачей повысить качество и точность изготовляемых деталей и конечной продукции в целом, снизить трудоёмкость и издержки с помощью внедрения и интеграции в технологический процесс станков с числовым программным управлением (СЧПУ) [1, 2].

В данной статье рассматриваются формирование и доработка управляющей программы (УП) для обтяжного пресса с ЧПУ FET-1500 (рис. 1).

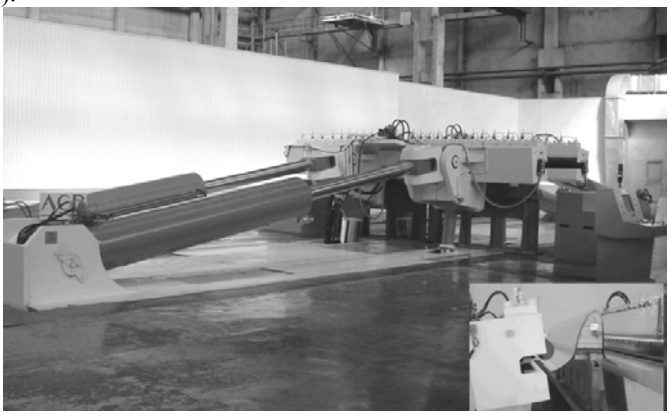


Рис. 1. Гидравлический пресс FET-1500

Рассмотрим процесс подготовки и расчёта УП. Исходной информацией является электронная модель детали (ЭМ), по которой формируется ЭМ пуансона, которая требует оптимизации в соответствии с требованиями программного обеспечения (ПО) для расчёта УП, по которой создают геометрию для ПО.

Полученная геометрия поступает в ПО S3F, в котором задаются геометрические характеристики заготовки, материал, переходы и прочие расчётные параметры. На выходе получаем готовую к работе УП. S3F показывает напряжения, деформации по заготовке в ключевых точках, однако проанализировать процесс движений губок и оценить возможные контакты, а также более подробно проанализировать процессы, возникающие в заготовке, не может [3, 4].

Для решения данной проблемы используется стороннее ПО: CAD/CAE/CAM-программы PAM-STAMP и AutoCAD, разработанные в КнАГТУ вспомогательные программы FET1500Trans и на базе Microsoft Excel специальный макрос для извлечения из УП координат перемещения цилиндров пресса.

Используя макрос в Microsoft Excel, извлекаются координаты перемещения цилиндров пресса, которые загружаются в FET1500Trans (рис. 2) для перевода параметров цилиндров в траектории губок. Далее в AutoCAD создается ЭМ-пресса с губками в крайнем ближнем положении (рис. 3). И на этом этапе можно оценить риски контакта губок с подставкой пуансона и сделать необходимые корректировки, чтобы этого избежать.

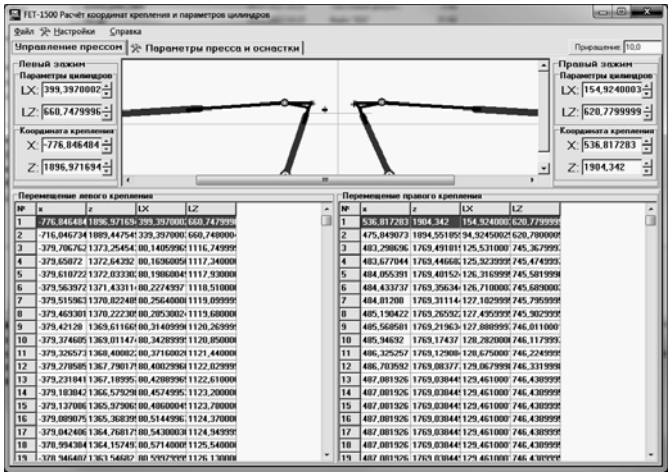


Рис. 2. Определение траектории губок в FET1500Trans

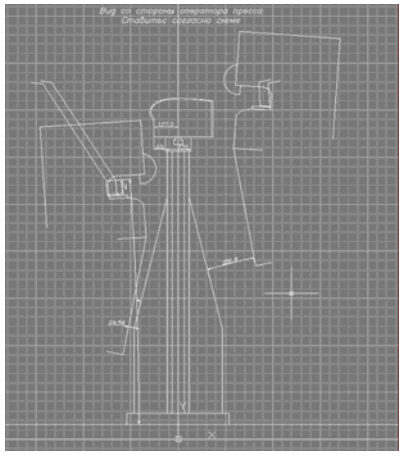


Рис. 3. Моделирование траектории губок в AutoCAD

Для подробного моделирования обтяжки используется PAM-STAMP (рис. 4), в который импортируется геометрия из ЭМ, задаются расчётные характеристики. По результатам анализа можно оценить деформации, напряжения, утонения и другие характеристики, происходящие в листе, сделав вывод о правильности УП.

Данная подготовка УП позволит сэкономить время и средства на ликвидацию ошибок, вызванных упрощенностью расчётов УП, позволит избежать повреждений пресса и губок и минимизировать потери от бракованных изделий [5].

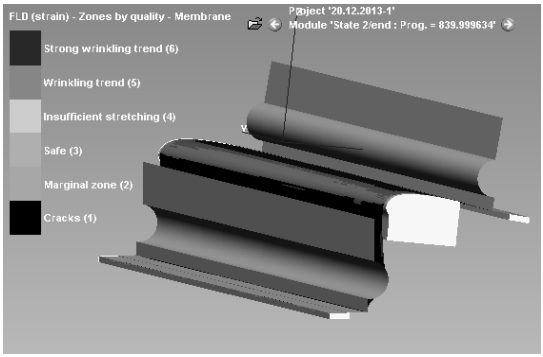


Рис. 4. Анализ расчётов в PAM-STAMP

ЛИТЕРАТУРА

1. Пекарш А.И., Клочков В.В. Экономическое обеспечение развития конкурентоспособной авиационной промышленности на принципах CALS // Наука и технология в промышленности. 2012. №2. С. 95–103.

2. Белых С.В., Станкевич А.В., Кривенок А.А., Перевалов А.А. Особенности автоматизированного изготовления стрингеров летательного аппарата с использованием роликового оборудования, оснащённого ЧПУ // Авиационная промышленность. М., 2000.

3. Белых С.В., Кривенок А.А., Мироненко В.В., Мишагин В.А., Определение положения пуансона в рабочем пространстве обтяжного пресса FET в процессе технологической подготовки производства // Вестник Иркутского государственного технического университета. 2013. №12. С. 36–40.

4. Кривенок А.А., Станкевич А.В., Феоктистов С.И. и др. Формообразование профильных заготовок с помощью листового пресса // Ученые записки Комсомольского-на-Амуре государственного технического университета. Науки о природе и технике. 2013. №II – 1(14). С. 4–8.

5. Одинг С.С. Управление процессом формообразования обшивкой двойной кривизны на обтяжном оборудовании с программным управлением // Изв. вузов. Авиац. техника. 1987. №3. С. 47–51; №4. С. 39–43.

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ БЛОКА УПРАВЛЕНИЯ РОТАЦИЕЙ РЕНТГЕНОВСКОГО РОТАЦИОННОГО КОМПЛЕКСА

А.Л. Павленко, студент каф. КИБЭВС
Научный руководитель Н.М. Федотов, к.т.н.
г. Томск, ТУСУР, pavlenko.sanya@sibmail.com

Рентгеновский ротационный комплекс (РРК) [1] предназначен для выполнения продолжительных рентгеноскопически контролируемых интервенционных процедур.

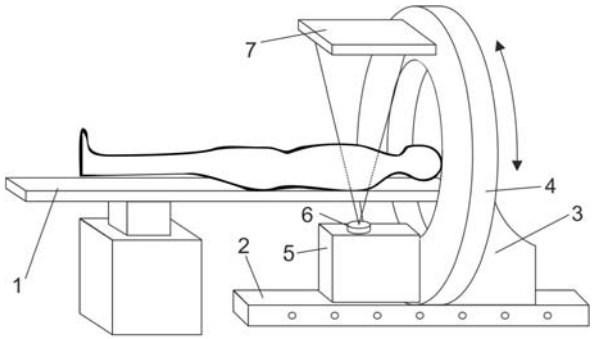


Рис. 1. Рентгеновский ротационный комплекс «Биоток-XR»: *1* – операционный стол (стол); *2* – направляющая для штатива; *3* – штатив; *4* – кольцо штатива; *5* – рентгеновский излучатель (моноблок); *6* – коллимационная система (коллиматор); *7* – приемник рентгеновского изображения (приемник)

Штатив способен перемещаться вдоль направляющей. При проведении рентгеноскопически контролируемых процедур положение стола и штатива жестко фиксируется. При этом кольцо штатива способно вращаться вместе с закрепленными на нем устройствами – моноблоком, коллиматором и приемником, что позволяет получать рентгеновские изображения в разных плоскостях. За осуществление вращения ответствен блок управления ротацией (см. рис. 2). Для данного блока необходимо реализовать систему управления.

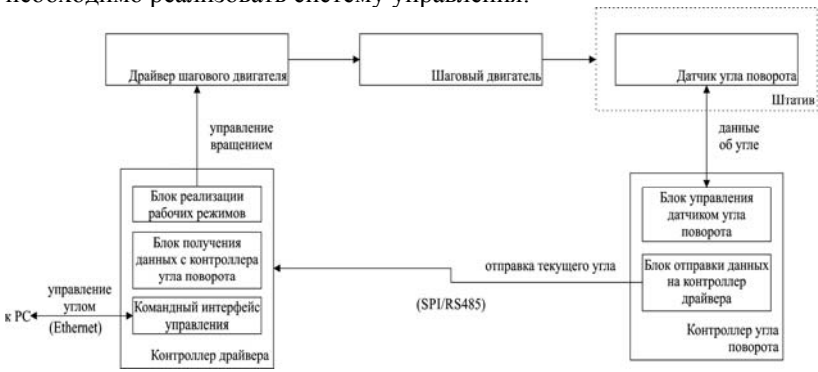


Рис. 2. Функциональная схема блока ротации

Система управления блока ротации реализуется с помощью контроллера драйвера и контроллера угла поворота.

Контроллер драйвера основан на модуле Wiz-Embedded WebServer. Он осуществляет управление драйвером шагового двигателя. Угловой шаг применяемого шагового двигателя составляет 1,8°.

Применение драйвера позволяет реализовать деление шага 1/ 125, что обеспечивает микрошаг в 0,0144°, который значительно снижает вибрации конструкции и обеспечивает плавность хода.

Контроллер угла поворота основан на микроконтроллере Texas Instruments MSP430F2132. Он занимается опросом цифрового датчика Analog Devices ADIS16209, закрепляемого на моноблоке РРК. Полученные данные о текущем угле передаются по SPI организованному поверх RS485, на контроллер драйвера.

Результаты работы. В ходе работы в рамках преддипломной практики была разработана система управления блока ротации, функционирующая по следующему принципу. Контроллер угла поворота с частотой 200 Гц осуществляет опрос датчика о текущем угле наклона и действующем на него ускорении. Данные об угле поворота используется контроллером драйвера для слежения за текущим углом поворота кольца штатива. Командный интерфейс управления реализован на контроллере драйвера и представлен следующими основными командами:

- SetAbsoluteAngle;
- SetRelativeAngle;
- GentleHalt;
- ImmediateHalt.

Команда SetAbsoluteAngle осуществляет выставление моноблока РРК в указанный угол.

Команда SetRelativeAngle осуществляет поворот моноблока РРК с текущего положения на указанный угол.

Основной особенностью выполнения данных команд вращения является реализация системой управления трех скоростных режимов: ускорение при старте, по достижении максимальной скорости равномерное движение, торможение и доводка на малой скорости при окончании установления угла. Необходимость данных режимов обуславливается большой массой устройств, закрепляющихся на кольце штатива и как следствие их большой инерционностью. Параметры разгона и торможения, максимальная и минимальная скорость регулируются.

Команда GentleHalt осуществляет плавное торможение вращения. Параметры торможения также регулируются.

Команда ImmediateHalt осуществляет резкое торможение кольца штатива и создана на случай возникновения непредвиденных ситуаций.

Заключение. К основным отличительным особенностям и преимуществам разработанной системы управления можно отнести:

- выставление угла осуществляется в автоматическом режиме;

– при вращении кольца штатива используются скоростные режимы, которые позволяют одновременно повысить как точность, так и скорость выставления угла;

– система управления представляет гибкий командный интерфейс, позволяющий детально настраивать её работу.

ЛИТЕРАТУРА

1. Федотов Н.М. Разработка ротационного рентгеновского аппарата с кольцевым штативом для оперативного создания 3D-изображений сердца / Н.М. Федотов, А.И. Оферкин, А.И. Буллер и др. // Доклады ТУСУРа. 2010. № 2 (22), ч. 2. С. 97–101.

ЧИСЛЕННОЕ ОБРАЩЕНИЕ ПРЕОБРАЗОВАНИЯ ЛАПЛАСА

Е.С. Перебейносова, магистрант, В.А. Онуфриев, аспирант,
каф. интегрированных компьютерных систем управления
Научный руководитель В.И. Гончаров, профессор, к.т.н.
г. Томск, Томский политехнический университет,
katik-90@bk.ru, onufrievva@tpu.ru

Одной из основных задач при построении самонастраивающихся систем автоматического управления (САУ) является задача идентификации объектов управления. Для того чтобы оценить точность идентификации, необходимо сравнить исходную функцию времени с соответствующей функцией, полученной по модели объекта. С этой целью необходимо решить задачу обращения преобразования Лапласа.

Обращение преобразования Лапласа на основе численных характеристик. В работе предлагается вариант решения задачи, направленный на снижение объема вычислений при обращении преобразования Лапласа. С этой целью привлекается подход, который базируется на вещественном интерполяционном методе (ВИМ) [2]. Он отличается сравнительной экономичностью в расчетах и моделировании. Кроме того, он хорошо сочетается с численными методами и цифровыми вычислительными средствами.

В основе ВИМ лежит интегральное преобразование, которое можно рассматривать как частный случай преобразования Лапласа

$$F(p)=\int_0^{\infty} f(t)\cdot e^{-pt}dt,\ p=\delta+j\omega \qquad (1)$$

при $\omega = 0$.

Приближенное обращение преобразования Лапласа можно выполнить с помощью определения оригинала в виде функционального ряда.

Рассмотрим решение задачи обращения преобразования Лапласа при помощи ВИМ, в основе которого лежит интегральное уравнение (1). Для получения приближенного решения функцию $f(t)$ представляют в таком виде, которая позволила бы выполнить операцию интегрирования:

$$f(t) = \sum_{j=0}^{\infty} c_j \varphi_j(t) . \qquad (2)$$

При этом, подставляя соотношение (2) в формулу (1), получим

$$F(\delta) = \int_0^{\infty} \sum_{j=0}^{\infty} c_j \varphi_j(t) \cdot e^{-\delta t} dt = \sum_{j=0}^{N-1} c_j T_j(\delta), \ \delta \in [0, \infty) . \qquad (3)$$

В качестве координатных функций $\phi_j(t)$ будем использовать полиномы Чебышева I рода в силу их привлекательных свойств, в частности, они наименее отклоняются от нуля. Выбранные полиномы имеют следующий вид:

$$T_j(t) = \sum_{k=0}^{j} b_{jk} \cdot e^{-kat} ,$$

где $j = 0, 1, \ldots, N-1$, a – масштабный множитель.

Для записи полиномов в матричной форме, удобной для практических расчетов, введем следующие обозначения:

$$B = \begin{bmatrix} b_{00} & 0 & 0 & 0 \\ b_{01} & b_{11} & 0 & 0 \\ b_{02} & b_{12} & b_{22} & 0 \\ b_{03} & b_{13} & b_{23} & b_{33} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 \\ 1 & -8 & 8 & 0 \\ -1 & 18 & -48 & 32 \end{bmatrix} . \qquad (4)$$

$$T = B \cdot \Phi . \qquad (5)$$

Матрица B известна, также ее можно проверить, выразив из выражения (5).

Возвращаясь к формуле (1), найдем значения коэффициентов c_j. Это можно сделать при помощи метода наименьших квадратов в виде

$$C = [(U_\delta B^T)^T U_\delta B^T]^{-1} (U_\delta B^T)^T F . \qquad (6)$$

В формуле (6) известны значения вектора B, необходимо найти значения матрицы U_δ, которая может быть представлена следующим выражением:

$$U_\delta = \begin{bmatrix} 1/\delta_1 & 1/(\delta_1 + a) & \ldots & 1/(\delta_1 + (N-1) \cdot a) \\ 1/\delta_2 & 1/(\delta_2 + a) & \ldots & 1/(\delta_2 + (N-1) \cdot a) \\ \ldots & \ldots & \ldots & \ldots \\ 1/\delta_\eta & 1/(\delta_\eta + a) & \ldots & 1/(\delta_\eta + (N-1) \cdot a) \end{bmatrix} . \qquad (7)$$

После того как найдем матрицу U_δ, можно приступить к нахождению вектора C, что позволит затем получить аналитическое

выражение искомой функции времени $f(t)$ по формуле (2). Однако для определения функции $f(t)$ необходимо решить ряд частных задач: выбрать интервал $\left[\delta_1,\delta_\eta\right]$, определить размерность численной характеристики η, найти значение масштабного множителя a, а также принять определенным число N членов усеченного ряда.

Пример нахождения функции $f(t)$. Для демонстрации работоспособности подхода обратимся к расчетному примеру. Дано изображение (передаточная функция двигателя постоянного тока по взмущающему воздействию – моменту нагрузки)

$$F(p)=\frac{4p+2}{(p+1)(p+2)(p+3)}.$$

Требуется найти оригинал – импульсную переходную характеристику двигателя. После проведения всех необходимых расчетов получим следующую зависимость $f(t)$. Для проверки полученных результатов сравним полученную зависимость с импульсной переходной характеристикой (рис. 1).

$$k(t)=6\cdot e^{-2t}-2\cdot e^{-t}-5\cdot e^{-3t}.$$

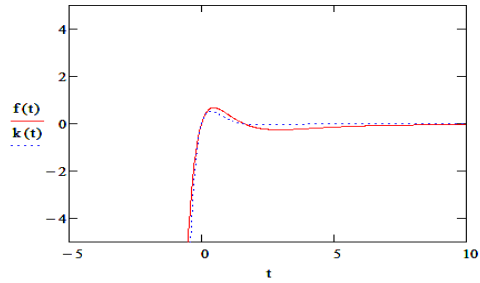


Рис. 1. Переходные характеристики объекта и модели

Для определения ошибки построим следующую зависимость $g(t)=\left|f(t)-k(t)\right|$ (рис. 2).

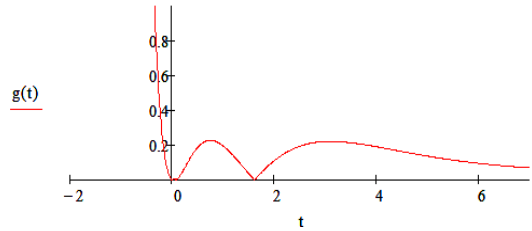


Рис. 2

Заключение. В работе предложен подход, который характеризуется малым объемом вычислений и ориентирован на встроенные в системы автоматического управления вычислительные структуры. В основе подхода лежит интегральное преобразование Лапласа. Получаемые с помощью ВИМ результаты могут найти применение для мобильных и встроенных устройств, что позволяет снизить их стоимость за счет отказа от дорогостоящих программных систем.

ЛИТЕРАТУРА

1. Doetsch G. Anleitung zum praktischen gebrauch der Laplace-transformation und der z-transformation, R.Oldenbourg, Munchen, wien, 1967.

2. Амербаев В.М. Численный анализ лагерровского спектра / В.М. Амербаев, Н.А. Утембаев / Академия наук Казахской ССР (АН КазССР). Институт сейсмологии. Алма-Ата: Наука, 1982.

3. Вадутова Ф.А. Модели и алгоритмы анализа и синтеза линейных систем управления на основе интегрального и дискретного вещественных преобразований. Томск, 1986.

РАЗРАБОТКА ЭЛЕКТРОИМПУЛЬСНОГО ГЕНЕРАТОРА ДЛЯ НИЗКОЭНЕРГЕТИЧЕСКОЙ КАРДИОВЕРСИИ

Я.Н. Подскарбий, А.С. Семенов, студенты каф. КИБЭВС

Научный руководитель Н.М. Федотов, зав. лаб. безопасных биомедицинских технологий ЦТБ ТУСУРа, к.т.н.

г. Томск, ТУСУР, n.m.fedotov@gmail.com

Электроимпульсное лечение фибрилляции предсердий сопровождается значительным болевым воздействием на пациента разряда электрического тока, который без применения наркоза пациент не переносит. Болевой порог кардиоверсии обычно определяется по энергии импульса [1]. Считают, что воздействие разрядов мощностью 0,01–0,5 Дж все больные переносят вполне удовлетворительно, а мощностью свыше 2,2 Дж практически никто из больных не переносит [2]. Экспериментальные исследования по снижению энергий до значений ниже болевого порога показывают на возможность ее выполнения [3]. Широкому проведению исследований препятствует отсутствие специализированных генераторов, разрешенных к применению в клинической практике и пригодных для формирования импульсов с требуемыми характеристиками, а также специальных электродных систем.

Цель – разработка генератора для проведения клинико-экспериментальных исследований по низкоэнергетической эндокардиальной кардиоверсии последовательностями электрических импульсов с энергиями ниже болевого порога.

Материалы и методы. Анализ публикаций по кардиоверсии и дефибрилляции с целью определения минимальных эффективных уровней энергий используемых в клинической практике показал, что для наружной кардиоверсии и дефибрилляции используют энергии до 360 Дж (в среднем около 200 Дж – это значение использовано в дальнейших расчетах), для эндокардиальной – в среднем 7 Дж [4], для имплантируемых устройств – до 35 Дж, в том числе для подкожных имплантируемых устройств – до 70 Дж. Рекомендуемая начальная мощность первого разряда при наружной кардиверсии составляет 200 Дж. Эта стратегия позволяет достигнуть высокой частоты успеха [2].

Требования к устройству (генератору): импульс биполярный, суммарная длительность 10 мс, энергия в нагрузке не менее 0,2 Дж.

То есть чтобы эффективно воздействовать на миокард при кардиоверсии, необходимо получить однородное электрическое поле или селективно воздействовать на области, провоцирующие фибрилляцию предсердий [5]. Воздействие можно проводить через существующие многополюсные диагностические типа «Basket» и абляционные электродные системы типа «Lasso». Кроме того, необходимо устройство коммутации, которое позволит распределить энергию импульса оптимальным образом, например в локализованную заранее область патологической активности.

Результаты. Структура предлагаемой биотехнической системы для проведения кардиоверсии (область воздействия обозначена Б.О. – биологический объект) представлена на рис. 1.

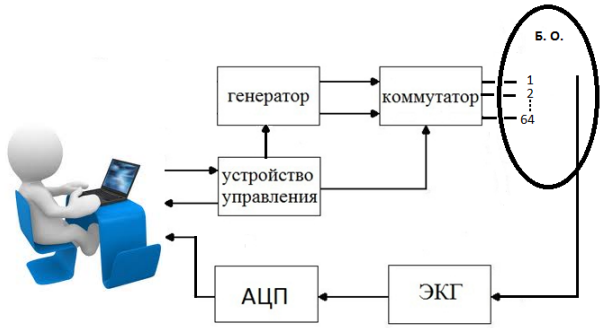


Рис. 1. Структура биотехнической системы

Принцип работы системы заключается в селективном воздействии на зоны аритмии. Импульсы с необходимой энергией подаются на определенные электроды, расположенные в предсердии. Для оптимального выбора электродов, на которые будет подаваться энергетические импульсы, а также для правильного выбора интервала времени подачи

импульса в систему включен электрокардиограф, позволяющий контролировать фазы сердечного цикла (систолу, диастолу желудочков). Также при помощи информации, получаемой с электродов, определяются очаги фибрилляции.

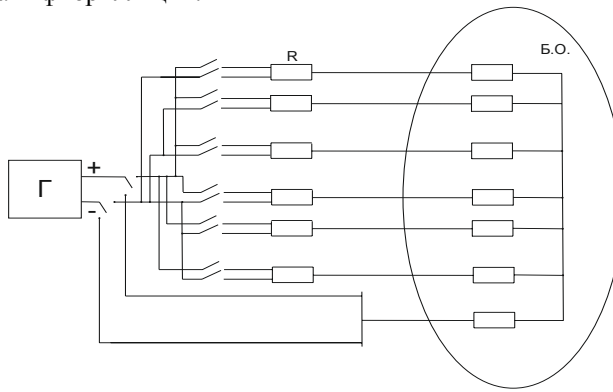


Рис. 2. Схема коммутации генератора и электродов

Основным элементом, позволяющим выбирать зоны воздействия и тем самым воздействовать селективно на патогенные зоны, является коммутатор. Благодаря коммутатору оператор системы через устройство управления задает последовательность подключения электродов и подачу импульсов, а также контролирует величину разряда для каждого электрода в определённый момент времени. Схема коммутации генератора и электродов представлена на рис. 2.

Заключение. Разработана структурная схема генератора для проведения низкоэнергетической кардиоверсии. Определены параметры порогового градиента электрического поля, длительности действия этого поля в геометрической области сердца, необходимые для выполнения безболевой кардиоверсии и дефибрилляции. Для электрического импульса длительностью 10 мс получены пороговые значения плотности тока порядка 400 А/м^2 и напряженности электрического поля порядка 500 В/м в миокарде.

ЛИТЕРАТУРА

1. Dosdall D.J., Ideker R.E. Intracardiac atrial defibrillation // Heart Rhythm. 2007. Vol. 4(3 Suppl). P. 51–56.

2. Pain Threshold for Low Energy Intracardiac Cardioversion of Atrial Fibrillation with Low or No Sedation / Richard Ammer, Eckhard Alt, Gregory Ayers, Claus Schmitt, Jay Pasquantonio, Matthias Schmidt, Katja Pütter and Albert Schömig // Pacing and Clinical Electrophysiology. 1997. Vol. 20, Issue 1. P. 230–236.

3. Li W. Low-energy multistage atrial defibrillation therapy terminates atrial fibrillation with less energy than a single shock / W. Li, A.H. Janardhan, V.V. Fedorov, Q. Sha, R.B. Schuessler, I.R. Efimov // Circ Arrhythm Electrophysiol. 2011. Vol. 4(6). P. 917–925.

4. Бокерия Л.А. Электрическая кардиоверсия при фибрилляции предсердий: показания и выбор оптимального метода / Л.А. Бокерия, В.А. Базаев, А.Х. Меликулов, Р.В. Висков, О.Л. Бокерия, А.Г. Филатов, А.Н. Грицай, В.В. Чумаков // Анналы аритмологии. 2005. № 3. С. 18–25.

5. Халифе Ж., Беренфелд О. «Частотное» картирование при фибрилляции предсердий: трансформация знаний от фундаментальных исследований к клинической практике // Вестник аритмологии. 2006. № 45. С. 75–85.

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ПРОВЕДЕНИЯ ОПРОСОВ

А.К. Пономарев, студент, Е.Ю. Костюченко, доцент

г. Томск, ТУСУР, каф. КИБЭВС, key@keva.tusur.ru

В настоящее время многие кафедры производят опросы среди студентов о качестве преподнесения им знаний, и эти опросы производятся путем заполнения бланков вручную. В связи с этим было решено автоматизировать процесс сбора статистики и ее дальнейшей обработки с целью позволить студентам осуществлять заполнение анкет удаленно по сети, а также предоставить сотрудникам кафедры оперативную информацию о качестве преподавания дисциплин с точки зрения студентов. Кроме того, получаемые данные являются необходимыми при проведении конкурсов среди преподавательского состава.

Целью данной работы является сокращение времени на проведение опросов. Разработка ведется для проведения опросов на кафедре КИБЭВС Томского государственного университета систем управления и радиоэлектроники (ТУСУР).

Были выделены следующие задачи:

− Выбор среды реализации.

− Проектирование базы данных.

− Реализация оболочки и взаимодействия ее с базой.

− Проектирование и реализация сервисов для статистической обработки данных.

Поэтапное описание работы комплекса:

1. Создание записей о студентах, преподавателях и критериях оценки. Необходимо обеспечить сохранность хранимых и обрабатываемых персональных данных.

2. Генерируются логин и пароль для входа в систему оценки. При генерации логина и пароля необходимо будет реализовать криптографический протокол, позволяющий проводить анонимную оценку каче-

ства с целью повышения объективности оценивания, но не допускающий до оценки посторонних лиц, а также не позволяющий одному лицу проставлять оценки многократно.

3. Сгенерированные логин и пароль раздаются объектам оценки.

4. Производится автоматизированный сбор оценок путем расставления оценок на веб-ресурсе, где размещен комплекс. Размещение планируется на кафедральном сайте kibevs.tusur.ru, что позволит при необходимости предоставить доступ к анкетированию всем заинтересованным лицам.

5. Подсчитываются статистические величины, требуемые для оценки качества преподавания. В рамках дальнейших исследований необходимо получение средних оценок по преподавателям в соответствии с заданными критериями, получение среднеквадратических отклонений оценок в соответствии с характеристиками, что позволит оценить однородность в области оценки работы преподавателя среди студентов. Дополнительно предлагается ввести расчет корреляционных характеристик для оценки взаимозависимостей между критериями и выбора независимых составляющих опроса.

На рис. 1 представлена база данных, используемая в комплексе. Она предназначена для автоматизированного сбора оценок по соответствующим критериям преподнесения знаний преподавателем.

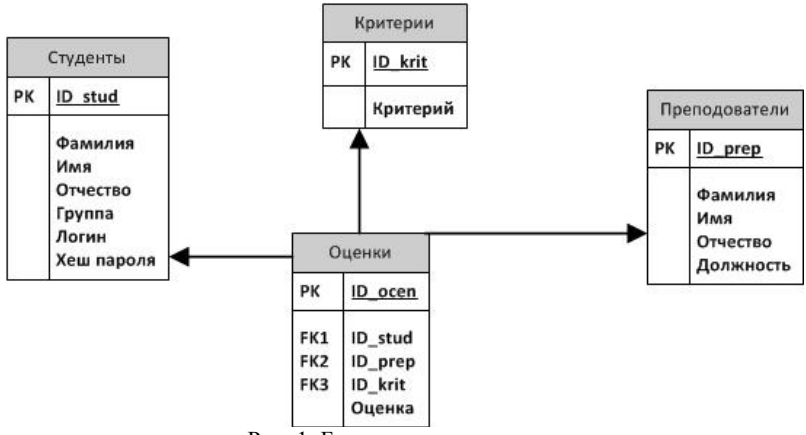


Рис. 1. База данных комплекса

По сравнению с ручной обработкой данных, которая используется в настоящее время, реализуемый комплекс позволит сократить время, затрачиваемое на сбор и обработку опросов среди студентов, и позво-

лит сотрудникам оперативно получать информацию о качестве ведения учебного процесса и оперативно реагировать на выявленные недостатки с целью повышения качества ведения дисциплин. Кроме того, разрабатываемая система может быть использована не только для проведения одного вида опросов, но и в дальнейшем, после доработки при проведении анкетирования среди студентов по любым вопросам.

Работа поддержана Министерством образования и науки, проект № 1220 «Фундаментальные основы проектирования информационно-безопасных систем»

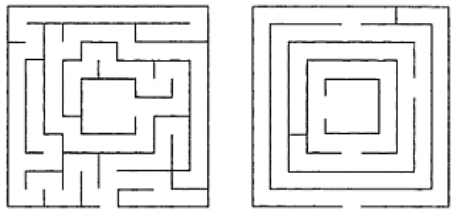
ПОИСК ВЫХОДА ИЗ ЛАБИРИНТА, ПЕРЕДВИЖЕНИЕ В ПРОСТРАНСТВЕ ПО ЗАДАННОМУ АЛГОРИТМУ

П.К. Пузырев, Н.М. Кривдюк, студенты каф. РЗИ,
Н.А. Шумилин, Е.Д. Демидова, студенты каф. КИБЭВС
Научные руководители: Ю.О. Лобода, доцент каф. КИБЭВС, к.т.н.,
О.В. Пехов, аспирант каф. КИБЭВС
г. Томск, ТУСУР, krivduk.nadezhda@gmail.com
Проект ГПО КИБЭВС-1202 – «Робототехника»

Тема выбранного проекта актуальна по сей день. Этот вопрос требует регулярноо совершенствования и доработки. Сейчас на рынке активно встречаются устройства, напрямую связанные с робототехникой – начиная с роботов-пылесосов, заканчивая роботами-охранниками. Все это – разные по категориям продукты, разработчики которых по-разному уделяют внимание их поведению в действии – в частности, речь идет о передвижении в пространстве. Пылесосу достаточно обойти все помещение и вернуться на место, независимо от рациональности передвижения, в то время как охраннику необходимо уверенно двигаться в помещении, своевременно осуществлять объезд помех, перекрывающих проезд, параллельно анализируя происходящее. Главная часть таких роботов – средства передвижения и разнообразные датчики, черпающие информацию об окружении. Но все эти устройства бесполезны без продуманного алгоритма.

В данной работе рассматриваются алгоритмы прохождения лабиринта роботом. В качестве лабиринта могут выступать завалы зданий, вентиляционные шахты, пещеры, газовые трубы.

Лабиринты делятся на многосвязные (рис. 1, *а*) и односвязные (рис. 1, *б*). Односвязными принято считать лабиринты, в которых все стенки связаны друг с другом. Многосвязные лабиринты делятся на лабиринты с петлей, когда замкнутый маршрут проходит вокруг препятствия, и без петли [1].



а *б*

Рис. 1. Вид многосвязного и односвязного лабиринтов

Отсюда можно сделать вывод, что распространенное и простое правило «одной руки» нельзя применять, не зная параметров лабиринта, т.е. невозможно заранее определить, является ли лабиринт односвязным или многосвязным. Универсальный метод решения лабиринтов описали французские математики Э. Люк и М. Тремо в 1882 г. Таким образом, алгоритм стал известен как алгоритм Люка–Тремо. Он является наиболее оптимальным вариантом решения поставленной задачи, а также позволяет построить карту лабиринта.

Согласно алгоритму Люка–Тремо следует соблюдать правила:

1. Выйдя из любой точки лабиринта, необходимо сделать отметку и двигаться в произвольном направлении до тупика или перекрестка.

2. Если тупик, то следует вернуться назад и поставить вторую метку и идти в направлении, не пройденном ни разу.

3. Если перекресток, то нужно идти в произвольном направлении, отмечая каждый перекресток на входе и на выходе.

4. Если на перекрестке уже имеется одна отметка, то следует идти новым путем, если такого нет – то пройденным путем, отметив его второй раз [2].

Карта представляется в виде двумерного массива фиксированного размера, в котором хранится информация о развилках, препятствиях и стенках лабиринта.

Данный проект разрабатывается для совершенствования и адаптации алгоритмов передвижения или поиска выхода из лабиринта для конкретных продуктов на базе алгоритма Люка–Тремо. В качестве продукта, на котором будет реализован усовершенствованный алгоритм, выступает робот-охранник, создаваемый на базе Arduino.

ЛИТЕРАТУРА

1. Прохождение лабиринта: правила и алгоритмы [Электронный ресурс]. Режим доступа: http://myrobot.ru/articles/logo_mazesolving.php, свободный (дата обращения: 20.02.2014).

2. Уолкер Д. Как пройти через лабиринт не заблудившись // Scientific American. 1986. №2. С. 62–74.

АВТОМАТИЗАЦИЯ ЦИФРОВОГО ИЗМЕРИТЕЛЯ ИММИТАНСА Е7-20

Н.В. Скотников, А.В. Белоножко, студенты каф. ФЭ
Научный руководитель С.В. Смирнов, профессор, д.т.н.
г. Томск, ТУСУР, nickky@sibmail.com

Возрастание количества измерений, нарастание сложности аппаратуры, повышение требований к точности, расширение использования математических методов обработки результатов измерений и обнаружения ошибок приводят к значительному росту трудоемкости и стоимости измерений и требуют создания специализированных автоматизированных средств измерений. Одним из таких средств является цифровой измеритель иммитанса Е7-20 [1].

Е7-20 – прецизионный прибор класса точности 0,1 с широким диапазоном рабочих частот от 25 Гц до 1 МГц и скоростью измерений до 25 измерений/с. С помощью Е7-20 можно измерять индуктивность (L_S, L_P), емкость (C_S, C_P), сопротивление (R_S, R_P), проводимость (G_P), фактор потерь, добротность, модуль комплексного сопротивления (Z), реактивное сопротивление (X_S), угол фазового сдвига, ток утечки (I), а также устанавливать напряжение смещения на измеряемом объекте в диапазоне от 0 до 40 В с помощью внутреннего источника напряжения. На рис. 1 представлена структурная схема Е7-20 [2].

Несмотря на высокие технические характеристики данного прибора, без специализированного программного обеспечения исследование полупроводниковых приборов превращается в рутинную задачу. Только для построения одной вольт-амперной характеристики обыкновенного диода необходимо вручную записать около 100 точек, а затем занести это все в таблицу и построить соответствующие графики. Целью данной работы является автоматизация прибора Е7-20.

Управление процессом измерений и регистрация полученных данных осуществляется через интерфейс RS-232. Прибор обеспечивает следующие режимы работы:

– дистанционное/местное управление;
– выдачу результата измерения;
– выдачу сообщения о перегрузке;
– выдачу сообщения об ошибке;
– выдачу сообщения о состоянии измерителя.

Прибор постоянно находится в режиме приема данных. Управлять прибором можно как от кнопок передней панели, так и через интерфейс.

После каждого измерения Е7-20 посылает компьютеру по COM-порту строку из 22 чисел в шестнадцатеричной системе счисления [3].

В руководстве по эксплуатации данного прибора приводится расшифровка каждого полученного байта. Так как прибор посылает данные непрерывно, то необходимо отслеживать стоповый байт (в данном случае это число АА), для того чтобы знать, где начало и конец строки.

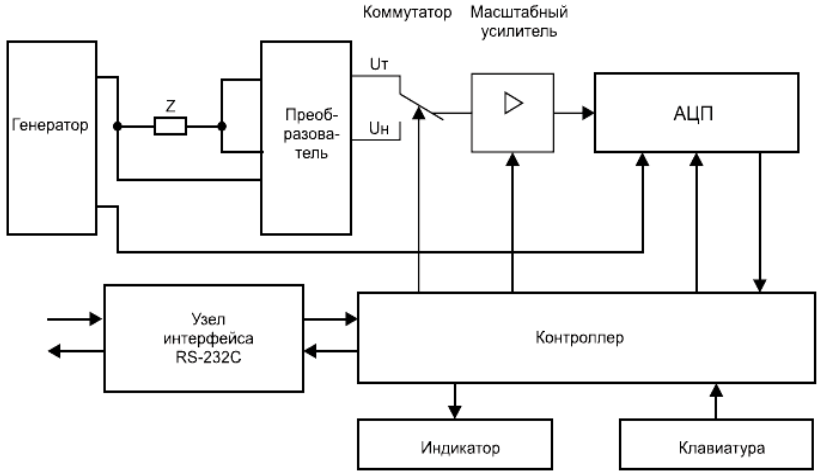


Рис. 1. Структурная схема измерителя иммитанса Е7-20

На графическом языке программирования Labview [4] был создан виртуальный прибор «Decoder», который преобразует машинный код в экспериментальные данные (рис. 2).

Е7-20 принимает однобайтные команды, соответствующие нажатию клавиш управления. Например, для автоматизации измерения вольт-амперных характеристик после каждого измерения прибору необходимо посылать команду для увеличения напряжения смещения. Для автоматизации измерений был создан виртуальный прибор «VisaRead» (рис. 3), который автоматически посылает необходимые команды и принимает результаты. В этот подприбор уже встроен «Decoder», поэтому нет необходимости расшифровывать полученные данные. Также «VisaRead» осуществляет проверку полученных данных. Если длина полученной стоки меньше 22 чисел, то на лицевой панели загорается сигнал «Ошибка измерения» и эти измерения не поступают в массив данных, в противном случае на табло высвечивается «Корректное изменение».

Таким образом с помощью подпрограмм «VisaRead» и «Decoder» можно автоматизировать все измерения на приборе Е7-20. Причем

написав одну программу, например для измерения вольт-амперных характеристик, переключившись в режим измерения емкости и запустив ту же программу, получим вольт-фарадные характеристики.

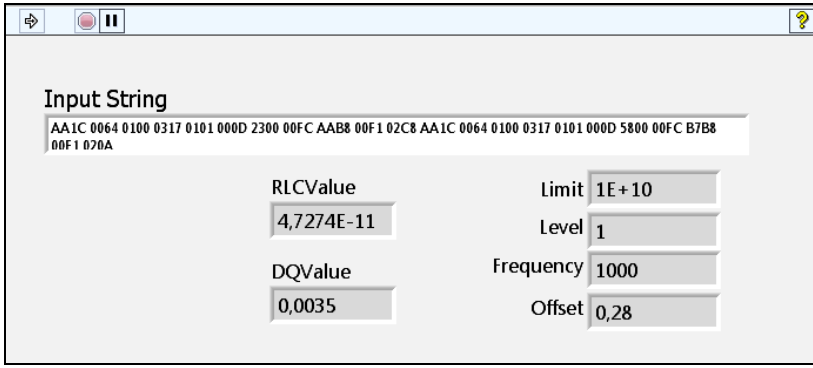


Рис. 2. Окно программы Decoder

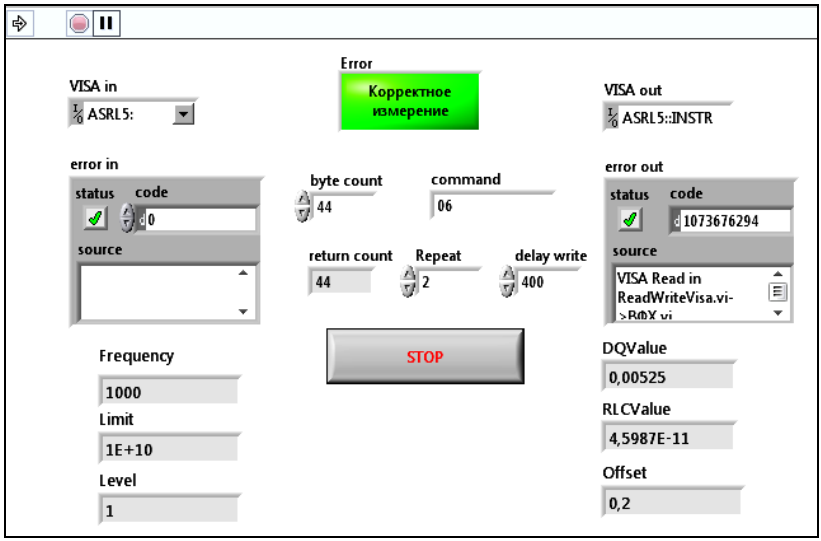


Рис. 3. Окно программы VisaRead

С помощью графического языка программирования Labview была написана программа для автоматизации Е7-20, превратившая данный прибор из простого измерителя иммитанса в незаменимый комплекс по исследованию полупроводниковых приборов.

ЛИТЕРАТУРА

1. Измеритель иммитанса (RLC) Е7-20. Режим доступа: http://www.mnipi.by/immitans11.html

2. Дьяконов В.А. Цифровые измерители иммитанса Е7-20/Е7-25 и их применение // Ремонт & Сервис. 2008. №10. С. 49–53.

3. Исследования полупроводниковых приборов с помощью измерителя иммитанса Е7-20. Режим доступа: http://www.astena.ru/e7-20_st.html

4. Графический язык программирования Labview. Режим доступа: http://russia.ni.com/labview

ЧАСТОТНЫЙ АНАЛИЗ ЭЛЕКТРОГРАММ ПРИ ФИБРИЛЛЯЦИИ ПРЕДСЕРДИЙ

Я.Н. Подскарбий, А.С. Семенов, студенты каф. КИБЭВС

Научный руководитель Н.М. Федотов, зав. лаб. безопасных биомедицинских технологий ЦТБ ТУСУРа, к.т.н.

г. Томск, ТУСУР, n.m.fedotov@gmail.com

Фибрилляция предсердий – самое распространенное нарушение ритма сердца, характеризующееся нескоординированной электрической активностью предсердий с последующим ухудшением их сократительной функции. Фибрилляция предсердий является наиболее распространенной формой аритмии, требующей терапевтического вмешательства. На данный момент поиск аритмогенных зон осуществляется при помощи анализа электрограмм в частотной области спектра сигнала [1].

Цель. Разработка программы для частотного анализа электрограмм с многополюсных электродных систем.

Материалы и методы. Одним из вариантов изучения электрической активности сердца и его участков является изучение электрограмм в частотной области. Частотный анализ основан на преобразовании Фурье [1]. Основной задачей в части исследования электрограмм является их анализ, с помощью которого можно определить зоны фибрилляции. Электрограммы снимаются с многополюсных электродов, которые помещены непосредственно в предсердие. Для уменьшения не подходящих для анализа осцилляций проводится низкочастотная фильтрация сигнала, обычно в полосе 4–10 Гц [1], так как значения доминантных частот – частот, которые имеют синусоиды с наибольшей амплитудой при ФП у человека, находятся в этих пределах. И непосредственно перед проведением анализа Фурье проводится свертка – смещение сигнала до нулевого уровня по краям анализируемого фрагмента с использованием специального способа – окна Хемминга. Это позволяет добиться более четкого выделения доминантной

частоты. Для лучшего сглаживания компонентов спектра может быть использован прием заполнения исходного сигнала нулями в качестве точек дискретизации. Тем самым как бы удлиняется время дискретизации и повышается частотное разрешение спектра без изменения его основных характеристик.

Результаты. Вид одной из электрограмм, полученных с многополюсных электродов, представлен на рис. 1.

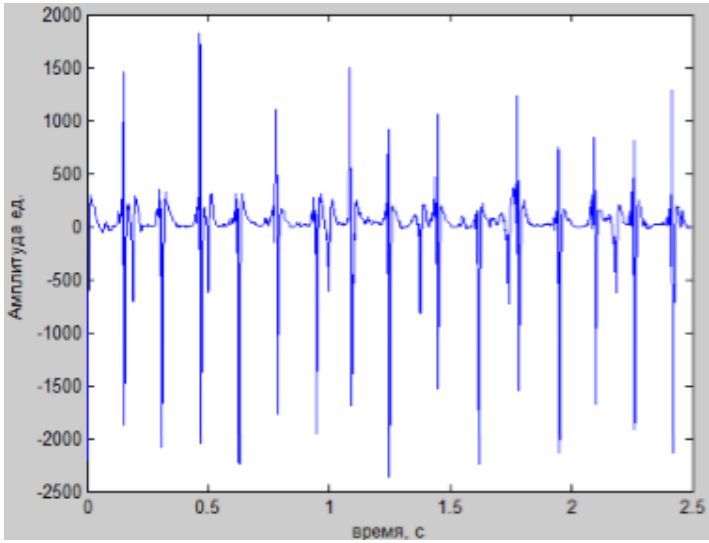


Рис. 1. Электрограмма во временной области

Далее для подавления шумов а также дальнейшего более четкого выделения доминантной частоты к исходному сигналу применяется оконная функция Хемминга [1]:

$$w_n = 0{,}53836 - 0{,}46164 \times \cos\left(\frac{2n\pi}{N-1}\right).$$

После процедуры свертки проводится дискретное преобразование Фурье для получения спектра сигнала (рис. 2).

Для фильтрации сигнала от лишних гармоник был выбран фильтр Баттерворта. Фильтр Баттерворта – один из типов электронного фильтра. Фильтры Баттерворта нижних частот характеризуются тем, что имеют максимально гладкую амплитудную характеристику в начале координат в s-плоскости [2], а также чаще всего применяются для частотных анализов биоэлектронных сигналов. Это является одним из критериев выбора данного типа фильтра.

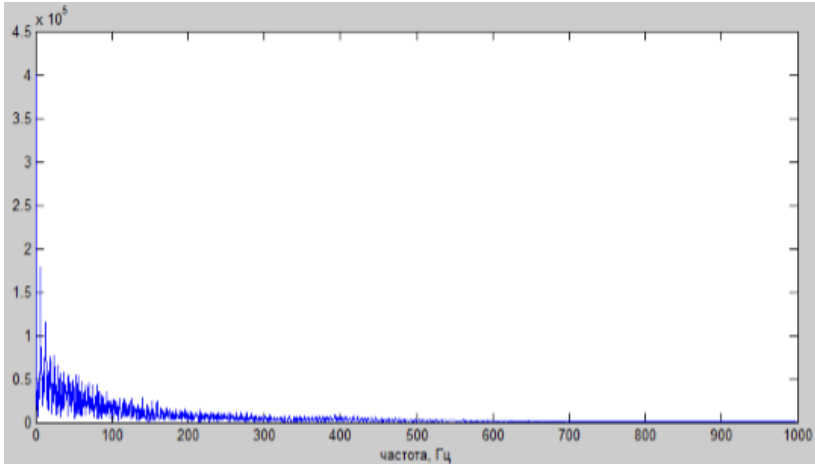


Рис. 2. Частотный спектр сигнала

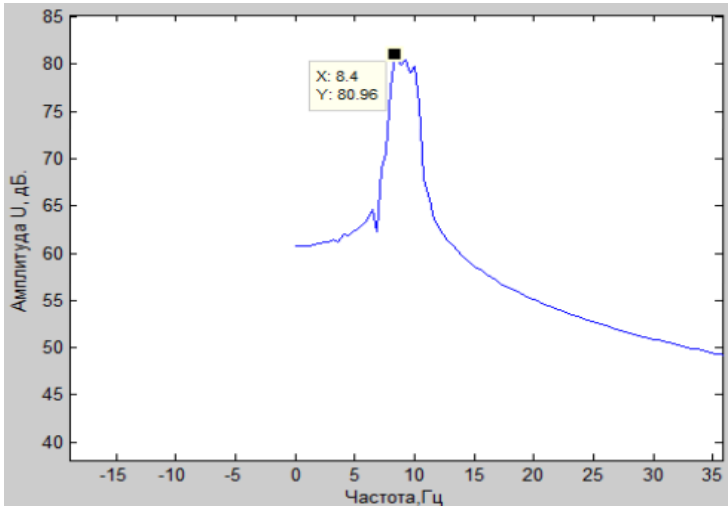


Рис. 3. Фильтрованный сигнал с выделенной доминантной частотой

Заключение. Разработана программа для обнаружения доминантных частот по электрограммам с внутрисердечных электродных систем для определения очагов фибрилляции. Для более точного определения источников фибрилляции предсердий планируется исследование электрограмм в фазовом спектре.

ЛИТЕРАТУРА

1. Оферкин И.А. Анализ электрической активности предсердий у пациентов с мерцательной аритмией / И.А. Оферкин, А.И. Петш, М.П. Шпилевой, Е.А. Покушалов,С.Е. Мамчур, И.В. Гущин // Вестник аритмологии №61, 2010. С. 38.

2. Дьяконов В.П., Абраменкова И.В. MATLAB 5.0/5.3. Система символьной математики. М.: Нолидж, 1999.

РАСПОЗНАВАНИЕ ОБРАЗОВ В СИСТЕМЕ УПРАВЛЕНИЯ ЭНЕРГОЭФФЕКТИВНОСТЬЮ.

К.В. Щурихина, студентка, В.В. Латровкин, аспирант

Научный руководитель Н.В. Замятин, профессор каф. АОИ, д.т.н

г. Томск, ТУСУР, каф. АОИ vindreise@gmail.com, latrovkin@yandex.ru

Проект ГПО АОИ-1302 – «Ситуационный центр управления энергоэффективностью»

Одним из главных ценообразующих факторов кирпича-сырца являются энергозатраты на его производство. Процесс изготовления включает в себя просушку в туннельных сушилках, где теплый воздух, поступающий от вентилятора, подготавливает кирпич к последующему обжигу. Наличие сколов и трещин, а также обжиг при недостаточной просушке приводят к тому, что кирпич становится непригодным для продажи.

Чтобы избежать этого, необходимо постоянно проверять влажность и дефектность еще в процессе сушки. Однако проверка человеком приводит к большим энергозатратам, т.к. необходимо отключать вентилятор, подающий теплый воздух, а после проверки – заново его запускать.

Предлагаемый вариант решает проблему энергозатрат, т.к. отключать вентилятор не нужно, процесс проверки происходит благодаря камерам, установленным в туннельных сушилках и программой распознавания образов.

Программа распознавания образов основана на методике, описанной в [1]. В основе методики лежит алгоритм адаптивного усиления (AdaBoost). Смысл алгоритма заключается в том, что если есть набор эталонных объектов, т.е. значения и класс, к которому они принадлежат, кроме того, имеется множество простых классификаторов, то мы можем составить один более совершенный и мощный классификатор. При этом в процессе составления или обучения финального классифи-

катора акцент делается на эталоны, которые распознаются «хуже». В этом и заключается адаптивность алгоритма, в процессе обучения он подстраивается под наиболее «сложные» объекты.

Для описания картинки используются признаки Хаара (примитивы). Суть метода заключается в следующем: на эталонное изображение накладывается один из примитивов, далее считается сумма значений пикселей в белой области примитива и черной области и отнимается от первого значение второго. В итоге получаем обобщенную характеристику анизотропии некоторого участка изображения.

Однако даже для небольшого изображения количество накладываемых примитивов очень велико, если взять изображение размером 24×24, то количество примитивов ~180000. Задача алгоритма AdaBoost – выбрать те примитивы, которые наиболее эффективно выделяют данный объект.

На основе классификаторов с отобранными наиболее эффективными примитивами строится каскад. Каждый последующий элемент каскада имеет более жесткие условия успешного прохождения, чем предыдущий, тем самым до конца доходят только самые «правильные».

Для реализации данной методики использовалась библиотека OpenCV.

Задача: обнаружить прототип кирпича на картинке (нужно учитывать, что в работе все цветные изображения переводятся в grayscale, иначе количество инвариантов слишком велико), при условии, что:

− объект может иметь разный цвет. ±50 значений от исходного;

− объект может иметь разный размер. Размер может изменяться до 2 раз;

− объект имеет случайное месторасположение на изображении.

Для начала создается обучающая выборка. Обучающая выборка создается двумя способами: с помощью заранее составленной базы изображений или же сгенерированной на основе одного эталонного объекта заданное количество случаев.

Выберем второй вариант, т.к. у нас нет достаточно большой базы изображений, а для генерации выборки на основе одного объекта в OpenCV есть модуль createsamples. В качестве фонового изображения используется залитый черным цветом фон.

В зависимости от заданных параметров модуль берет эталонный объект, применяет к нему различные деформации (цвет, добавляет шум), далее выбирает фоновое изображение и располагает случайным образом на нем объект.

Для обучения необходимо собрать образы. Есть два типа образов: негативные и позитивные. Негативные образы соответствуют отсутст-

вию объекта на изображении. Положительные образы соответствуют изображениям с обнаруженными объектами. Набор негативных образов должен быть подготовлен вручную, в то время как множество положительных образов создается с помощью утилиты opencv_createsamples.

Негативные образы должны быть взяты из произвольного изображения. Эти изображения не должны содержать обнаруженных объектов. Негативные примеры называют также фоновыми пробами или образцами фона изображения. Описанные изображения могут быть разных размеров. Но каждое изображение должно быть больше, чем размер окна обучения.

Большое множество позитивных образов создаются из заданного объекта изображения с изменениями интенсивности, размера. Количество и диапазон случайности можно менять с помощью аргументов командной строки утилиты opencv_createsamples.

Теперь необходимо создать каскад классификаторов для имеющейся базы объектов. Для этого используем модуль haartraining. В него передаётся много параметров, самыми важными из которых являются количество классификаторов в каскаде, минимальный необходимый коэффициент эффективности классификатора (minimum hit rate), максимально допустимая частота ложных срабатываний (maximum false alarm).

В результате получаем xml-файл, который можно подгружать в исходный код программы.

Одним из недостатков данного метода является низкая скорость обучения. Так, для обработки выборки из 7 позитивных и 10 негативных примеров потребовалось 4 минуты, в то время как для оптимального поиска объектов необходима выборка из как минимум 1000 примеров.

ЛИТЕРАТУРА

1. Paul Viola, Michael Jones Rapid Object Detection using a Boosted Cascade of Simple Features // Conference on computer vision and pattern recognition, 2001.

КИНЕТИЧЕСКОЕ ПРОГРАММИРОВАНИЕ РОБОТА

Н.А. Шумилин, Е.Д. Демидова, А.А. Габдрафиков,
А.В. Алешков, студенты каф. КИБЭВС,
П.К. Пузырев, Н.М. Кривдюк, студенты каф. РЗИ,
О.В. Пехов, аспирант каф. КИБЭВС,
Ю.О. Лобода, доцент каф. КИБЭВС
г. Томск, ТУСУР, friskaspro@hotmail.com
Проект ГПО КИБЭВС-1202 – «Робототехника»

Основой работы являлась разработка программы, задача которой – запоминать действия, передаваемые роботу удаленно, с помощью Bluetooth, а затем точно их воспроизводить [1].

Программа дает возможность облегчить программирование для тех случаев, когда написание новой программы будет трудоемким и времязатратным. Примером этого могут быть охранные роботы, которые достаточно один раз провести по нужному маршруту, затем они будут его повторять. Также ручное обучение нашло самое широкое применение в различных конструкциях промышленных роботов и в настоящее время наиболее распространено. Суть обучения заключается в том, что необходимые движения робота задаются оператором, а соответствующая им информация записывается при этом в память устройства управления. Затем робот переключают на автоматический режим, и он начинает воспроизводить всю последовательность движений до тех пор, пока не появится необходимость заменить программу. Как правило, современные устройства управления промышленными роботами позволяют хранить несколько программ, и поэтому записанную ранее программу при необходимости можно воспроизвести вновь. Этот способ прост, доступен рабочему соответствующей квалификации и не требует никаких дополнительных устройств.

При создании программы учитывалось, что она должна удовлетворять следующим требованиям: доступный интерфейс, актуальность, универсальность.

На начальном этапе разработки было необходимо разработать алгоритм, по которому в дальнейшем будет функционировать программа. Алгоритм должен быть несложным в понимании и реализации. Поэтому было решено записывать действия, выполняемые роботом, по порядку при нажатии на кнопки управления, с запоминанием их параметров (мощность, направление действия, время затраченное на выполнение действия), это запоминание необходимо для того чтобы в дальнейшем определить, в каком направлении двигался робот, с какой мощностью и сколько времени он двигался в данном направлении. При внесении оператором изменений в действия робота он производит

запись действия и его параметров в память и затем выполняет новую команду, которую он также занесет в память при выборе нового действия или нажатия кнопки «стоп». В конечном итоге в памяти робота находится некий набор действий и их параметров, которые в дальнейшем необходимо воспроизвести без участия оператора. Это достигается путем извлечения действий из памяти робота в порядке их записи с самого начала, а параметры, которые записывал робот, необходимы для того, чтобы робот как можно точнее воспроизводил необходимые действия. Как только набор действий заканчивается, по заранее заданной оператором команде осуществляется закрытие, повторное воспроизведение старой или запись новой программы.

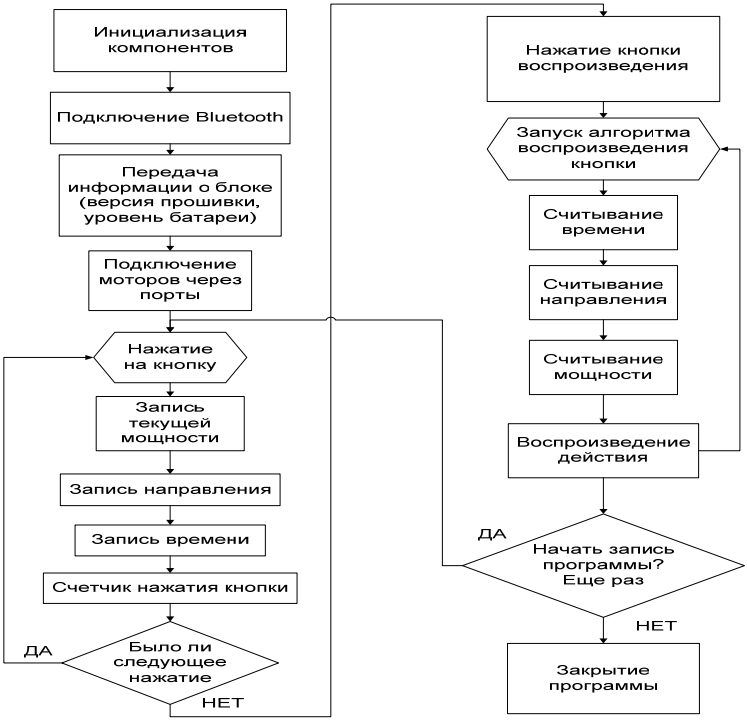


Рис. 1. Блок-схема алгоритма

Для реализации данного алгоритма было решено использовать среду программирования Microsoft Visual Studio 2010 [2]. Также было решено использовать библиотеку Mindsqualls – .Net библиотека для удаленного управления LEGO Mindstorms NXT роботами посредством

USB и Bluetooth [3]. Особенностью библиотеки является то, что для управления моторами в ней рекомендуется использовать инструментарий MotorControl, разработанный в рамках проекта RWTH – Mindstorms NXT Toolbox for MATLAB, – он дает возможность очень точного позиционирования.

В конечном итоге для достижения цели был разработан алгоритм для программы, задача которой – запоминать действия, передаваемые роботу удаленно, а затем точно их воспроизводить. Была выбрана среда программирования Microsoft Visual Studio 2010 и в ней на языке C# была реализована данная программа.

ЛИТЕРАТУРА

1. LEGO MINDSTORMS NXT Communication protocol [Электронный ресурс]. URL: http://www.lego.com/ru-ru/mindstorms/downloads/nxt/nxt-bdk/ (дата обращения: 18.11.2013).

2. Руководство по программированию на C# [Электронный ресурс]. URL: http://msdn.microsoft.com/ru-ru/library/9b9dty7d.aspx (дата обращения: 18.11.2013).

3. LEGO MINDSTORMS NXT Direct commands [Электронный ресурс]. URL: http://www.lego.com/ru-ru/mindstorms/downloads/nxt/nxt-bdk/ (дата обращения: 18.11.2013).

К ВОПРОСУ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ ЭФФЕКТИВНОСТИ БОРЬБЫ С ГОЛОЛЕДНЫМИ ОБРАЗОВАНИЯМИ НА ПРОВОДАХ ЛИНИЙ ЭЛЕКТРОПЕРЕДАЧ

С.И. Сухоруков, аспирант каф. ЭПАПУ

г. Комсомольск-на-Амуре, КнАГТУ, e-mail: sergei.svan@gmail.com

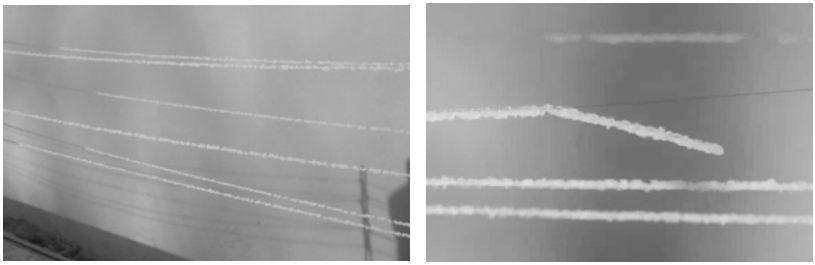
Периодически возникающие в последнее время природные аномальные явления («ледяной дождь», обильный снегопад при резком понижении температуры и т. п.), приводящие к возникновению аварийных ситуаций в системах энергоснабжения, заставляют искать высокоэффективные способы борьбы с такими природными процессами. Основным фактором, обусловливающим возникновение аварийных ситуаций, является образование гололеда на проводах ЛЭП и несущих опорах, масса которого в несколько раз может превышать предельно допустимое значение, определяемое прочностными характеристиками ЛЭП. На сегодняшний день наиболее распространённым способом борьбы с гололедными отложениями на проводах ЛЭП является плавка гололеда постоянным или переменным током, требующая больших затрат как энергии, так и времени [1]. Проводимая нами работа на-

правлена на разработку автоматизированной системы, способной производить удаление гололеда с проводов ЛЭП, основываясь на новом способе и значительно снижая при этом затраты энергии и времени, требуемые на очистку.

Экспериментальное исследование нового способа. В [2] предложен альтернативный способ удаления льда с проводов ЛЭП. Сущность данного способа состоит в комбинированном (механическом и тепловом) воздействии на провода. Если через провода пропускать импульсы тока определенной частоты и амплитуды, то под воздействием силы ампера провода, расположенные в одной плоскости, будут испытывать силовые возмущения, приводящие их в колебательное движение, что приведет к разрушению слоя льда. Для повышения эффективности процесса разрушения ледового покрытия необходимо, чтобы частота колебаний обледеневших проводов была близка к частоте собственных колебаний провода.

Для оценки работоспособности данного способа удаления льда с проводов ЛЭП было проведено экспериментальное исследование на физическом макете линии электропередач в масштабе 1:40. Лед на провода наносился путем напыления воды из пульверизатора при температуре окружающего воздуха –12 ºС. Возмущающие электрические воздействия создавались с помощью управляемого источника тока, описанного в [3].

Результаты эксперимента подтвердили работоспособность предложенного способа удаления льда (см. фото на рис. 1).



а *б*

Рис. 1. Фотоматериалы эксперимента: *а* – до очистки; *б* – в процессе очистки

В связи с неравномерностью распределения ледового покрытия на проводах, а также непостоянством массы осаждаемого льда для приведения проводов в колебательный процесс с частотой, близкой к резонансной, необходимо, чтобы электрический источник возмущающих воздействий был управляемым.

На рис. 2 приведены кривые зависимости амплитуды колебаний провода от частоты возмущающих воздействий для свободно подвешенного провода и провода с ледяным покрытием при равномерном его распределении по длине провода.

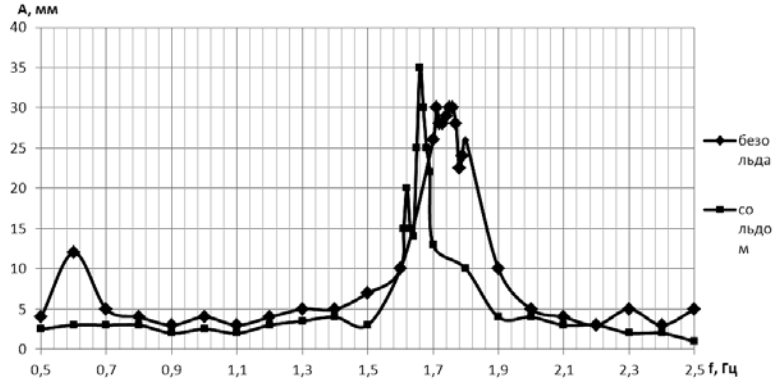


Рис. 2. Кривые зависимости амплитуды колебаний провода от частоты возмущающих воздействий

Заключение. На приведенных кривых четко прослеживается резкое повышение амплитуды колебаний при приближении частоты возмущающих воздействий к частоте собственных колебаний провода. Кроме того, видно, что при увеличении массы максимум амплитуды колебаний сдвигается в сторону низких частот. На частотах, отличных от резонансных, амплитуда колебаний провода снижается, а на частотах, близких к резонансным (амплитуда колебаний максимальна), не происходит схлестывания проводов. Время удаления льда с проводов в несколько раз меньше времени, необходимого на плавку гололеда стандартным способом. Это подчеркивает высокую энергетическую эффективность предложенного способа.

ЛИТЕРАТУРА

1. Соловьев В.А., Черный С.П., Козин В.М., Сухоруков С.И. Инновационные технологии управления: в 2 кн. Кн. 1. Одесса: КУПРИЕНКО СВ, 2013. 128 с.

2. Пат. 2442256 С1 Российская Федерация, МПК H 02 G 7/16. Способ удаления обледенения с проводов линий электропередач / Козин В.М., Соловьев В.А., Орлов Д.А., Сухоруков С.И., Малых К.С.; заявитель и патентообладатель Федеральное государственное образовательное учреждение высшего профессионального образования «Амурский гуманитарно-педагогический государственный университет». № 2010144485/07; заявл. 29.10.2010; опубл. 10.02.2012. Бюл. № 4. 4 с.

3. Сухоруков С.И. Управляемый источник тока для экспериментальной установки по удалению льда с проводов ЛЭП / С.И. Сухоруков, В.А. Соловьев // Электротехнические комплексы и системы управления. 2013. № 4. С. 6–10.

СЕКЦИЯ 18

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель секции – **Шелупанов А.А.**, проректор по НР ТУСУРа, зав. каф. КИБЭВС, д.т.н., профессор, зам. председателя – **Конев А.А**., доцент каф. КИБЭВС, к.т.н.*

ОПТИМИЗАЦИЯ И БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ

Д.А. Агеев, С.В. Полянский, студенты
Научный руководитель А.И. Гуляев, аспирант
г. Томск, ТУСУР, gai@keva.tusur.ru

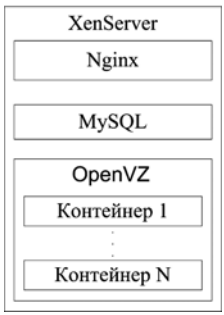
В ходе жизни и роста небольшой компании возникают проблемы масштабируемости и безопасности компьютерной сети при сравнительно небольших затратах. В корпоративной сети необходимо обеспечить несколько веб-сервисов, которые обычно работают с базами данных. Возникает необходимость обеспечить стойкость веб-сервисов к различным нагрузкам, атакам злоумышленников, а также безопасность баз данных, в особенности конфиденциальных и корпоративных данных.

Для решения этой задачи с минимальными затратами, при наличии небольшого количества веб-сервисов обычно используют среды виртуализации: кроссплатформенные гипервизоры, к примеру Oracle VM VirtualBox, Citrix XenServer [1], KVM (Kernel-based Virtual Machine). Гипервизор – это тонкий уровень программного обеспечения, которое эмулирует компьютерную архитектуру. Он запускается загрузчиком и позволяет нескольким операционным системам работать одновременно поверх него. Oracle VirtualBox имеет интуитивно понятный интерфейс и необходимый минимум функционала, когда XenServer и KVM более функциональны и производительны, но требуют больших знаний. На физический сервер устанавливается гипервизор, на котором создано несколько виртуальных машин с операционными системами, на каждой из которой запущен сервис вместе со своей базой данных. Это обеспечивает достаточную безопасность, потому как каждый сервис отделен от другого. Но на поддержку каждой ОС на виртуальной архитектуре гипервизора уходит много ресурсов.

Эта проблема может быть решена использованием технологии контейнеризации OpenVZ [2]. OpenVZ – это реализация технологии виртуализации на уровне операционной системы, которая базируется на ядре Linux. OpenVZ позволяет на одном физическом сервере запускать множество изолированных копий операционной системы, так называемых контейнеров. Таким образом, обеспечивается разделение веб-сервисов с экономией вычислительных ресурсов. При росте количества веб-сервисов достаточно создать дополнительный контейнер, в который поместить сервис, для этого не требуется большого количества времени и усилий, что решает проблему масштабируемости.

Для удобства работы с СУБД, а также обеспечения дополнительной безопасности баз данных их можно объединить под управлением одной СУБД и разместить отдельно от веб-сервисов. К примеру, на отдельной виртуальной машине гипервизора. При этом будет исключен непосредственный доступ из внешний сети, что обеспечивает безопасность. Помимо того, при сбое работы СУБД перезагрузка виртуальной машины на гипервизоре не займет много времени.

Также дополнительная безопасность может быть достигнута использованием проксирующего сервера Nginx [3], который позволяет скрыть все ресурсы в частной (серой) сети, проксируя адреса глобальной сети в частную сеть. Таким образом, структура сети менее уязвима, потому как непосредственно в глобальную сеть смотрит лишь один сервис.



В итоге с помощью средств виртуализации и контейнеризации можно обеспечить должную безопасность для веб-сервисов и баз данных компании, реализовав все необходимые сервисы на одном физическом сервере, при этом решив проблему масштабируемости и цены на техническую реализацию. Примерная структура такого сервера показана на рис 1.

Рис. 1. Логическая структура сервера

ЛИТЕРАТУРА

1. Citrix XenServer®6.2.0 Virtual Machine User's Guide, 2013 [Электронный ресурс]. http://support.citrix.com/article/CTX137830 (дата обращения: 04.03.2014).

2. OpenVZ Users Guide, version 2.7.0-8, 2005 [Электронный ресурс]. http://download.openvz.org/doc/OpenVZ-Users-Guide.pdf (дата обращения: 04.03.2014).

3. Nginx documentation [Электронный ресурс]. http://nginx.org/en/docs/index.html (дата обращения: 04.03.2014).

ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

Н.Н. Алексеева, студентка, А.И. Кураленко, аспирант
г. Томск, ТУСУР, каф. РЗИ, miss_xotton@mail.ru

Вопрос защиты информации в различных организациях на сегодняшний день является актуальным. Для достижения этой цели должна строиться система защиты информации (СЗИ), которая обеспечивает предотвращение ущерба в результате действия угроз информационной безопасности.

В работе описан процесс построения СЗИ организации, информационная система которой изображена на рис. 1.

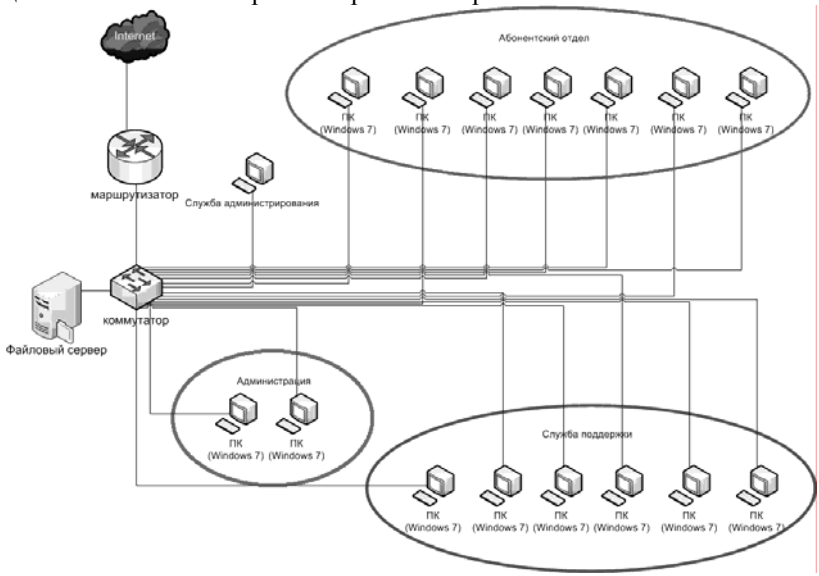


Рис. 1. Информационная система предприятия

Защищаемой информацией на предприятии являются: персональные данные (ПДн) и коммерческая тайна (КТ). ПДн и КТ предприятия обрабатываются в автоматизированном и в бумажном виде.

Основной методикой составления перечня сведений, составляющих КТ, является организация работы экспертной комиссии. На предварительном этапе экспертной комиссией выделяется вся информация, циркулирующая в организации. Эффективным способом выделения информации является метод интервьюирования сотрудников и руководителя организации. При составлении вопросов за основу взяты вопросы для интервью [1].

На основе интервьюирования сотрудников составлен предварительный перечень информации, составляющей КТ организации и выделен перечень сведений, относящихся к ПДн. Эксперты оценивают критичность ресурса из предварительного перечня информации, составляющей КТ организации, по параметрам конфиденциальности, целостности и доступности по десятибалльной шкале. На основе суммы полученных показателей определяется отношение информации к КТ организации. В результате получен перечень информации, составляющей КТ предприятия.

Источники угроз безопасности информации делятся на три основные группы: обусловленные техническими средствами, обусловленные стихийными источниками, обусловленные действиями субъекта. Из данных групп источников угроз выделены актуальные для ПДн и КТ организации согласно [2].

Модель угроз для ПДн и КТ построена на основе типовой модели угроз безопасности ПДн, обрабатываемых в локальных информационных системах ПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена [3]. Для КТ модель угроз дополнена основными способами несанкционированного доступа к информации из [4].

Система защиты информации должна обеспечивать конфиденциальность, целостность и доступность информации посредством организационных и технических мер защиты.

Выбор средств защиты информации произведен с учетом требований к уровню защищенности ПДн в соответствии с [5], классу защищенности АС в соответствии с [6].

Межсетевым экраном и средством обнаружения вторжения является Security Studio Endpoint Protection. На компьютерах пользователей установлена операционная система (ОС) Windows 7, поэтому защита от НСД будет реализована на ее основе путем установки лицензий, на использование программы контроля сертифицированной версии ОС Windows 7 Профессиональная и базового пакета для сертифицированной версии ОС Windows 7 Профессиональная. Решения являются наиболее экономичными из рассмотренных.

Приняты следующие организационные меры защиты ПДн и КТ: регистрация и сопровождение посетителей; разработка политики безопасности ПДн; разработка положения о КТ; разработка должностных инструкций по работе с ПДн и КТ; установление персональной ответственности за нарушения правил обработки ПДн и КТ; подбор и проверка персонала, имеющего доступ к конфиденциальной информации; дела с документами, содержащими КТ, хранятся в отдельном сейфе или металлическом шкафу.

В процессе работы проведен анализ информационной системы организации, ее свойств и характеристик, разработан метод классификации информации, подлежащей защите, построены модели угроз и нарушителя, осуществлены выбор и обоснование технических и организационных мер защиты информации. В результате работы построена СЗИ организации.

ЛИТЕРАТУРА

1. IT Baseline Protection Manual. Standard Security Measures. Version: October 2000 [Электронный ресурс]. Режим доступа: http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm.pdf (дата обращения: 23.01.2014).

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. [Электронный ресурс]. Режим доступа: http://fstec.ru/component/attachments/download/290 (дата обращения: 08.02.2014).

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. [Электронный ресурс]. Режим доступа: http://fstec.ru/component/attachments/download/289 (дата обращения: 07.02.2014).

4. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». [Электронный ресурс]. Режим доступа: http://fstec.ru/component/content/article/114-tekhnicheskaya-zashchita-informatsii/dokumenty/spetsialnye-normativnye-dokumenty/387-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g4 (дата обращения: 12.02.2014).

5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 07.02.2014).

6. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации». [Электронный ресурс]. Режим доступа: http://www.atlas-nsk.ru/assets/files/ruk_akt/doc_3_3_013.pdf (дата обращения: 04.03.2014).

ОПЕРАТОР СВЯЗИ И РЕЕСТР ЗАПРЕЩЕННЫХ РЕСУРСОВ

М.А. Ананев, студент

Научный руководитель В.Г. Миронова, мл. науч. сотрудник, к.т.н.

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

В современном мире компьютеры, которые позволяют получить доступ к сети Интернет, становятся всё доступнее и доступнее, огром-

ное количество смартфонов, планшетов, всевозможных компьютеров наполняют наш быт. Особенно остро встает вопрос доступности несовершеннолетних к информации в сети Интернет. Совсем недавно дети играли во дворе в песочнице, когда в нынешнее время им больше нравится проводить время за компьютером, сидя в Интернете. Не все родители понимают, какой опасности они подвергают своё чадо, а если и понимают, то не всегда могут ограничить доступ детей к информации, которая им не предназначена, а противопоказана, с экстремистским, наркотическим и порнографическим содержанием. Решением такой проблемы для Правительства стали ведение списка запрещенных ресурсов и принудительная блокировка этих ресурсов на территории Российской Федерации.

Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 обязывает Федеральную службу по надзору в сфере связи создать и держать в актуальном состоянии «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено». 1 ноября 2012 г. были внесены изменения в ФЗ №149 «Об информации, информационных технологиях и о защите информации», который, в свою очередь, обязывает операторов связи блокировать доступ пользователей к запрещенным ресурсам.

За наполнение реестра отвечают следующие государственные учреждения: Роскомнадзор, Роспотребнадзор, ФСКН, Генпрокуратура, суд. Также любой пользователь может оставить анонимную жалобу на сайте http://eais.rkn.gov.ru/ для рассмотрения органами власти вопроса о внесении ресурса в список запрещенных.

Логика работы с сервисом получения выгрузки из реестра запрещенных ресурсов такова:

– Оператор связи формирует запрос на получение выгрузки из реестра запрещенных ресурсов с указанием названием компании, юридическим адресом, ИНН, ОГРН. Далее этот запрос подписывается электронной подписью и отправляется на сервер Роскомнадзора с помощью протокола Simple Object Access Protocol (SOAP) и с использованием Web Services Description Language схемы (WSDL) обращения к сервису. Сервис получения выгрузки реестра работает по протоколу SOAP, расшифровывается как простой протокол доступа к объектам. Протокол SOAP не различает вызов процедуры и ответ на него, а просто определяет формат послания (message) в виде документа XML. Послание может содержать вызов процедуры, ответ на него, запрос на

выполнение каких-то других действий или просто текст. Спецификацию SOAP не интересует содержимое послания, она задает только его оформление [1]. WSDL расшифровывается как язык описания web-сервисов. WSDL – это формат, базирующийся на XML и использующийся для описания сетевых сервисов при помощи сообщений, содержащих информацию о том, как осуществлять доступ к конкретному веб-сервису. WSDL расширяем, что позволяет описывать услуги (сервисы) и их сообщения независимо от того, какие форматы сообщений или сетевые протоколы используются для транспорта, однако чаще всего используется WSDL 1.1 вместе с SOAP 1.1, HTTP GET/POST и MIME. Поскольку WSDL был разработан совместно с SOAP, в его разработке участвовали все те же фирмы Microsoft, Ariba и IBM [2].

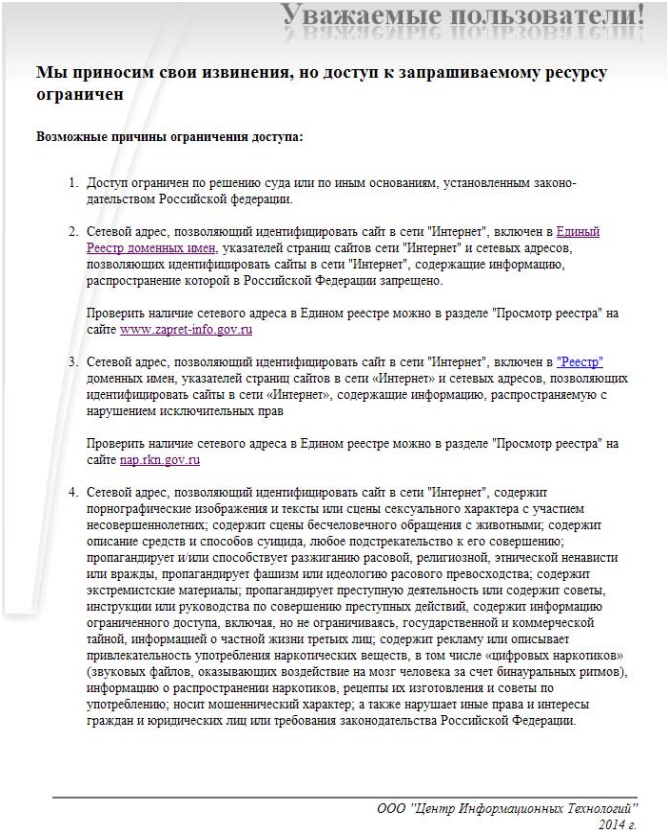
– На следующем этапе сервер обрабатывает запрос небольшое количество времени (от 30 до 300 с) и в случае успешного прохождения запроса на выгрузку предоставляет выгрузку из реестра запрещенных ресурсов оператору связи. Пример выгрузки из реестра запрещенных ресурсов представлен на рис. 1.

```
<content id="262" includeTime="2013-01-12T16:40:26">
        <decision date="2012-11-10" number="96-РИ" org="Роскомнадзор"/>
        <url>
                <![CDATA[ http://[redacted].jpg ]]>
        </url>
        <domain>
                <![CDATA[[redacted]]]>
        </domain>
        <ip>[redacted].144.68</ip>
</content>
```

Рис. 1. Пример выгрузки из реестра запрещенных ресурсов

На сегодняшний день выгрузка реестра запрещенных ресурсов содержит порядка 1500 записей запрещенных ресурсов. Также присутствуют ресурсы с использованием протокола HTTPS. Ввиду особенности передачи информации по протоколу HTTPS (весь пакет, в том числе и заголовок с доменным именем, передается в зашифрованном виде) блокировка производится на аппаратном уровне по IP-адресу. Пакеты, передающиеся по протоколу HTTP, блокируются на программном уровне. Используется «связка» межсетевых экранов Cisco ASA 5520/K8 (аппаратная часть) и Websense (программная часть). Одним из главных преимуществ программно-аппаратной реализации блокировки запрещенных ресурсов является практически нулевая нагрузка на аппаратную часть, большая часть вычислительных процессов приходится на программную часть.

В результате научной работы была разработана программа, позволяющая в автоматическом режиме получать выгрузку из реестра запрещенных ресурсов, а также производить изменения списка доступа на программно-аппаратном уровне по IP-адресу и по доменному имени. На рис. 2 изображен пример страницы блокировки запрещенного сервиса.



Уважаемые пользователи!

Мы приносим свои извинения, но доступ к запрашиваемому ресурсу ограничен

Возможные причины ограничения доступа:

1. Доступ ограничен по решению суда или по иным основаниям, установленным законодательством Российской федерации.
2. Сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", включен в Единый Реестр доменных имен, указателей страниц сайтов сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.

   Проверить наличие сетевого адреса в Едином реестре можно в разделе "Просмотр реестра" на сайте www.zapret-info.gov.ru
3. Сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", включен в "Реестр" доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространяемую с нарушением исключительных прав

   Проверить наличие сетевого адреса в Едином реестре можно в разделе "Просмотр реестра" на сайте nap.rkn.gov.ru
4. Сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", содержит порнографические изображения и тексты или сцены сексуального характера с участием несовершеннолетних; содержит сцены бесчеловечного обращения с животными; содержит описание средств и способов суицида, любое подстрекательство к его совершению; пропагандирует и/или способствует разжиганию расовой, религиозной, этнической ненависти или вражды, пропагандирует фашизм или идеологию расового превосходства; содержит экстремистские материалы; пропагандирует преступную деятельность или содержит советы, инструкции или руководства по совершению преступных действий, содержит информацию ограниченного доступа, включая, но не ограничиваясь, государственной и коммерческой тайной, информацией о частной жизни третьих лиц; содержит рекламу или описывает привлекательность употребления наркотических веществ, в том числе «цифровых наркотиков» (звуковых файлов, оказывающих воздействие на мозг человека за счет бинауральных ритмов), информацию о распространении наркотиков, рецепты их изготовления и советы по употреблению; носит мошеннический характер; а также нарушает иные права и интересы граждан и юридических лиц или требования законодательства Российской Федерации.

ООО "Центр Информационных Технологий"
2014 г.

Рис. 2. Пример страницы блокировки запрещенного сервиса

ЛИТЕРАТУРА

6. СибИнфоцентр // Подготовка профессионалов в области информационных технологий. Авторизированный учебный центр Microsoft, Oracle [Электронный ресурс]. URL: http://www.sibinfo.ru/archive/news/04_07_05/soap.html (дата обращения: 28.02.2014).

7. CitForum // WSDL: взгляд изнутри, часть I [Электронный ресурс]. URL: http://citforum.ru/internet/webservice/wsdl_1 (дата обращения: 28.02.2014).

НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

А.Ю. Арестов, студент каф. КИБЭВС

Научный руководитель А.А. Конев, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, aa_sec@mail.ru

Должный уровень информационной безопасности определяется в первую очередь качеством функционирования развернутой на предприятии системы нормативной документации, технические средства защиты в совокупности с деятельностью персонала всего лишь реализуют эти требования.

Внедрение целостной нормативной документации является важной составляющей процесса обеспечения информационной безопасности и поддержания непрерывности бизнеса. Результатом работы является то, что каждое должностное лицо имеет четкое представление, что делать в той или иной ситуации, какие действия запрещены, куда обращаться в экстренных случаях и т.п. Повышается уровень ответственности персонала. Расследование инцидентов и нарушений трудовой дисциплины позволяет однозначно и быстро установить степень вины конкретных должностных лиц. Как следствие, использование ИТ-ресурсов становится более эффективным, при этом возрастает общий уровень информационной безопасности компании.

В данный момент нет точных правил составления нормативной документации, разработка такой документации становится длительным и трудоемким процессом. Многие организации не располагают собственными ресурсами, необходимыми для квалифицированной разработки и внедрения политик безопасности. Многие документы составляются с большим количеством недочетов. В моей работе рассмотрена стандартизация процесса создания нормативных документов в области информационной безопасности и составлена эталонная структура этих документов для выбранных мной областей.

1. Инструкция по организации защиты персональных данных:

1) общие положения;

2) понятие и состав персональных данных;

3) принципы обработки персональных данных;

4) доступ к персональным данным;

5) защита персональных данных;

6) права и обязанности сторон в области защиты персональных данных;

7) ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

2. Инструкция по организации защиты коммерческой тайны:

1) общие положения;

2) порядок отнесения информации к коммерческой тайне;

3) допуск к сведениям, составляющим коммерческую тайну;

4) обязанности лиц, имеющих доступ к коммерческой тайне;

5) порядок обращения с документами, содержащими коммерческую тайну;

6) ответственность, за разглашение сведений, являющихся коммерческой тайной.

3. Инструкция по организации антивирусной защиты:

1) общие положения;

2) термины и определения;

3) порядок применения средств антивирусной защиты (АВЗ);

4) порядок обновления баз данных средств АВЗ;

5) обязанности, права и порядок назначения администраторов АВЗ;

6) обязанности пользователей АВЗ;

7) порядок действий пользователей и администраторов АВЗ при обнаружении вирусов.

8) ответственность за организацию АВЗ.

4. Инструкция об организации пропускного и внутриобъектового режима:

1) общие положения;

2) организация пропускного режима;

3) порядок пропуска автотранспорта на территорию организации;

4) порядок вноса/выноса и ввоза/вывоза материальных ценностей на территорию организации;

5) внутриобъектовый режим;

6) обязанности персонала объекта и посетителей по соблюдению пропускного и внутриобъектового режима;

7) действия персонала при обнаружении на территории объекта подозрительных предметов, нарушителей пропускного и внутриобъектового режима;

8) действия сотрудника охраны при срабатывании охранной или охранно-пожарной сигнализации.

5. Должностная инструкция администратора информационной безопасности:

1) общие положения;

2) задачи и функции администратора безопасности;

3) обязанности администратора безопасности;

4) права администратора безопасности;

5) ответственность администратора безопасности.

Отыскать готовые политики безопасности, которые бы оказались применимыми в организации, соответствовали бы ее структуре и тре-

бованиям безопасности, практически невозможно. Несмотря на доступность многих из них в Интернете, они зачастую непригодны для практического использования. На основе результатов данной работы, т.е. эталонной структуры и подробного описания каждого типа инструкций, процесс создания таких инструкций для конкретной организации намного упрощается.

ЛИТЕРАТУРА

1. Аудит информационной безопасности [Электронный ресурс]. Режим доступа: http://www.iso27000.ru/chitalnyi-zai

2. Правила оформления должностных инструкций [Электронный ресурс]. Режим доступа: http://instrukciy.ru/text/page171.html

3. Документы по информационной безопасности [Электронный ресурс].Режим доступа: http://securitypolicy.ru/index.php/

4. Производство оборудования и систем безопасности [Электронный ресурс]. Режим доступа: http://www.perco.ru/support/

5. Образцы и примеры должностных инструкций [Электронный ресурс]. Режим доступа: http://instrukciy.ru/text/

6. Должностная инструкция специалиста по защите информации [Электронный ресурс]. Режим доступа: http://www.it-rabota.ru/spec_zashita.phtml

7. Инструкции специалистов по защите информации [Электронный ресурс]. Режим доступа: http://www.vep.ru/bbl/catalog/

ТЕХНОЛОГИИ ИДЕНТИФИКАЦИИ ПОСЕТИТЕЛЕЙ ВЕБ-РЕСУРСОВ

С.В. Авдяков, студент каф. АДМ

Научный руководитель М.Г. Адигеев, доцент каф. АДМ, к.т.н., ЮФУ

Соруководитель В.А. Новосядлый, к.ф.-м.н.

ФГАНУ НИИ «Спецвузавтоматика»

г. Ростов-на-Дону, ЮФУ, sergeyavdyakov@yandex.ru

Сегодня сеть Интернет стала неотъемлемой частью жизни миллиардов людей. При ежедневном использовании веб-ресурсы получают значительное количество информации от пользователей. В связи с этим в последнее время резкое развитие получили технологии идентификации посетителей веб-ресурсов. Эти технологии используются для разнообразных целей: как для защиты посетителей и ресурсов от злоумышленников, так и для извлечения коммерческой выгоды.

Рассмотрим основные примеры использования данных технологий. Такие компании, как Facebook, Google и ВКонтакте, используют идентификацию для защиты учетных записей клиентов. В случае подозрительной активности, например попытки входа с неизвестного браузера или IP адреса, пользователя могут попросить пройти допол-

нительную аутентификацию. Технологии идентификации также используются для защиты веб-ресурсов от атак ботов, спам атак и автоматических краулеров. Например, известный сервис CloudFlare предоставляет возможности для защиты от DoS-атак, спам-рассылок и автоматизированного сбора информации. Кроме того, данные технологии используются и в коммерческих целях. Компании Google и Яндекс предоставляют владельцам веб-ресурсов бесплатные инструменты для анализа активности пользователей. Для этого необходимо встроить скрипты данных компаний в исходный код веб-ресурса. В результате таких действий указанные компании получают практически неограниченный доступ к данным пользователей и их активности на таких ресурсах. Собранные данные используются для коммерческих сервисов контекстной рекламы Google AdSense и Яндекс.Директ, которые обеспечивают значительную часть дохода данных компаний.

Технологии идентификации. В литературе по данной тематике в качестве эталона рассматривается подход, описанный в работе [1]. Эта работа является одной из немногих открытых реализаций подобных алгоритмов, и при этом в ней очень подробно описаны способы идентификации, включая математические обоснования. Хотя в общем результаты показывают высокую эффективность, в данной работе использованы лишь базовые способы идентификации, и она все еще требует значительных улучшений. Также в [2] производится сравнение реализации panopticlick (www.panopticlick.eff.org) с коммерческими реализациями. Рассматриваются продукты таких компаний, как BlueCava (www.bluecava.com), Iovation (www.iovation.com) и ThreatMetrix (www.threatmetrix.com). Применяемые в этих продуктах решения, в целом схожи с аналогичными в реализации panopticlick и содержат, в основном, качественные улучшения.

Рассмотрим основные подходы к идентификации посетителей веб-ресурсов. Методы идентификации можно классифицировать по уровню воздействия:

– пользовательская конфигурация браузера (плагины, дополнения и т.д.);
– браузер и его версия;
– операционная система и установленные приложения;
– аппаратные характеристики.

Также можно ввести классификацию по технологиям, использованным для воздействия:

– JavaScript;
– HTTP;
– Flash;

– Java;
– HTML5 API.

Воздействие на уровне пользовательской конфигурации браузера позволяет посредством JavaScript выявить установленные плагины, дополнения для браузера и их последовательность, установленные активные компоненты, типы данных, поддерживаемые браузером, часовой пояс пользователя, включен ли Flash, включена ли опция Do-Not-Track; посредством HTTP возможно установить, включены ли HTTP cookies и язык операционной системы; посредством ActionScript возможно определить, использует ли пользователь прокси. На уровне браузера посредством HTTP и JavaScript можно установить значение заголовка User-Agent браузера пользователя. Воздействие на уровне операционной системы позволяет посредством ActionScript и Java определить установленные шрифты, операционную систему и версию ее ядра. На уровне аппаратных характеристик с помощью JavaScript можно установить разрешение экрана пользователя, а пользуясь ActionScript и Java IP адрес, – пропускную способность канала связи и различные другие аппаратные характеристики.

В связи с бурным развитием HTML5, который поддерживает скриптовый интерфейс прикладного программирования (API), большое развитие могут получить методы идентификации уровня воздействия на аппаратные характеристики, т.к. данный API тесно связан с производительностью и аппаратными возможностями клиентского оборудования. В API содержатся функции для работы с файловой системой, графической системой (включая аппаратное ускорение), звуковой системой, локальным хранилищем и базой данных.

Заключение. Несмотря на успехи в развитии технологий идентификации посетителей веб-ресурсов, в этой области все еще необходимы значительные исследования. В связи с тем, что существует мало открытых реализаций, а существующие, как правило, опираются на базовые методы, необходимо реализовать новую комплексную систему идентификации с углублением в воздействие на уровне аппаратных характеристик. Разработка такой системы позволит более эффективно использовать технологии идентификации в целях защиты как посетителей, так и самих веб-ресурсов.

ЛИТЕРАТУРА

1. Eckersley P. How unique is your web browser // Proceedings of the 10-th international conference on Privacy enhancing technologies. 2010. P. 1–18.

2. Nikiforakis N., Kapravelos A., Joosen W., Piesssens F., Vigna G. Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting // IEEE Symposium on Security and Privacy. 2013. P. 541–555.

МОДИФИЦИРОВАННАЯ СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА С ИСПОЛЬЗОВАНИЕМ КЛЕТОЧНЫХ АВТОМАТОВ

Д.О. Бондаренко, А.В. Ращупкина, студенты 3-го курса
Научный руководитель О.О. Евсютин, доцент, к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, dima030793@gmail.com
Проект ГПО КИБЭВС-1307 – «Клеточные автоматы»

Схемы разделения секрета представляют собой одну из разновидностей криптографических протоколов [1], предназначенных для распределения секретной (ключевой) информации между участниками информационного обмена. В данной работе рассматривается реализация такой схемы для цифровых изображений, основанная на использовании двумерных линейных клеточных автоматов [2], и предлагается ее модификация.

Целью работы является увеличение количества частей (более двух), с помощью которых можно восстановить секретное изображение.

Модифицированная схема разделения секрета. Представленная в [2] схема разделения секрета основана на (m,n)-пороговой схеме, где $m=2$ – количество частей, по которым возможно восстановление изображения, n – количество участников.

В основе восстановления секрета участниками лежит теорема: $\Phi_0^t + \Phi_1^t = Id \pmod 2$ тогда и только тогда, когда $t=2^m$, $m \in Z^+$. Здесь Φ – глобальная функция перехода клеточного автомата [3], основанная на локальных функциях перехода (1) и (2) соответственно, Id – преобразуемый массив данных.

$$s_{i,j}^{t+1} = (s_{i,j-1}^t + s_{i,j+1}^t) \bmod 2, \quad (1)$$

$$s_{i,j}^{t+1} = (s_{i,j-1}^t + s_{i,j}^t + s_{i,j+1}^t) \bmod 2. \quad (2)$$

Данная теорема легла в основу идеи об увеличении количества частей m.

Допустим, что одна из конфигураций клеточного автомата на шаге t была получена с помощью суммы двух других, развивающихся по правилам (1) и (2): $\Phi_2 + \Phi_3 = \Phi_0$, где каждая конфигурация также может быть представлена суммой двух других. Тогда:

$$\Phi_2 + \Phi_3 + \ldots + \Phi_{2i} + \Phi_{2i+1} = \Phi_0;$$
$$\Phi'_2 + \Phi'_3 + \ldots + \Phi'_{2j} + \Phi'_{2j+1} = \Phi_1.$$

Основываясь на рассматриваемой теореме, массив данных Id можно получить, суммируя составляющие каждой конфигурации:

$$\Phi_2 + \Phi_3 + \ldots + \Phi_{2i} + \Phi_{2i+1} + \Phi'_2 + \Phi'_3 + \ldots + \Phi'_{2j} + \Phi'_{2j+1} = Id.$$

Для организации данной структуры начальную конфигурацию клеточного автомата необходимо будет поделить на $2(i+j)$ частей и, изменив конфигурацию по необходимым правилам, раздать каждому участнику.

Но при такой схеме разделения секрета участники, количество которых меньше $2(i+j)$, смогут частично восстановить начальную конфигурацию, что будет являться уязвимостью данного алгоритма.

Если же Φ_0 и Φ_1 представить в виде суммы двух других конфигураций, каждая из которых тоже представляется суммой, то получаем древовидную схему (рис. 1).

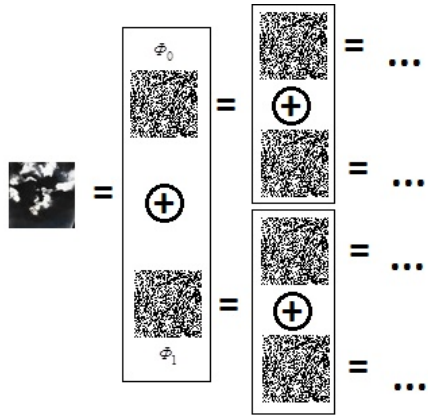


Рис. 1. Древовидная схема

В итоге для того чтобы получить конфигурацию клеточного автомата Id, необходимо сложить 2^m конфигураций, каждая из которых прошла m преобразований. Причем, согласно рис. 1, каждой конфигурации соответствует одна из возможных комбинаций переходных функций (1) и (2). Данный алгоритм имеет преимущество над предыдущим, так как описанная выше уязвимость отсутствует.

Модифицированная схема разделения секрета была программно реализована. В качестве примера на рис. 2 показаны конфигурации, рассчитанные программой, необходимые для восстановления исходного изображения для $(4,n)$-пороговой схемы. Из результатов работы программы видно, что исходное изображение и изображение, полученное после процедуры восстановления секрета (рис. 3), совпадают.

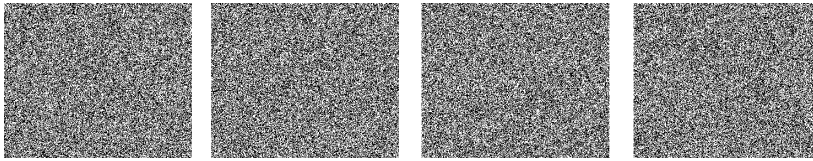
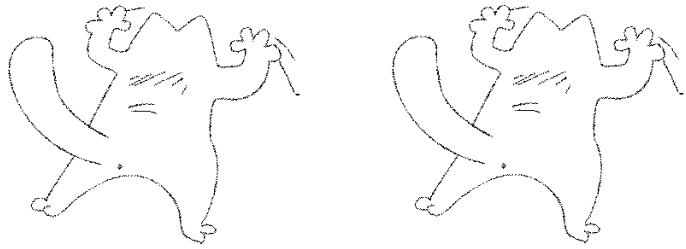


Рис. 2. Разделение секретного изображения



а *б*

Рис. 3. Исходное (*а*) и восстановленное (*б*) изображения

Заключение. Разработанный алгоритм представляет собой модификацию схемы разделения секрета: переход от схемы с n участниками и 2 необходимыми частями для восстановления секретного изображения к $(2^m, n)$-пороговой схеме, где n кратно 2^m, $n, m \in Z^+$. При этом устранена возможная уязвимость частичного восстановления.

ЛИТЕРАТУРА

1. Смарт Н. Криптография. М.: Техносфера, 2005. 528 с.

2. del Rey A.M. A secret sharing scheme for digital images based on two-dimensional linear cellular automata // Proc. of the 12-th Int. Workshop on Combinatorial Image Analysis (IWCIA 2008). Buffalo, NY, USA. 2008. P. 318–329.

3. Тоффоли Т. Машины клеточных автоматов / Т. Тоффоли, Н. Марголус. М.: Мир, 1991. 280 с.

ПОСТРОЕНИЕ БЕЗОПАСНОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ТЕСТИРОВАНИЯ ПРОГРАММ

С.А. Черепанов, М.М. Антонов,
И.В. Черноусов, П.Е. Густокашин, студенты
Научные руководители: Н.В. Кирнос, доцент каф. КИБЭВС, к.т.н.;
М.Ю. Катаев, профессор каф. АСУ, д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, каф. АСУ, sivkinpunk@gmail.com
Проект ГПО КИБЭВС-1102 (АСУ-1101) – «Программное обеспечение для организации и проведения спортивного программирования»

Терминология. Задача – вычислительная проблема, имеющая чётко сформулированное условие, строгий формат входных и выходных данных, алгоритм проверки соответствия входных данных выходным и ограничения на память и процессорное время.

Контест – набор задач, объединенных для проведения олимпиады, тренировки или лабораторной.

Решение – исходный код программы, написанный на одном из доступных пользователю языков программирования, получающий по заданным входным данным выходные [1].

Проблема автоматизированного тестирования решений. Одним из самых распространенных методов оценки корректности решений является визуальный анализ программного кода в сочетании с ручной проверкой решения на нескольких наиболее важных с точки зрения проверяющего тестах. Анализ производится человеком и потому не может являться объективным. Небольшое же количество тестов обусловливает низкое качество полученных результатов.

Значительно более надежным методом является полноценное тестирование – подача на вход программе набора тестов и сравнение реальных выходных данных с ожидаемыми выходными данными. Для достижения объективной оценки набор тестов должен покрывать все возможные ситуации.

На данный момент существуют системы, способные в автоматическом режиме проверять программы на наборах тестов. Они позволяют проводить олимпиадные соревнования, но малопригодны для учебного процесса по следующим соображениям:

– соревновательный элемент среди студентов не является необходимым;

– многие подсчитываемые характеристики (такие, как штрафное время сдачи задания) являются избыточными;

– диалог между студентом и преподавателем отсутствует.

Задачей нашего проекта является разработка и внедрение системы, позволяющей проводить автоматизированную проверку решений поставленных задач. Характеристики разрабатываемой системы: высокая производительность, доступность результатов проверки в реальном времени, интерактивное взаимодействие с пользователем, совместимость с правилами олимпиад по программированию ACM и ВКОШП, возможность проведения на ней лабораторных работ и тренировок, возможность запуска решения на исчерпывающем наборе тестов с указанными ограничениями.

Архитектура системы. Для решения поставленной задачи была разработана следующая структура (рис. 1). Система состоит из логически независимых блоков: интерфейса пользователя (сайта), базы данных и сервера тестирования. Пользователь взаимодействует с сайтом, информация с сайта записывается в базу данных, после чего сервер обрабатывает её: ядро тестирующей системы формирует вердикт, который заносится в базу данных и передаётся на сайт.

Сервер является блоком, реализующим бизнес-логику тестирования: поступающий от сайта исходный код сохраняется в базе данных,

после чего производится выборка всех непроверенных решений, каждое из которых впоследствии поступает в ядро для последующего тестирования.

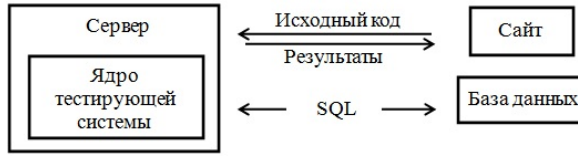


Рис. 1. Архитектура системы

Ядро выполняет компиляцию полученного от сервера решения, последующий его запуск на наборе тестов и отслеживание выполнения установленных ограничений.

Безопасность системы. Ключевым вопросом при построении описываемой системы является вопрос обеспечения ее безопасности. В разработанной системе данный вопрос рассмотрен с нескольких сторон.

Во-первых, в качестве системы безопасной аутентификации пользователей на сайте было выбрано готовое решение Authlogic от Binarylogic [2]. Данное решение является распространенным и отличается от аналогов повышенной гибкостью при адаптации под конкретную систему.

Во-вторых, для использования различных ресурсов и возможностей сайта была создана система разграничения доступа. Она основана на различных уровнях доступа пользователей: одноразовый, обычный, модератор и администратор. Одноразовые пользователи создаются на время проведения олимпиады, имеют доступ только к задачам данной олимпиады и уничтожаются по ее окончании. Обычные пользователи могут просматривать новости сайта, а также все задачи, размещенные на сайте, сдавать решения к этим задачам. Модераторы, помимо вышеперечисленного, могут создавать и редактировать новости. Администраторы имеют доступ к административному интерфейсу вебсайта, позволяющему управлять всем наполнением данного сайта.

В-третьих, не стоит забывать, что пользователь системы имеет возможность запустить на сервере тестирования абсолютно любой код, что не является допустимым, т.к. пользователь может модифицировать файловую систему, произвести запуск стороннего приложения, изменить скрипт тестирования и другие несанкционированные манипуляции. Чтобы этого не произошло, все решения запускаются на виртуальной машине, которая не имеет доступа к скрипту тестирования. Кроме того, все решения запускаются от имени специально созданного пользователя, у которого нет никаких прав, кроме права на чтение и

запись в папке с решением. После выполнения решения папка полностью очищается. Такой подход позволяет обеспечить должную безопасность и скорость восстановления после возможного сбоя – в этом случае достаточно лишь восстановить файл виртуальной машины.

По этим же соображениям для каждой задачи имеются ограничения по используемому времени и по используемой памяти. При превышении данных ограничений процесс решения немедленно уничтожается, а попытка получает вердикт о превышении соответствующего предела.

Кроме того, перед компиляцией все решения проверяются на наличие ассемблерных вставок. В олимпиадах формата ACM данные вставки запрещены, т.к. благодаря им даже нерациональное решение может все равно уложиться в ограничение по времени.

ЛИТЕРАТУРА

1. Cormen T. Introduction to algorithms / T. Cormen, C. Leiserson, R. Rivest, C. Stein. McGraw-Hill Science, 2003. 1056 с.

2. Documentation for binaryligic/authlogic [Электронный ресурс]. Режим доступа: http://rdoc.info/github/binarylogic/authlogic. 27.02.2014.

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРИМЕРЕ ООО «РИЦ ЖКХ»

Р.О. Дектяренко, студент, А.И. Кураленко, аспирант

г. Томск, ТУСУР, РТФ, каф. РЗИ, ulquiorra4esp@gmail.com

Желание иметь систему обеспечения информационной безопасности (СОИБ), адекватную целям информационной безопасности организации, приводит к стремлению совершенствовать СОИБ. Для этого необходимо оценивать эффективность и на ее основе модернизировать СОИБ. В настоящее время активно развиваются различные методы оценки эффективности СОИБ. Большинство подходов при этом опираются на мнение экспертов [1].

Большинство факторов, влияющих на информационную безопасность организации, имеют качественный характер. Эксперт использует качественные, нечеткие оценки типа «система недостаточно эффективна», «система эффективна», «система очень эффективна» и т.д. Естественно, что нечеткие понятия должны использоваться при оценке эффективности системы обеспечения информационной безопасности.

В качестве инструмента оценки эффективности СОБИ разработан метод, в основе которого лежит аппарат нечеткой логики [2].

В качестве входных значений для проведения оценки используются «Вероятность угрозы», «Соответствие мер защиты требованиям»,

выходные значения «Эффективность СОБИ» и степень истинности данных значений.

Оценка эффективности проводится на основе эталона, в качестве которого, например, могут выступать требования нормативных документов либо экспертные оценки. Например, при угрозе внедрения программной закладки согласно [3] должны быть приняты меры реализации антивирусной защиты, обновления базы данных признаков вредоносных компьютерных программ (вирусов). На основе экспертной оценки выставляется коэффициент «Соответствие мер защиты требованиям».

Запись полученных входных и выходных значений, необходимых для проведения оценки, на примере входного параметра «Вероятность угрозы»:

β = вероятность угрозы; T = («очень низкая», «низкая», «средняя», «высокая», «очень высокая»); X = [0, 100].

$P1$ = <«Вероятность угрозы» («очень низкая», «низкая», «средняя», «высокая», «очень высокая»), [0, 100] >

Аналогично и для «Соответствия мер требованиям» и «Эффективность СОБИ».

Для каждой из переменных задаются функции принадлежности (зависимость степени истинности от количественного значения переменной), например, для «Вероятности угрозы» они представлены на рис. 1.

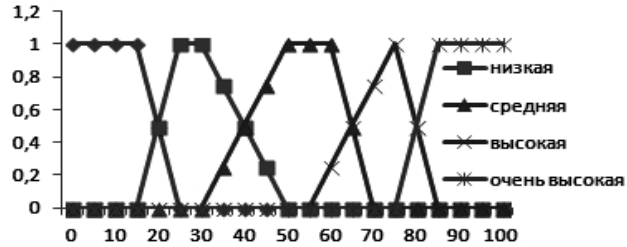


Рис. 1. Функции принадлежности переменной «Вероятность угрозы»

Степень истинности показывает, насколько можно быть уверенным при отнесении количественного значения к качественному терму (классу).

С помощью полученных качественных значений входных переменных осуществляется переход к качественным значениям выходной переменной на основе созданных правил. Например, если актуальность угрозы очень высокая или высокая и соответствие мер требованиям малое, то СОИБ совсем не эффективна.

Преимущества данного метода в том, что он позволяет оценить эффективность СОБИ как возможность противостоять актуальным угрозам. Также предусмотрен вариант учитывать требования нормативных документов и различных стандартов по ИБ.

На примере ИСПДн ООО «РИЦ ЖКХ» проведена оценка эффективности СОИБ таким методом. Схема информационной сети РИЦ ЖКХ представлена на рис. 2.

Определен 3-й уровень защищенности ИСПДн[4], перечень угроз РИЦ ЖКХ [5].

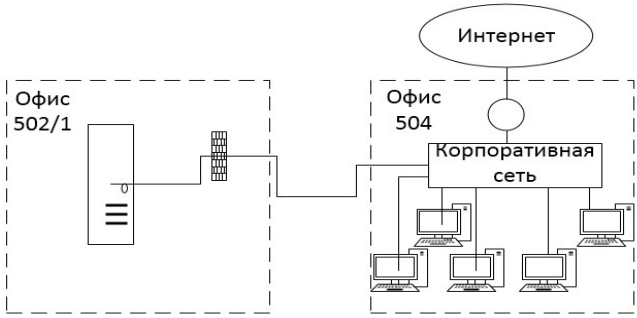


Рис. 2. Схема информационной сети РИЦ ЖКХ

Вероятность угроз определена в соответствии с методикой [5], каждой из угроз присвоен весовой коэффициент «Вероятность угрозы» в зависимости от вероятности угрозы. Определение значений «Соответствие мер требованиям» проведено экспертным путем. На основе базы правил определенно значение выходной величины «Эффективность СОБИ» для каждой из ранее определенных угроз. Представлены рекомендации по модернизации СОБИ.

В результате работы предложен метод оценки эффективности СОБИ на основе нечеткой логики. Произведена оценка эффективности системы защиты ПДн ООО «РИЖ ЖКХ» данным методом. Определена вероятность реализации угроз, оценена эффективность системы защиты ПДн ООО «РИЦ ЖКХ» по каждой угрозе.

ЛИТЕРАТУРА

1. Голдуев Н.А., Адрианов В.В., Голованов В.Б., Зефиров С.Л. Обеспечение информационной безопасности. М.: Алпина паблишер, 2011. 338 с.

2. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений. М.: Мир, 1976. 167 с.

3. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

8. Постановление Правительства от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК от 14 февраля 2008 г.

ИЗУЧЕНИЕ СЕТЕВЫХ ТЕХНОЛОГИЙ НА ПРИМЕРЕ МЕЖСЕТЕВОГО ЭКРАНА CISCO ASA

Д.О. Дубровин, студент

Научный руководитель А.С. Ковтун, аспирант

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, tcompote@gmail.com

Число пользователей Internet продолжает неуклонно расти. Организации рано или поздно принимают решение по подключению своих локальных сетей к сети глобальной. Но не стоит забывать, что Интернет – не только неисчерпаемый источник информации и перспективное поле деятельности для бизнеса, но еще и источник множества угроз – угроз нарушения безопасности компьютеров локальной сети и конфиденциальности содержащейся в них информации.

Часть задач по отражению наиболее возможных угроз для внутренних сетей могут решать межсетевые экраны. Использование межсетевых экранов дает возможность организовать внутреннюю политику безопасности сети предприятия.

Цель работы – рассмотрение одного из наиболее часто используемых средств защиты – межсетевого экрана на примере Cisco ASA 5505.

Были исследованы следующие функциональные возможности Cisco ASA:

– реализация технологии VLAN;

– реализация технологии NAT;

– реализация технологии ACL;

– реализация технологии QoS.

Кроме того, потребовалось исследовать возможность работы ОС Cisco ASA в эмулируемой среде.

Практические задания выполнялись на лабораторном стенде, представленном на рис. 1 (слева). В составе стенда следующее оборудование:

– межсетевой экран Cisco ASA 5505;

– KVM-переключатель Aten CS1308;

– коммутатор Mikrotik RouterBoard 1100 AH;

– 2 сервера 1U-формата Supermicro.

Для реализации поставленных практических задач все устройства были соединены согласно схеме на рис. 1 (справа).

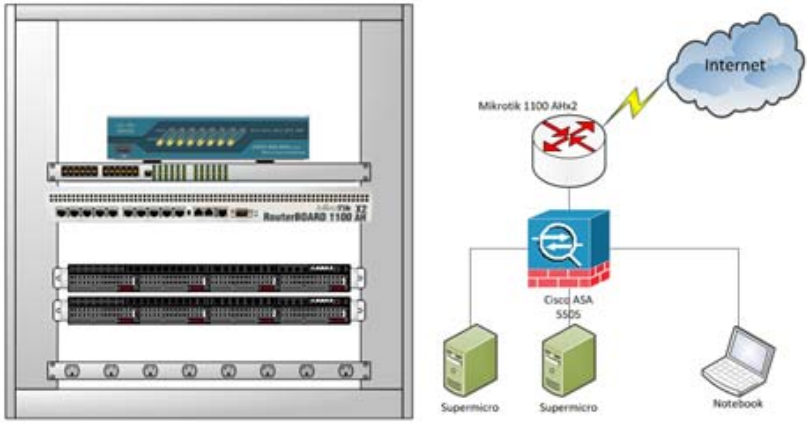


Рис. 1. Лабораторный стенд и схема соединений

По мере выполнения поставленных задач сформировалась логическая схема сети (рис. 2).

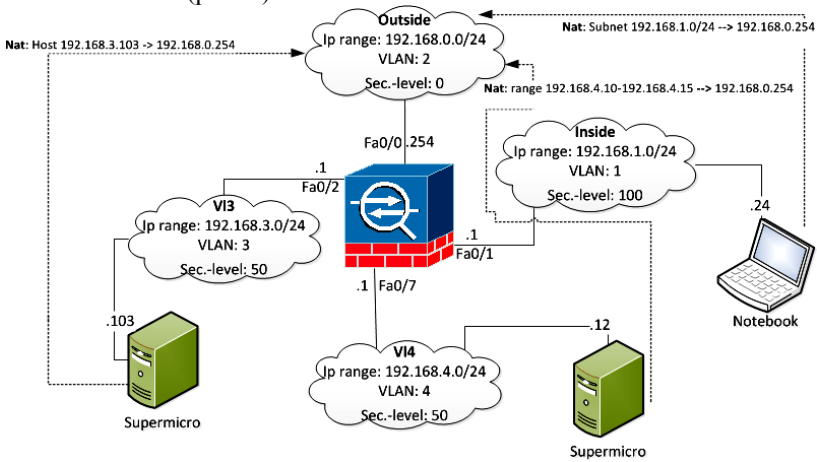


Рис. 2. Логическая схема сети

Разберем получившуюся сеть по пунктам:

1. VLAN: в каждой сети своя адресация вида 192.168.<VLAN_ID>.0/24 (кроме Outside). Настроены ip-адреса на интерфейсах ASA. Для локальных сетей включен DHCP-сервер. У каждой сети свой уровень безопасности.

2. Настроен SSH-, Telnet-, Web-доступ к управлению устройством.

3. Настроена трансляция локальных адресов во внешний адрес Cisco ASA.

4. ACL: разрешен трафик только определенного вида между локальными сетями (icmp, NetBIOS). Между локальными и внешними сетями разрешен только DNS- NTP- и HTTP-трафик. Настроена Time-Based ACL для HTTP-трафика.

5. QoS: ограничена полоса пропускания для HTTP-трафика определенным хостам.

Все действия были воссозданы в GNS3-эмуляторе сетевого оборудования Cisco и Juniper.

Следующий этап – продолжение изучения функций межсетевого экрана Cisco ASA. Например, агрегирование каналов, резервные маршруты, PoE, реализация отказоустойчивости и др.

В дальнейшем на основе полученных результатов будет разработан курс лабораторных работ.

ЛИТЕРАТУРА

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов. 4-е изд. СПб.: Питер, 2010. 944 с.

2. Таненбаум Э. Компьютерные сети. Сер. Класссика Computer Science. 4-е изд. СПб.: Питер, 2003. 902 с.

3. Руководство по конфигурированию устройств Cisco ASA 5500 серии, [Электронный ресурс]. Режим доступа: http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/configuration/guide/config.html

АНАЛИЗ СОСТОЯНИЯ УТЕЧЕК ИНФОРМАЦИИ В РФ В 2013–2014 гг.

Ю.М. Фурсова, студентка

Научный руководитель О.Н. Мызников, доцент каф. КТИБ, к.т.н.

г. Краснодар, КубГТУ, iitib_krasnodar@mail.ru

К настоящему времени в нормативно-правовой базе РФ сформировался перечень документов, направленных на регулирование вопросов в сфере информационной безопасности: Доктрина информационной безопасности РФ, Стратегия развития информационного общества, Основы государственной политики Российской Федерации в области информационной безопасности (ИБ) на период до 2020 г. и ряд других. Но несмотря на существующие методы организационно-правового регулирования, в правовой сфере остаются пробелы, образовавшиеся в связи с появлением таких сравнительно новых явлений, как кибернаемники и кибероружие [1].

Следует понимать невозможность построения полноценной системы мер по обеспечению ИБ государства и общества, основываясь только на законодательной части. Поэтому, помимо законотворческой инициативы, стоит поддерживать на государственном уровне производителей отечественного программного обеспечения (ПО) и аппаратно-программных средств, разработать новые и модернизировать существующие подходы к подготовке специалистов в области информационных технологий (ИТ) [2].

Согласно исследованию в области утечек конфиденциальной информации, проводимому ГК «Infowatch», в 2013–2014 гг. было зафиксировано свыше 800 случаев утечки информации [3, 4]. Большая часть утечек приходится на персональные данные (ПДн) – 93,8%, причем 67% приходится на коммерческие организации, и около 30% на государственные структуры. При этом количество неопределенных источников утечки сократилось до 3%.

Следует отметить, что почти в половине случаев утечка произошла умышленно. Это позволяет говорить, что утечка конфиденциальной информации не всегда является злонамеренным действием.

Исследования, представленные в [4], свидетельствуют:

1) о крайней ликвидности ПДн и стабильной популярности у злоумышленников;

2) общий уровень защиты данных крайне низок;

3) коммерческие и государственные организации готовы раскрывать факт утечки и проводить исследования инцидентов;

4) те же коммерческие организации не проводят эффективных мер для предотвращения утечек данных.

Следующими по количеству утечек являются конфиденциальные сведения, связанные с коммерческой деятельностью, – 3,4%. Так как утечка данного характера полностью сказывается на финансовом положении компаний любого размера, то для них вопрос о защите секретов производства встает наиболее остро.

Согласно [5] остаются популярными атаки, связанные с кражей данных государственных, ведомственных и муниципальных учреждений, а также крупных промышленных, отраслевых компаний. Такие атаки приобрели целевой характер и организовывались профессиональными группировками, в том числе наёмными, занимающимися кибершпионажем и кибердиверсиями [6].

Стремительный прогресс в области ИТ привел к активной компьютеризации бизнес-процессов. Поэтому в последнее время жертвами краж данных становились коммерческие организации. Целью атак в данном случае становились хищение и уничтожение ценной коммерческой информации, кража денежных средств, нанесение финансового

ущерба и, как следствие, падение доверия к компании. В подавляющем большинстве случаев злоумышленники действуют так же целенаправленно и планомерно, предварительно собрав и изучив всю необходимую информацию о компании.

Как и раньше, злоумышленники активно используют пресловутый «человеческий фактор». Зная о неграмотности подавляющего большинства пользователей в вопросах ИБ, злоумышленники прибегают к методам социальной инженерии, чтобы собирать данные об организации, ее сотрудниках и другую информацию, необходимую для проведения успешной атаки.

С развитием и популяризацией мобильных технологий под угрозой оказались данные пользователей, хранящиеся на смартфонах и других мобильных устройствах. Особенно уязвимы устройства на базе ОС Android, для которых за последний год было обнаружено почти 98% вирусных приложений из всего вредоносного ПО для мобильных телефонов (в том числе мобильные ботнеты, бэкдоры).

Помимо этого, на практике оказывается, что мобильное вредоносное ПО более опасно по сравнению со зловредами, предназначенными для персональных компьютеров (ПК).

Распространение кроссплатформерного ПО дает злоумышленникам больший простор для их деятельности – это позволяет разрабатывать вредоносные приложения для различных ОС и платформ, используя эксплойты одних и тех же, в том числе популярных программ (например, Java, Adobe).

В дальнейшем, предполагают авторы [5], следует ожидать динамику в развитии вредоносного ПО для мобильных устройств, учащение атак на облачные хранилища данных в связи с огромным количеством информации на них, а также популяризации услуг кибернаемников.

Таким образом, представив сложившуюся картину в области утечек, можно заметить назревающие сложности и проблемы:

1) из-за увеличивающегося массива данных будет необходимо посмотреть на безопасность пользовательских данных с новой стороны, изменив существующие концепции в применении средств и систем защиты информации;

2) реализация комплексного подхода в анализе угроз и методов их предотвращения будет требовать привлечения многих специалистов, каким-либо образом связывающих свою деятельность с информационными коммуникациями;

3) по причине роста числа угроз и изменения их характера стоит обратить внимание не только специалистов в области ИТ, но и самих пользователей на эту проблему.

ЛИТЕРАТУРА

1. Проект концепции Стратегии кибербезопасности Российской Федерации [Электронный ресурс]. Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf, свободный (дата обращения: 24.02.2014).
2. Прогноз научно-технологического развития Российской Федерации на период до 2030 года [Электронный ресурс]. Режим доступа: http://government.ru/media/files/41d4b737638b91da2184.pdf, свободный (дата обращения: 24.02.2014).
3. Глобальное исследование утечек конфиденциальной информации в 2013 году [Электронный ресурс]. Режим доступа: http://www.infowatch.ru/report2013, открытый (дата обращения: 04.03.2014).
4. Безопасность персональных данных в России в 2013 году. Статистика утечек. Отраслевые особенности [Электронный ресурс]. Режим доступа: http://www.infowatch.ru/analytics/reports/5538, открытый (дата обращения: 24.02.2014).
5. Kaspersky Security Bulletin 2013. Развитие угроз в 2013 году [Электронный ресурс]. Режим доступа: http://www.securelist.com/ru/analysis/208050823/Kaspersky_Security_Bulletin_2013_Razvitie_ugroz_v_2013_godu, свободный (дата обращения: 22.02.2014).
6. Конкурентная разведка и аналитические системы для бизнеса и госсектора: матер. практ. конф., г. Москва, 14 ноября 2013 года [Электронный ресурс]. Режим доступа: http://infosystems.ru/services/conference/competitive_intelligence_and_analysis_systems/speaker_presentations.html (дата обращения: 22.02.2014).

СПОСОБЫ ОПРЕДЕЛЕНИЯ ВОЗРАСТА ЧЕЛОВЕКА ПО УЧЕТНОЙ ЗАПИСИ В СОЦИАЛЬНОЙ СЕТИ

В.С. Грезин, магистр каф. АДМ ЮФУ

Научный руководитель М.Г. Адигеев, доцент каф. АДМ, к.т.н., ЮФУ

Соруководитель В.А. Новосядлый, к.ф.-м.н.,
ФГАНУ НИИ «Спецвузавтоматика»

г. Ростов-на-Дону, ЮФУ, vladimirgrezin@gmail.com

Современные социальные сети не могут обеспечить правильность заполнения всех граф учетной записи. Особенно это касается графы «возраст», которую пользователи социальной сети часто предпочитают скрывать. Это не позволяет в автоматическом режиме контролировать доступ таких пользователей к контенту, доступ к которому ограничен по закону №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». В связи с этим тематика автоматического определения возраста на основе профиля учетной записи социальной сети является актуальной.

Целью данного исследования является изучение и разработка способов автоматического определения наиболее вероятного возраста участника социальной сети по информации из его учетной записи.

Способы определения возраста. Тематика определения возраста владельца учетной записи социальной сети или автора сообщений изучается во множестве работ. Например, исследование [1] описывает характеристики текста и метаданных блогов, которые могут быть использованы для определения возраста, в том числе количество и время размещения сообщений, словарный запас, грамматические и пунктуационные особенности, количество и метаданные профилей друзей. В работе [2] используется анализ сообщений в чате, чтобы определить возраст. В работе [3] исследуется определение возраста человека, опираясь на его историю посещенных страниц в Интернет.

В отличие от указанных работ, в данной работе для определения возраста использован возраст людей из круга общения владельца учетной записи. В настоящем исследовании изучены три способа определения возраста человека на основе его круга общения: математическое ожидание, медиана и нейронная сеть.

Математическое ожидание. Одним из наиболее очевидных статистических способов определения возраста человека, исходя из данных о возрасте людей из его круга общения, является среднее арифметическое возрастов этих людей, то есть математическое ожидание в случае дискретной выборки (рис. 1). Действительно, логично предположить, что в кругу общения каждого человека есть люди несколько старше и несколько младше него, а также значительная часть ровесников. Проведенные эксперименты показали, что во многих случаях это действительно так. Однако нельзя забывать, что источником данных для анализа служат открытые страницы в социальных сетях. Как показала практика, люди нередко указывают совершенно неверный, даже абсурдный год рождения по тем или иным причинам. Как показано на рис. 1, указанный у друзей некорректный год рождения приводит к резкому перекосу частотной диаграммы возрастов, который может оказать большое влияние на результат, в данном случае – 6 лет.

Медиана.Чтобы нейтрализовать показанный в предыдущем случае эффект, следует воспользоваться медианой вместо среднего арифметического (рис. 2). Ее главной особенностью является игнорирование всплесков на краях интервала. Если применить ее к предыдущему случаю, то получится более точный результат. Теперь некорректно указанный возраст не приводит к смещению результатов из-за некорректно указанного года рождения в некоторых учетных записях.

Рис. 1. Распределение возрастов друзей и предполагаемый год рождения для математического ожидания

Рис. 2. Распределение возрастов друзей и предполагаемый год рождения для медианы

Нейронная сеть. Принципиально другим подходом к проблеме является использование нейронной сети вместо статистических методов. Имея достаточно хорошую обучающую выборку, можно добиться лучших результатов по сравнению с предыдущими способами. Эксперименты показали точность определения возраста с ошибкой не более года на широком наборе тестовых данных. Для обучения сети следует использовать заранее подготовленные пары (возраст – возраст людей из окружения). Основной проблемой этого подхода является как раз сложность выбора обучающих данных.

Заключение. Представленные методы позволяют добиться хороших результатов в подавляющем большинстве случаев. Данная информация не может быть использована напрямую для автоматического ограничения доступа к контенту, однако может послужить сигналом для необходимости запроса на подтверждение личности и возраста владельца учетной записи. Также заметим, что на некоторых выборках, например когда частотная диаграмма распределения возрастов почти горизонтальная, необходимо использовать дополнительные приемы. Наиболее перспективным представляется работа с социальным графом использования модифицированного алгоритма поиска клик для нахождения социальных подгрупп. Далее на этих подгруппах можно использовать описанные выше способы.

ЛИТЕРАТУРА

1. Burger J. and Henderson J. An Exploration of Observable Features Related to Blogger Age // AAAI Spring Symposium: Computational Approaches to Analyzing Weblogs. AAAI, 2006. P. 15–20.

2. Peersman C., Daelemans W., and L. Van Vaerenbergh. Predicting age and gender in online social networks // In Proceedings of the 3-rd international workshop on Search and mining user-generated contents (SMUC '11). ACM, New York, NY, USA, 2011. P. 37–44. DOI=10.1145/2065023.2065035 http://doi.acm.org/10.1145/2065023.2065035

3. Kakkar M., Upadhyay D. Web Browsing Behaviors Based Age Detection // International Journal of Soft Computing and Engineering (IJSCE). 2013. Vol. 3, Issue-1. March. P. 99–101.

КОМПЛЕКСНАЯ СИСТЕМА ЭЛЕКТРОННОГО ОБУЧЕНИЯ

Р.П. Хрусталёв, студент каф. КИБЭВС

Научный руководитель А.А. Конев, доцент каф. КИБЭВС

г. Томск, ТУСУР, hrhryst@gmail.com

В современном обществе во всех сферах люди стараются всё автоматизировать и упростить, в чём им помогают быстро развивающиеся технологии. Информация становится всё более доступна, и это не могло не повлиять на процессы обучения. Такие системы, которые помогают проводить удалённые веб-конференции и лекционные занятия, также сейчас принято называть e-learning или электронное обучение.

Представителем таких систем являются open source продукты Big Blue Button и Moodle, их связка даёт возможность организовать электронный центр обучения, что позволяет проводить удалённые лекционные занятия в реальном времени с интерактивным взаимодействием преподавателя и студента посредством видео- и аудиосвязи.

Big Blue Button – это открытое программное средство, которое используется для проведения онлайн-встреч или показа презентаций в режиме реального времени, через сеть Интернет, в данном продукте имеется поддержка транслирования аудио и видеопотока в режиме реального времени, возможность показа презентаций форматов документов пакета Microsoft Office и OpenOffice, изображений, PDF-файлов, предоставление доступа к рабочему столу пользователей и прямое транслирование рабочего стола в веб-конференцию, это удобно для просматривания проделанных работ студентов лектором.

Big Blue Button имеет возможность предоставления доступа к рабочему столу пользователей и прямоо транслирования рабочего стола в веб-конференцию, это удобно для просматривания проделанных работ студентов лектором методом поочерёдной передачи прав слушателем для показа рабочих столов.

Второй элемент данной комплексной системы электронного обучения – LMS Moodle (модульная объектно-ориентированная динамическая учебная среда) – это свободная система управления обучением, ориентированная прежде всего на организацию взаимодействия между преподавателем и студентами, которая была специально разработана для электронного обучения. Она даёт расширенные возможности преподавателям и студентам, первым позволяет создавать курсы лекций, добавлять к курсам материалы к лекциям с помощью различных расширений в виде плагинов, вторым – отслеживать появление новых курсов из своих электронных кабинетов, просматривать записи прошедших лекций.

Взаимодействие между Big Blue Button и LMS Moodle происходит по специальному плагину, который устанавливается в LMS Moodle.

После создания курса и подключения модуля мы имеем готовый курс удалённого ведения лекционных занятий по различным дисциплинам, которые предусмотрены учебным планом.

В данной комплексной системе обучения существуют различные роли пользователей, каждый из которых наделён своими полномочиями:

– *Слушатели* – это пользователи, которые могут только смотреть презентации и видео, а также использовать чат для переговоров с другими участниками вебинара. Например, налогоплательщики – это слушатели.

– *Выступающий* – имеет все возможности слушателя и дополнительно может загружать и управлять показом презентаций и демонстрировать другим участникам работу программ на рабочем столе своего компьютера. Например, инспектор ИФНС – это выступающий.

– *Ведущий* – имеет все возможности слушателя и выступающего и дополнительно может осуществлять управление параметрами BigBlueButton.

Каждый зарегистрированный пользователь после входа в учебную среду попадает в личный кабинет, где наглядно представлены все курсы, на которые он записан, и расписание предстоящих занятий, также для него открывается возможность по управлению своего личного профиля с широким спектром инструментов

Профиль студента отображает различные настройки, список тех курсов, на которые он записан, систему обмена сообщений между пользователями moodle.

У администратора и ведущего в комплексной системе по электронному обучению более высокие приоритеты, создание новых курсов, регистрация новых пользователей и т.д.

Также в комплексе по электронному обучению присутствует как ручное создание курсов и запись пользователей на них, так и существует дополнение к LMS Moodle «электронный деканат», это свободно распространяемая разработка. Free Dean's Office (Электронный деканат) – это модуль для среды дистанционного обучения Moodle, который добавляет возможность управления процессом обучения колледжей и вузов. Free Dean's Office позволяет оперировать такими объектами, как «Специальность», «Академическая группа», «Семестр», «Нагрузка преподавателя», «Расписание», «Текущие оценки и посещаемость», «Зачетная книжка» и т.д.

Данный комплекс работает со всеми известными на данный момент браузерами, для комфортной работы требуется стабильная связь с сетью Интернет, не менее 10 Мбит/с, предустановленные программные продукты java runtime environment и adobe flash player; техническое оснащение для работы предполагает, что у пользователя имеется аудиогарнитура с микрофоном и веб-камера.

Гибкость настроек – в модуль можно внести любые изменения: добавить нужный функционал, интегрировать «Деканат» с вашими базами данных или информационными системами, адаптировать его к бизнес-процессам. При этом итоговая стоимость проекта может оказаться значительно ниже, чем покупка лицензий на аналогичные продукты, которые нужно будет внедрять и настраивать самостоятельно, без возможности какой-либо адаптации сверх предусмотренных разработчиками настроек.

Открытый исходный код – «Электронный деканат» поставляется клиенту под свободной лицензией GNU GPL. Эта лицензия не ограничивает использование продукта, в том числе и по истечении договора технической поддержки. Модель можно настраивать или дорабатывать.

Система имеет очень большой спектр возможностей и манипуляций, также имеется возможность доработки и подключения своих собственных разработанных плагинов и дополнений за счёт широкой освещённости и масса ресурсов, посвящённых данной технологии.

Преимущество данной технологии заключается в удобной подаче материала для слушателей и интерактивном взаимодействии с аудиторий, где сами слушатели напрямую общаются с лектором не зависимо от их географического места расположения как слушателей, так и лектора.

ЛИТЕРАТУРА

1. Big Blue Button [Электронный ресурс]. Режим доступа: http://bigbluebutton.org/overview/, свободный (дата обращения: 05.03.2014).

2. LMS Moodle [Электронный ресурс]. Режим доступа: https://moodle.org/?lang=ru, свободный (дата обращения: 05.03.2014).

3. Free Dean's Office (Электронный деканат) [Электронный ресурс]. Режим доступа: http://www.deansoffice.ru/, свободный (дата обращения: 05.03.2014).

РЕАЛИЗАЦИЯ ПЕРЕКРЕСТНОГО ШИФРОВАНИЯ НА ОСНОВЕ АЛГОРИТМОВ RIJNDAEL И MARS. ГЕНЕРАЦИЯ НЕПРИВОДИМЫХ ПОЛИНОМОВ. ГЕНЕРАЦИЯ КЛЮЧЕЙ

С.А. Кошлаков, Р.С. Шубин, студенты

Научный руководитель В.Г. Дурнев, д.ф.-м.н., профессор

г. Ярославль, Ярославский государственный университет им. П.Г. Демидова, rectorat@uniyar.ac.ru

Цель работы состояла в решении следующих задач:

- модификация алгоритмов Rijndael и MARS, а также реализация модифицированных алгоритмов;
- реализация перекрестного шифрования указанными алгоритмами;
- генерация неприводимых унитарных полиномов над произвольным полем Z_p;
- генерация ключей для используемых алгоритмов;
- анализ криптографических свойств реализованных алгоритмов.

Rijndael и MARS являются алгоритмами блочного симметричного шифрования, оба участвовали и стали финалистами в конкурсе AES, направленном на выбор нового криптографического стандарта США. 2 октября 2000 г. победителем конкурса AES был признан алгоритм Rijndael, который до настоящего времени продолжает быть криптографическим стандартом США. В рамках выполнения работы оба алгоритма были модифицированы и программно реализованы на языке программирования C#. В данном случае модификация означает рас-

ширение возможностей алгоритмов для их корректной работы в любых конечных полях $Z_p[x] / f(x) = GF(p^n)$, где p – простое число; n – целое положительное, $f(x)$ – произвольный неприводимый унитарный полином степени n над Z_p. Соответственно все внутренние методы модифицируемых алгоритмов были адаптированы для работы в таких полях с условием сохранения их структуры и смысловой нагрузки. Для достижения упомянутой цели была реализована арифметика в произвольном конечном поле вышеуказанного вида. Кроме того, модифицированные алгоритмы допускают включение/исключение из их составов основных методов, что позволяет при анализе отслеживать их роль и вклад в параметры алгоритмов, а также изменение количества раундов и итераций на произвольное значение.

Следующим шагом была реализация перекрестного шифрования на основе модифицированных алгоритмов, которая позволяет применить к открытому тексту поочередное шифрование обоими алгоритмами согласно случайной последовательности произвольной длины, состоящей из 0 и 1, где 0 отвечает за выбор алгоритма Rijndael, а 1 – MARS.

Оригинальный алгоритм Rijndael работает в поле $Z_2[x]/f(x)=GF(2^8)$, где $f(x) = x8 + x4 + x3 + x + 1$. Для его работы в произвольном конечном поле $Z_p[x] / f(x) = GF(p^n)$, где p – простое число; n – целое положительное, необходим неприводимый унитарный полином $f(x)$ степени n над Z_p. Для этой цели служит метод генерации неприводимых унитарных полиномов степени n над произвольным полем Z_p, который также реализован в рамках выполнения работы. При этом пользователю дается возможность сгенерировать любой неприводимый полином $f(x)$ из множества всех неприводимых полиномов степени n над Z_p для заранее определенных p и n.

Согласно правилу разработки криптографических систем в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключевой информацией, а сам алгоритм шифрования должен быть открытым. В рамках созданной программной реализации в понятие ключевой информации помимо ключа входит набор всех параметров шифрования, доступных для изменения пользователю. При генерации ключей нестойким алгоритмом криптосистема будет нестойкой. Вскрытию подвергнется не сам шифр, а алгоритм генерации ключей. Хорошими ключами являются последовательности случайных бит, то есть все возможные ключи из пространства ключей должны быть равновероятны. Чем больше мощность ключевого пространства, тем лучше. При реализации метода генерации ключей был использован стандарт ANSI X9.17. Данный стандарт допускает использовать в качестве своей основы произвольный криптоалгоритм,

поэтому выбор пал на реализованные модифицированные алгоритмы Rijndael, MARS, а также перекрестное шифрование на их основе в зависимости от выбранных параметров.

Завершающим этапом в работе является анализ криптографических свойств реализованных алгоритмов, который основывался на следующих показателях:

- расстояние Хэмминга между блоками данных до и после применения метода шифрования (есть возможность сравнения вновь зашифрованного текста с начальным открытым текстом либо с зашифрованным на предыдущем шаге);
- коэффициент лавинного эффекта между блоками данных (есть возможность сравнения вновь зашифрованных текстов между собой с условием, что их прообразы (начальные открытые тексты либо тексты, зашифрованные на предыдущем шаге) случайным образом отличаются на заданное расстояние Хэмминга;
- коэффициент корреляции между блоками данных до и после применения метода шифрования (есть возможность сравнения вновь зашифрованного текста с начальным открытым текстом либо с зашифрованным на предыдущем шаге);
- разница между блоками данных до и после применения метода шифрования, представимая в виде суммы разностей значений соответствующих псевдобит двух сравниваемых блоков данных (есть возможность сравнения вновь зашифрованного текста с начальным открытым текстом либо с зашифрованным на предыдущем шаге);
- деление блока данных пополам и интерпретация каждой половинки как координаты x и y соответственно, а также последующая визуализация на графике.

Следует добавить, что все перечисленные показатели реализованы и визуализированы в программной реализации рассматриваемых алгоритмов в виде соответствующих графиков. Таким образом? пользователю при выборе параметров шифрования дается возможность наглядного представления криптографических свойств выбранной им модификации алгоритма шифрования, что позволяет ему настроить алгоритм шифрования в соответствии с приоритетами конкретных задач (использование алгоритмов с различным соотношением скорости работы и криптозащищенности).

При анализе было выявлено, что стандартные алгоритмы Rijndael и MARS являются достаточно стойкими, а при изменении их параметров в сторону усложнения (увеличения p, q, неприводимого полинома, увеличения ключа и ключевого множества, увеличения количества раундов и итераций алгоритмов, применении перекрестного шифрова-

ния) анализируемые параметры выдают значения лучше или такие же, как в случае использования оригинальных алгоритмов. На основании этого можно сделать предположение, что стойкость модифицированных алгоритмов возрастает или как минимум не убывает при усложнении параметров.

ЛИТЕРАТУРА

1. Спецификация алгоритма Rijndael. Federal Information Processing Standards Publication 197, 2001 // Сайт NIST (National Institute Of Standarts and Technology): http://csrc.nist.gov/. Веб страница: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

2. Мао Венбо. Современная криптография: теория и практика: Пер. с англ. М. : Изд. дом «Вильямс», 2005. 768 с.

3. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001. 368 с.

4. Doe J. Преимущества алгоритма шифрования Rijndael (AES). 20 марта 2010 // http://www.lapshin.biz/ Веб-страница: http://www.lapshin.biz/6778/preimushestva_algoritma_shifrovanija_rijndael_(aes).php

5. Фергюсон Нильс, Шнайер Брюс. Практическая криптография. М.: Изд. дом «Вильямс», 2005. 424 с.

6. Чмора А.Л. Современная прикладная криптография. 2-е изд. М.: Гелиос АРВ, 2002. 256 с.

7. Яблокова С.И. Основы алгебраической алгоритмики. Ч. 2. Ярославль: ЯрГУ, 2009.

8. Создание случайных чисел // ИНТУИТ национальный открытый университет: http://www.intuit.ru/. Веб-страница: http://www.intuit.ru/studies/courses/28/28/lecture/885?page=6

9. Генерация ключей // Бесплатный электронный учебник по информационной защите компьютера: http://www.help-antivirus.ru/. Веб-страница: http://www.help-antivirus.ru/protectioninformation/6/Index6.php

10. Carolynn Burwick. Спецификация алгоритма MARS // IBM Corporation. August, 20. 1999.

11. Carolynn Burwick. MARS – a candidate cipher for AES. IBM Corporation. 1999. September, 22.

12. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. 576 с.

13. Victor Shoup. A Computational Introduction to Number Theory and Algebra (Version 2). 2008

14. Глухов М.М., Нечаев А.А., Елизаров В.П. Алгебра: учеб. для вузов: в 2 т. М.: Гелиос АРВ, 2002. 336 с.

МОДЕЛЬ АДАПТИВНОГО УПРАВЛЕНИЯ ПРОФИЛЕМ ЗАЩИТЫ МОБИЛЬНОГО УСТРОЙСТВА

Д.О. Маркин, адъюнкт

Научный руководитель В.В. Комашинский, к.т.н., доцент

г. Орел, Академия ФСО России, admin@nikitka.net

На современном этапе развития все более активно в повседневную деятельность внедряются различные мобильные устройства (МУ) [1]. Однако, применение МУ в корпоративных сетях создает новые проблемы в сфере обеспечения *безопасности информации* [2], поскольку появляются условия для нарушения безопасности информации вследствие различных объективных и субъективных факторов как внутреннего, так и внешнего характера [3].

Решение данных проблем может быть найдено в случае разработки такой модели управления доступом пользователей МУ, в которой будут учтены:

– закономерности и зависимости динамики использования МУ;

– параметры окружения или так называемого контекста доступа, в условиях которого осуществляется доступ к услугам корпоративной сети, в том числе с разными уровнями конфиденциальности;

– функциональные особенности и аппаратно-программные особенности МУ, способные спровоцировать появление инцидентов безопасности внутри корпоративной сети;

– способы управления профилем защиты МУ, позволяющие повысить безопасность информации и в том числе устранить возможности утечки информации, минимизировать вероятность НСД к информации, обрабатываемой как внутри корпоративной сети, так и на МУ.

Среди исследований вопросов управления доступом, оценки защищенности, в том числе связанных с использованием МУ, известны работы М.Б. Гузаирова, И.В. Машкиной, А.Ю. Бабикова, В.А. Десницкого, Д.О. Карпеева, И.С. Ястребова и др.

Одним из вариантов решения проблем безопасности информации является постоянный мониторинг состояния МУ, а также ряда параметров окружения как устройства, так и пользователя, позволяющий управлять функциональным состоянием МУ таким образом, чтобы обеспечивать необходимый уровень безопасности информации при изменении параметров окружения МУ и его пользователя.

Наглядной интерпретацией реализации функций мониторинга состояния МУ, параметров окружения устройства и пользователя, управления профилем защиты МУ и реализации с помощью этого адаптивного управления политикой безопасности корпоративной сети является схема, представленная на рис. 1.

Рис. 1. Схема управления профилем защиты мобильного устройства при реализации правил политики безопасности корпоративной сети

Обобщенное изложение алгоритма управления доступом к услугам корпоративной сети пользователей МУ может выглядеть следующим образом:

1. Пользователь запрашивает доступ к определенным услугам корпоративной сети, при этом в запросе МУ передает по защищенному каналу на шлюз текущий контекст доступа, который содержит перечень запрошенных услуг корпоративной сети и параметры контекста доступа, характеризующие условия, в которых пользователь запрашивает доступ.

2. На шлюзе проводится оценка с точки зрения защищенности параметров контекста доступа, на основе которого формируется профиль защиты МУ. Профиль защиты МУ определяет настройки МУ, а также привилегии и права пользователя, которые обеспечивают заданный уровень защищенности. Данный уровень защищенности определяется требованиями политики безопасности и ассоциируется с некоторым информационным доменом, которому принадлежит контекст доступа, в условиях которого пользователь запрашивает доступ к услугам.

3. Шлюз высылает по защищенному каналу мобильному устройству новый профиль защиты, после чего предоставляется доступ к запрошенным услугам.

Из данного обобщенного изложения алгоритма управления доступа пользователей МУ к услугам корпоративной сети видно, что управление доступом осуществляется за счет учета контекста доступа и требуемого уровня защищенности, ассоциированного с данным контекстом доступа, и выражается в адаптивном назначении МУ профиля защиты. Профиль защиты МУ обеспечивает заданный уровень защищенности путем гарантированного отключения критичных, с точки зрения безопасности функциональных блоков МУ и назначения заданных политикой безопасности привилегий и цифровых прав пользователю.

ЛИТЕРАТУРА

1. Российский рынок мобильной коммерции 2012: Отчет Департамента консалтинга «РосБизнесКонсалтинг». М., 2012. 91 с.

2. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. Введ. 2006.12.27. М.: Федеральное агентство по техническому регулированию и метрологии, 2007. 8 с. (Национальный стандарт Российской Федерации).

3. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введ. 2006.12.27. М.: Федеральное агентство по техническому регулированию и метрологии, 2007. 8 с. (Национальный стандарт Российской Федерации).

КОМПЛЕКС ПРОГРАММ АЛГОРИТМОВ ШИФРОВАНИЯ

Ю.А. Мажников, студент каф. АСУ
Научный руководитель А.Н. Горитов, профессор каф. АСУ, д.т.н.
г. Томск, ТУСУР, yuramazh@mail.ru

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности, а также невозможности отказа от авторства) информации. Это одна из старейших наук.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого текста на основе секретного алгоритма или ключа в шифрованный текст.

Целью данной работы является проектирование и реализация программного комплекса, решающего задачи конкретной предметной области (криптографии).

Данный программный комплекс создается для того, чтобы наглядно представить работу некоторых алгоритмов шифрования для пользователя, который будет использовать эту систему. Программа предназначена исключительно в ознакомительных целях работы алгоритмов шифрования. Примеры алгоритмов, которые будут в системе: Mars, TwoFish, Serpent, RC6 и множество простых алгоритмов шифрования, такие как: Шифры перестановки, Магический квадрат, TEA, Книжный шифр, Шифр Виженера, Шифр Гронсфельда и др.

Для реализации этого программного комплекса были выбраны среда разработки Qt Creator и язык программирования C++.

Программный комплекс – набор технических и программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

Основным направлением назначения данной системы, помимо криптопреобразования текста, является графическое отображение порядка шифрования текста для того, чтобы более наглядно показать работу алгоритмов.

Рассмотрим, как программа выглядит на данном этапе разработки, на примере алгоритма MARS:

Главное окно приложения, где доступно на выбор несколько алгоритмов шифрования, которые разделены на разделы – сложные и простые (рис. 1).

Окно алгоритма MARS тоже разделено на 2 части: 1-я часть – это иллюстрация работы алгоритма, где представлена схема (рис. 2), а 2-я часть – это поля, где можно видеть зашифрованные и расшифрованные тексты (рис. 3).

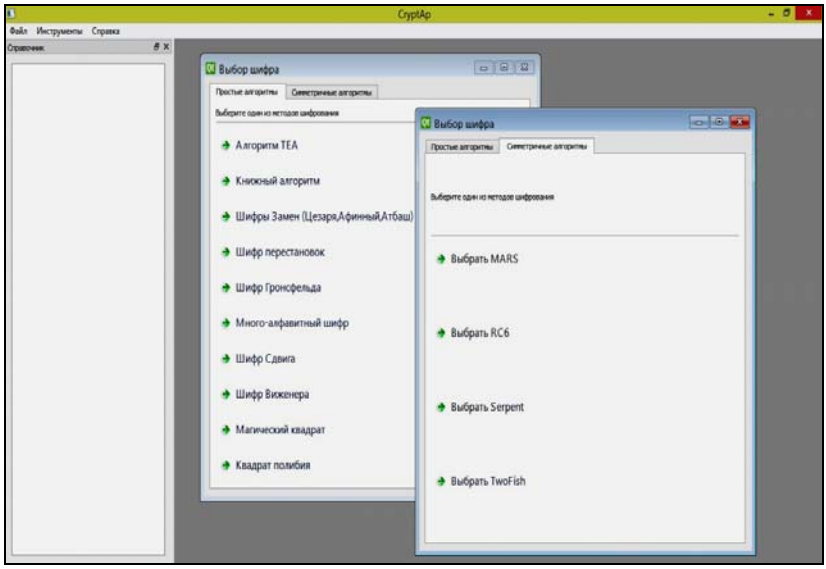


Рис. 1. Главное окно

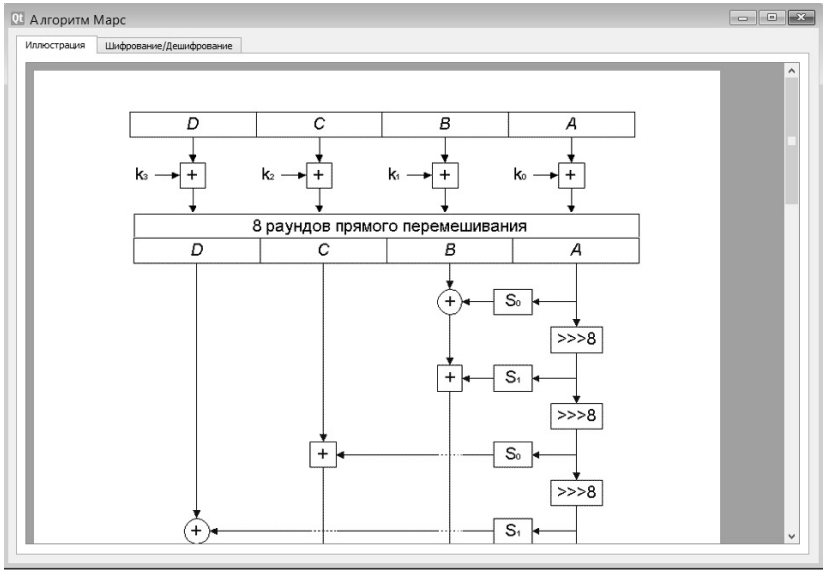


Рис. 2. Алгоритм MARS-иллюстрация

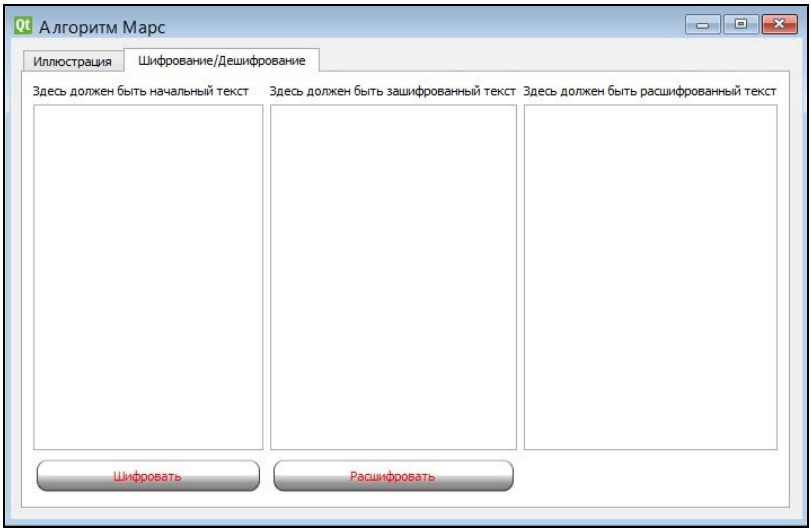


Рис. 3. Алгоритм MARS-шифрование/дешифрование

Заключение. В ходе работы было реализовано некоторое количество алгоритмов, которые уже можно использовать в качестве ознакомления с их работой, и, по моему мнению, данная программа должна позволит лучше изучить наиболее известные алгоритмы шифрования.

Для дальнейшего развития необходимо реализовать работу других алгоритмов шифрования, но кроме самих алгоритмов необходимо добавить еще и подробную справку по работе с программой, и краткую теорию о каждом алгоритме шифрования.

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ СБОРА И АНАЛИЗА ИНФОРМАЦИИ ИЗ ЖУРНАЛЬНЫХ ФАЙЛОВ ОПЕРАЦИОННЫХ СИСТЕМ И ПРИЛОЖЕНИЙ

А.В. Моргуненко, Д.С. Никифоров, И.Ю. Поляков, А.К. Пономарев, студенты каф. КИБЭВС

Научный руководитель А.И. Гуляев, аспирант каф. КИБЭВС

г. Томск, ТУСУР, gai@keva.tusur.ru

Проект ГПО КИБЭВС-1208 – «Компьютерная экспертиза»

В современном мире очень часто преступления совершаются при помощи компьютера. Для того чтобы доказать использование определенного компьютера при совершении преступления или найти следы преступления на атакованном компьютере, проводятся компьютерно-технические экспертизы.

Компьютерно-техническая экспертиза – это вид криминалистической экспертизы, направленной на поиск следов, оставленных на ЭВМ, с целью доказательства причастности исследуемого устройства к совершению преступления [1].

Одним из главных источников информации для эксперта служат журнальные файлы операционной системы и приложений. Для получения доступа к этой информации используются различные приложения. Недостатком таких приложений является их узкая направленность, из-за чего необходимо большое количество приложений.

Конечно, существуют инструменты (такие, как DEFT Linux), которые объединяют в себе множество приложений, но не всегда в подобных инструментах есть все необходимое, а также каждое приложение отображает информацию в определенном формате, который может резко отличаться от того формата, в котором отображают информацию остальные приложения. Это приводит к тому, что задача обобщения информации становится сложной и времязатратной.

Поэтому одна из задач, которые необходимо автоматизировать, – это задача приведения информации к единому виду (обобщение информации).

После обобщения необходимо проанализировать найденную информацию. Под анализом может пониматься как построение временных диаграмм или поиск по ключевым словам, так и обобщение данных из различных источников с целью выявления какой-либо конкретной активности. Что и является ещё одной задачей, которую возможно автоматизировать.

Идея данного проекта состоит в разработке программного комплекса, который может исследовать жесткие диски и собирать из них информацию, хранящуюся в журнальных файлах, приводить её к определенному виду и проводить её анализ.

Из всего вышеизложенного можно выделить задачи, которые будет решать разрабатываемый комплекс:

1) сбор информации;

2) преобразование информации в метаформат (к единому виду);

3) поверхностный анализ собранной информации, который включает в себя построение временных диаграмм событий;

4) вывод полученных результатов в виде, удобном для восприятия человеком.

Сам же комплекс будет обладать рядом особенностей, которые будут способствовать наиболее эффективной работе и легкой доработке данного комплекса. Под доработкой понимается добавление в комплекс новых функций, отладка и модернизация существующих функций.

Для достижения необходимого результата было принято решение разработать комплекс на основе шаблона factory [2], благодаря которому комплекс представляет собой «каркас», к которому можно легко подключить все необходимые модули (наборы инструкций для решения определенной задачи), сам же каркас отвечает только за доступ к жесткому диску, который он передает каждому модулю. Все модули независимы и никак не влияют на работу друг друга.

Итого комплекс обладает рядом следующих особенностей:

1) функционирует на базе операционных систем Linux;

2) модульная структура;

3) хранение собранных данных в формате XML.

На данный момент реализованы каркас программного комплекса, который можно легко расширять при помощи модулей, несколько модулей по работе с операционными системами семейства Windows и месенджеров.

В планах на будущее: расширение списка имеющихся модулей, реализация возможности генерации отчетов о происходящих на исследуемом компьютере событиях и добавление поддержки MAC OS. Также планируется проведение тестирования программного комплекса на компьютерах с различной конфигурацией.

Данный программный комплекс позволит экспертам намного эффективнее проводить компьютерно-техническую экспертизу за счёт автоматизации работы и уменьшения времени, затраченного на проведение экспертизы.

ЛИТЕРАТУРА

1. Федотов, Н.Н. Форензика. Компьютерная криминалистика / Н.Н. Федотов. 2-е изд. М.: onebook.ru, 2012. 420 с.

2. Фаулер М. Шаблоны корпоративных приложений (Signature Series) / М. Фаулер, Д. Райс, М. Фоммел, Э. Хайет, Р. Ми, Р. Стаффорд. М.: Вильямс, 2013. 544 с.

КИБЕРТЕРРОРИЗМ И МИРОВОЕ СООБЩЕСТВО

Ю.Ю. Наумская, студентка

Научный руководитель О.Н. Мызников, доцент каф. КТИБ, к.т.н.

г. Краснодар, КубГТУ, iitib_krasnodar@mail.ru

Современное сообщество напрямую связано с использованием информационно-коммуникационных и компьютерных технологий, и ежедневно в мире фиксируется множество попыток несанкционированного воздействия и доступа к банковским, военным и прочим компьютерным системам, то есть совершаются компьютерные преступления [1].

На основе компьютерных преступлений формируется кибертерроризм, определение которого можно сформулировать так: комплекс преднамеренных мер, направленных на информацию, обрабатываемую компьютером и компьютерными системами, представляющий собой опасность для жизни и здоровья людей, с целью нарушения общественной безопасности.

Понятия «киберпреступность» и «кибертерроризм» в каждой стране трактуются по-своему, не имея единого определения. Также они не имеют определенной, разделяющей их грани, но для осуществления каждого необходимо использование компьютерных технологий. Ущерб от данных видов преступности может иметь как высокую государственную опасность (выведение из строя систем управления промышленных предприятий), так и не столь важную (электронные хищения, хищения денежных средств при помощи банковских карт).

Все ведущие мировые международные организации признают опасность киберпреступности, ее трансграничный характер и ограниченность подхода к решению этой проблемы. Признается также необходимость международного сотрудничества в выработке международного законодательства и принятии необходимых технических мер. Важную роль в борьбе с киберпреступностью и кибертерроризмом играют такие организации, как ОЭСР, Совет Европы, Европейский союз, ООН. Деятельность этих организаций направлена на разработку политики и стратегии в области обеспечения кибербезопасности, борьбу с киберпреступностью и противодействие угрозам кибертерроризма.

С 1985 по 1989 г. Специальный комитет экспертов Совета Европы по вопросам преступности, связанной с компьютерами, определил список правонарушений, рекомендованный странам-участницам ЕС, для разработки единой уголовной стратегии относительно компьютерных преступлений [2].

Кибербезопасность – одна из основных целей настоящего времени, которая требует постоянного совершенствования. Существует уже немало международных соглашений, норм, принципов, но они требуют еще некоторых доработок и прежде всего реализации.

Немаловажным фактором в борьбе с кибертерроризмом может стать оперативный обмен информацией, который обеспечит взаимовыгодный обмен между правительствами и между региональными организациями.

С развитием Интернета распространение информации стало гораздо проще, быстрее и не требует больших затрат, что и стали использовать террористы в своих целях: распространяется террористическая пропаганда, поощряющая радикализацию и вербовку; террористы

получают необходимую информацию; используется перевод денежных средств; связь между группами; подготовка и планирование терактов.

Так же, как террористы используют Интернет в своих целях, его можно использовать и против них: предпринимаются меры обеспечения безопасности киберпространства с целью предотвращения возможных негативных последствий. Но использование Интернета террористами может интерпретироваться как право на свободу высказывания, регулируемого соответствующими национальными законами, что весьма усложняет борьбу.

Одним из действенных способов привлечения к ответственности кибертеррористов является гармонизированная международная правовая система. Эта система позволяет не только привести законы к общему характеру, но и укрепить международное сотрудничество, так как необходимо регулярно пересматривать национальные правовые системы в соответствии с изменениями, чтобы учитывать быстрое развитие технологий.

В сентябре 2010 г. в Екатеринбурге на Второй Международной встрече высоких представителей, которые курируют вопросы безопасности, была представлена Конвенция об обеспечении международной информационной безопасности, разработанная Российской Федерацией. Предполагается, что эта концепция может послужить основой для выработки универсальной Конвенции под эгидой ООН [3].

Целью ее является противодействие используемых информационных и коммуникационных технологий для нарушения международного мира и безопасности, а также организация сотрудничества в сфере обеспечения международной информационной безопасности для поддержания мира и содействия международной экономической стабильности.

В итоге можно выделить основные причины, препятствующие созданию полноценной международной стратегии по борьбе с киберпреступностью и кибертерроризмом:

1) до сих пор не был разработан полный и единый международный список кибепреступлений, отсутствует гармоничный свод определений в данной сфере, законопроекты государств существенно отличаются;

2) непрерывное развитие киберпространства – территории совершаемых преступлений;

3) недостаток высококвалифицированных специалистов и экспертов, осведомленных в сфере кибербезопасности.

ЛИТЕРАТУРА

1. Справочник ООН по предотвращению и контролю преступности, связанной с компьютерами [Электронный ресурс]. Режим доступа: http://www.uncjin.org/Documents/congr10/10r.pdf

2. Конвенция Совета Европы о киберпреступности [Электронный ресурс]. Режим доступа: http://iam.duma.gov.ru/node/2/4601/16186

3. Конвенция об обеспечении международной информационной безопасности [Электронный ресурс]. Режим доступа: http://www.mid.ru/bdomp/nsosndoc.nsf/e2f289bea62097f9c325787a0034c255/542df9e13d28e06ec3257925003542c4!OpenDocument

ИССЛЕДОВАНИЕ МЕТОДА ВОССТАНОВЛЕНИЯ ПРООБРАЗА ПО ЗНАЧЕНИЮ ЕГО ХЭШ-СУММЫ НА ОСНОВЕ ВЛИЯНИЯ БИТ ВХОДНОГО ЗНАЧЕНИЯ НА ВЫХОДНОЕ

Д.С. Никифоров, студент каф. КИБЭВС

Научный руководитель Е.А. Сопов, аспирант каф. КИБЭВС

г. Томск, ТУСУР, nds@keva.tusur.ru

На сегодняшний день криптографические хэш-функции широко применяются для решения различных задач. Данные функции используются при реализации контроля целостности данных или построения парольных систем защиты.

Хэш-функции представляют собой математические функции, которые получают на вход бинарные данные любой длины (прообраз) и преобразуют их в бинарные данные фиксированной длины (значением хэш-суммы, хэшем) [1]. Длина выходных данных зависит от алгоритма хэш-функции. Криптографической хеш-функцией называется всякая хэш-функция, являющаяся криптостойкой, удовлетворяющая требованиям специфичных для криптографических приложений.

Криптографические хэш-функции должны обладать следующими свойствами [2]:

1. Защищенностью от восстановления прообразов: должно быть невозможно в вычислительном отношении найти сообщение (прообраз) с данным значением хэш-функции.
2. Защищенностью от коллизий: вычислительно или математически невозможно найти два разных прообраза с одним и тем же значением хэш-функции.
3. Защищенностью от вторых прообразов: по данному прообразу невозможно найти другой с тем же значением хэш-функции.

Из определения хэш-функции понятно, что ввиду неограниченности множества входных значений и ограниченности множества выходных значений неизбежно возникновение коллизий. Например: у нас есть подсистема аутентификации пользователя по паролю, стандартная реализация базы учетных записей – это таблица, где хранятся пары [{идентификатор пользователя, хэш от пароля}] (пример представлен в

таблице), хранение паролей в виде хэшей обусловлено тем, что если такая база данных попадет в руки к злоумышленнику, то тот в свою очередь не сможет попасть в систему, потому что получение прообразов – трудоемкая задача и требует большого количества времени, за это время пользователи смогут сменить пароль и база в руках злоумышленника потеряет свою актуальность. Но если хэш-функция имеет часто встречаемые коллизии (для md5 – каждые 2^{512}), то злоумышленнику нет необходимости знать значение прообраза для входа в систему достаточно получить прообраз, который будет давать тот же самый хэш, то есть найти коллизию.

Пример хранения паролей

Идентификатор	Хэш от пароля
ura	50f3fca4c6134bd001fdfe3159686be9
vasya	a127c4fdad3080541ec6acc0d8acd704
petr	2f0714f5365318775c8f50d720a307dc

Первое требование для криптографической хэш-функции из списка, приведенного выше, гласит о невозможности восстановления прообраза, но на практике добиться этого возможно, так как всегда есть возможность полного-перебора, что заставляет нас переформулировать требование: задача восстановления прообраза по известному значению хэша должна быть вычислительно сложной настолько, чтобы время решения такой задачи было очень велико.

На сегодняшний день существует множество способов позволяющих получить прообраз по значению хэш-функции; правда, данные методы либо не дают стопроцентного результата, либо работают недопустимо долгое время. Данные методы сводятся либо к методу грубой силы (brut force), либо генерации таблиц соответствий, по которым для значения хэш-функции определяются прообразы. Данные методы требуют высоких вычислительных мощностей и объемов памяти и в обоих случаях – времени.

Изучая способы атак на хэш-функции, возникла идея использовать для нахождения прообразов вероятностные алгоритмы.

Идея состоит в том, чтобы создать систему, которая может изучать алгоритм подсчета хэш-функции, и на основе этих знаний подбирать прообраз для конкретного значения хэш-функции с некоторой вероятностью.

Целью работы является выявление и изучение возможных зависимостей и использования их для построения алгоритма, который на основе выявленных зависимостей подбирает прообраз для заданной хэш-суммы. В качестве первого исследуемого алгоритма подсчета

хэш-сумм выбрана функция md5, а также она является типичным представителем итеративных хэш-функций [3].

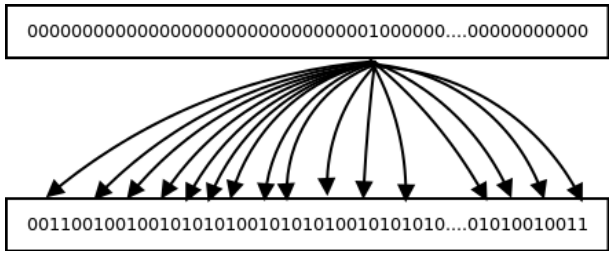


Рис. 1. Пример влияния входного бита на хэш-сумму

Для начала исследования проводятся на видоизменённом алгоритме md5, из которого убран шаг дополнения данных. Данный алгоритм принимает на вход 64 байта данных и производит расчёт хэш-суммы по алгоритму, после чего возвращает результат. Первая задача – это выявить, на какие биты выходного значения влияет каждый входной бит, и на основе выявленных зависимостей построить алгоритм, который выявлял бы, какие биты входных данных необходимо изменить для того, чтобы текущее значение хэш-суммы стало близже по Хэммингу к заданному и в конечном итоге совпало с ним. После чего сравнить эффективность работы данного алгоритма с имеющимися методами обращения хэш-функций.

Если разработанный алгоритм окажется эффективным, то будут проведены тесты с использованием других хэш-функций.

ЛИТЕРАТУРА

1. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходный код на языке С. 2 изд. М.: Триумф, 2002. 448 с.

2. Евсютин О.О. Криптографические методы защиты информации: электронное издание. М., 2000. 66 с.

3. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004. 173 с.

ОЦЕНКА КАЧЕСТВА ЗАЩИЩЕННОСТИ СЕТЕЙ

А.К. Новохрестов, студент каф. КИБЭВС

Научный руководитель А.А. Конев, доцент каф. КИБЭВС

г. Томск, ТУСУР, AlexBigGluk@gmail.com

В настоящее время большинство организаций при обработке и передаче информации используют компьютерные сети. В связи с этим одной из важнейших задач становится обеспечение безопасности се-

тей. На рынке систем защиты существует множество продуктов в разных ценовых категориях, сертифицированных и нет, однако сколько бы ресурсов организации не вкладывали в обеспечение безопасности, инциденты продолжают случаться, поскольку ни одно средство не может обеспечить стопроцентной защиты.

Возникает проблема оценки качества существующих систем защиты, однако инструменты для объективной оценки отсутствуют. В итоге результаты оценки качества защищенности сетей в большей степени зависят от субъективного мнения эксперта, а не от используемых им вспомогательных инструментов.

В качестве примера таких инструментов можно привести системы: «ГРИФ», разработанный компанией «Digital Security», и Microsoft Security Assessment Tool.

«ГРИФ» предоставляет возможность проводить анализ рисков информационной системы двумя способами:

– с помощью модели информационных потоков;
– с помощью модели угроз и уязвимостей.

Выбор между двумя методами осуществляется в зависимости от того, какими исходными данными располагает пользователь, а также от того, какие данные интересуют пользователя на выходе. Так как входные данные задаются пользователем вручную, то вероятность неверной оценки зависит в большой степени от того, учел ли эксперт при построении модели все существующие в системе элементы.

Программное средство Microsoft предлагает оценку рисков путем ответов на вопросы. Процесс разбит на два этапа, вопросы первого этапа направлены на построение информационной системы, второй этап оценки включает в себя четыре раздела: инфраструктуру, приложения, операции, персонал. После ответов на все вопросы сформируется отчет, по которому эксперт может судить о состоянии безопасности в организации. Вся методика оценки заключается в ответе на вопросы, которые не всегда могут быть корректны по отношению к структуре информационной системы организации, что увеличивает вероятность неверной оценки экспертом системы при ответе на вопросы.

Для объективной оценки качества защищенности сетей необходимо разработать методику, которая исключает влияние субъективного мнения на итоговую оценку. Для этого необходимо построить модель системы, которая может быть применима к любой современной сети обработки информации. Также необходимо выделить из множества существующих классификаций угрозы, которые относятся непосредственно к сетям, и поставить в соответствие каждой угрозе применяемые механизмы защиты.

Сейчас в качестве модели системы решено использовать схему документооборота, представленную на рис. 1.

Рис. 1. Модель документооборота

Виртуальный канал передачи информации – передача информации между устройствами компьютера, программами, драйверами, по сети, работа с содержимым носителя информации.

Для каждого документопотока выделяются типовые угрозы, в соответствие которым ставятся механизмы защиты. Таким образом, в упрощенном виде применение методики включает в себя следующие этапы:

1) определение структуры системы и актуальных для нее угроз;

2) определение наличия механизмов защиты для каждой угрозы;

3) составление отчета по «закрытым» угрозам и угрозам, для которых механизмы защиты отсутствуют.

В настоящее время ведется проработка классификации угроз, которая соответствовала бы существующим стандартам и при этом могла быть применена для классификации механизмов защиты. Также требуется проработка модели системы, для того чтобы методика была легче применима на практике, т.е. при рассмотрении инфраструктуры реальных сетей.

Такая методика в случае успешной реализации может быть положена в основу программного средства для автоматической оценки защищенности сетей.

ИССЛЕДОВАНИЕ ПРИЗНАКОВ РЕЧИ, ИСПОЛЬЗУЕМЫХ В ЗАДАЧЕ АВТОМАТИЧЕСКОЙ ИДЕНТИФИКАЦИИ ДИКТОРА ПО ГОЛОСУ

И.А. Рахманенко, аспирант каф. КИБЭВС

Научный руководитель Р.В. Мещеряков, профессор каф. КИБЭВС, д.т.н.

г. Томск, ТУСУР, ria@keva.tusur.ru

Вопрос развития речевых технологий, включая проблему голосовой идентификации, стоит уже не один десяток лет в научном сообществе. Основная трудность, с которой сталкиваются ученые, состоит в том, что на данный момент не существует универсальных методов, позволяющих проводить идентификацию диктора по голосу с полной уверенностью в ее корректности в любых акустических условиях.

Существуют модели, работающие эффективно в «лабораторных» условиях, но теряющие эффективность при низком соотношении сигнал–шум. С распространением биометрических систем многофакторной аутентификации, с применением голосовой аутентификации, банковских систем, использующих голосовую аутентификацию для подтверждения личности говорящего и предоставления доступа к личным данным, повышаются требования к точности идентификации. В настоящее время точность автоматических, текстонезависимых систем голосовой аутентификации составляет порядка 90–95% [1]. Такая точность является недостаточной для современных систем голосовой идентификации, так как в случае наличия большого числа пользователей, работающих с системой, будут неизбежны ошибки.

Выбор признаков, используемых для голосовой идентификации, является ключевым моментом при создании таких систем. Влияние признаков, оказываемое на точность системы, нельзя недооценивать, так как ими должна оцениваться индивидуальность голоса. Таким образом, была поставлена задача выявления эффективных характеристик, позволяющих повысить точность системы голосовой идентификации.

Индивидуальность акустических характеристик голоса определяется тремя факторами: механикой колебаний голосовых складок, анатомией речевого тракта и системой управления артикуляцией [1].

Для вычисления характеристик голоса используют спектр речи. Несмотря на то, что в спектре речи нет характеристик, четко позволяющих различать дикторов, было показано, что его можно эффективно использовать при решении задач идентификации по голосу [2]. Это происходит благодаря тому, что спектр отражает структуру речевого тракта человека, которая является основным физиологическим фактором, позволяющим различать голоса.

В [3] сообщается, что наиболее важный фактор индивидуальности голоса – это частота основного тона F_0, за ней следуют формантные частоты, размер флюктуаций F_0 и наклон спектра. В [4] высказывается мнение, что признаки, связанные с F_0, обеспечивают наилучшую разделимость голосов, а за ними следуют энергия сигнала и длительность сегментов. В основном, частота основного тона и связанные с ней характеристики используются при проведении криминалистических экспертиз. Однако при оценке частоты основного тона появляются трудности, такие как низкая точность оценки, ошибки, связанные с грубыми промахами (например, удвоение частоты основного тона), неустойчивость алгоритма оценки к шумам.

В другой работе наиболее важным фактором считаются формантные частоты [5]. В частности, четвертая форманта практически не за-

висит от типа фонемы и характеризует тракт [6]. Механика артикуляции такова, что в области высоких частот на сужение в речевом тракте приходятся как пучность, так и узел соответствующих собственных функций акустических колебаний, и это не позволяет управлять частотами высших резонансов. Известен метод извлечения формант при помощи дискретного вейвлет-преобразования с логарифмированием спектральной плотности мощности [7].

Также в качестве признаков могут использоваться векторы кепстральных коэффициентов: линейно-частотных кепстральных коэффициентов (LFCC, Linear-Frequency Cepstral Coefficients) или мэл-частотных кепстральных коэффициентов (MFCC, Mel-Frequency Cepstral Coefficients), получаемых по спектру Фурье; коэффициентов линейного предсказания (LPCC, Linear Prediction Cepstral Coefficients); коэффициентов перцептивного линейного предсказания (PLP, Perceptual Linear Prediction) [8]. Достоинством кепстральных коэффициентов является простота их вычисления, благодаря чему их можно вычислять в реальном времени.

Одним из перспективных направлений, позволяющих увеличить точность идентификации диктора по голосу, является применение супер-векторов признаков, являющихся комбинацией различных голосовых признаков [8, 9]. В дальнейшем, планируется проведение эксперимента по голосовой идентификации с использованием различных супер-векторов признаков с целью определения эффективного вектора с наибольшей точностью идентификации.

ЛИТЕРАТУРА

1. Сорокин В.Н., Вьюгин В.В., Тананыкин А.А. Распознавание личности по голосу: аналитический обзор // Информационные процессы. 2012. Т. 12, №1. С. 1–30.

2. Atal B. Automatic recognition of speakers from their voices // Proc. IEEE 1976. Vol. 64. P. 460–475.

3. Matsumoto H., Hiki S., Sone T., Nimura T. Multidimensional representation of personal quality of vowels and its acoustical correlates // IEEE Trans. AU. 1973. Vol. AU-21. P. 428–436.

4. Shriberg E., Ferrer L., Kajarekar S., Venkataraman A. Stolcke A. Modeling prosodic feature sequences for speaker recognition // Speech Communication. 2005. Vol. 46, № 3–4. P. 455–472.

5. Lavner Y., Gath I., Rosenhouse J. The effects of acoustic modifications on the identification of familiar voices speaking isolated vowels // Speech Communication. 2000. Vol. 30. P. 9–26.

6. Takemoto H., Adachi S., Kitamura T., Mokhtari P., Honda K. Acoustic roles of the laryngeal cavity in vocal tract resonance // Journal Acoustic Society of America. 2006. Vol. 120. P. 2228–2239.

7. Daqrouq K., Khalaf E., Al-Qawasmi A., Abu Hilal T. Wavelet formants speaker identification based system via neural network // Interational Journal of Recent Trends in Engineering. 2009. Vol. 2, № 5. P. 140–144.

8. Матвеев Ю.Н. Исследование информативности признаков речи для систем автоматической идентификации дикторов // Известия вузов. Приборостроение. 2013. Т. 56, №2. С. 47–51.

9. Первушин Е.А. Система идентификации дикторов на основе объединения признаков, векторного квантования и нормализации расстояния // Фундаментальные исследования. 2011. № 12. С. 151–154.

КЛЮЧЕВОЙ НОСИТЕЛЬ ЭЛЕКТРОННОЙ ПОДПИСИ КАК НОВЫЙ ПОДХОД К БЕЗОПАСНОСТИ

Д.С. Ризванов, студент каф. КИБЭВС

Научный руководитель Н.С. Михайлов, м.н.с.

г. Томск, ТУСУР, dinar-sama@yandex.ru

Проект ГПО КИБЭВС 1213 – «Криптоменеджер»

С развитием информационных технологий электронная подпись (ЭП) стала привычным атрибутом нашей жизни. ЭП позволяет придать электронному документу юридическую силу, равную юридической силе собственноручно подписанного и скреплённого печатью бумажного документа.

Как для собственноручной подписи нужна авторучка, так и для ЭП необходим соответствующий инструментарий. Изначально в роли средства ЭП выступали обычные компьютеры, на которых выполнялись соответствующие программы. Однако это неудобно и очень небезопасно – компьютер может быть заражен вирусом, способным похищать пароли, ключи шифрования или выполнить транзакцию без вашего ведения. К тому же доступ к компьютеру могут иметь посторонние лица. Одной из мер защиты ЭП от киберпреступников являются аппаратные ключи защиты – токены, которые бывают двух видов: с извлекаемым и неизвлекаемым закрытым ключом. Они являются ярким примером двухфакторной аутентификации: Pin-код и токен. Не зная пароля, никто не воспользуется ключом. Pin-код же становиться простым набором цифр, если нет токена, к которому он принадлежит. В наше время наиболее широкое распространение получили ключи, выполненные в виде USB-брелоков и смарт-карт. Эти защищенные аппаратно-программные устройства предназначены для использования в инфраструктуре открытых ключей, платежных системах, системах доступа, в сетевой безопасности, в качестве электронного идентификатора, носителя ключевой информации, а также средства формирования электронной цифровой подписи. Их разработкой и продвижением в

России занимаются такие компании, как «Мультисофт», «Актив», «Аладдин».

Большинство токенов выполнены на базе нового поколения электронных ключей с использованием языка Java, они имеют открытую архитектуру и возможность добавления требуемой функциональности путем загрузки в ключ Java-апплета (например, реализующего функции «электронного кошелька» и пр.).

Взаимодействие компьютера с USB-брелоком производится с помощью штатного CCID-драйвера, входящего в состав современных ОС. Благодаря этому обеспечивается возможность работы без установки дополнительных драйверов и ПО на разных платформах (Windows, Mac OS X, Linux).

Технологическая платформа JaCarta ГОСТ компании «Аладдин» позволяет использовать ЭП в самых разных информационных системах. Благодаря одному электронному ключу пользователь имеет возможность безопасно работать с электронным документооборотом, платёжными системами, аутентифицироваться в облачных сервисах, участвовать в электронных торгах и др. Пользоваться электронным ключом можно не только со стационарного компьютера или ноутбука, но и со смартфона или планшета, который всегда под рукой.

Линейка продуктов JaCarta ГОСТ предназначена для обеспечения юридической значимости действий пользователей при использовании различных электронных сервисов:

- дистанционное банковское обслуживание (ДБО);
- электронные торговые площадки;
- сдача электронной отчётности;
- электронное декларирование грузов, перемещаемых через границу;
- публичные или корпоративные Web-порталы и облачные сервисы, например портал гос. услуг;
- системы корпоративного/ведомственного электронного документооборота (СЭД).

Токены позволяют решать задачи:

- строгая взаимная двухфакторная аутентификация пользователей Web-порталов и облачных сервисов (с использованием ЭП);
- формирование электронной подписи для Web-форм и документов;
- генерация ключей, формирование и проверка электронной подписи с неизвлекаемым ключом ЭП при работе с криптопровайдерами КриптоПро CSP, VipNet CSP, Signal-COM CSP, Lissi CSP, JaCarta CSP;
- хранение ключевых контейнеров для программных СКЗИ КриптоПро CSP, VipNet CSP и др.;

• хранение пользовательских данных (пароли, коды доступа, настройки и пр.) в защищённой PIN-кодом памяти токена;

• использование в качестве отчуждаемого сертифицированного криптомодуля в составе других продуктов.

Можно заключить, что уже сейчас USB-ключи и смарт-карты являются неотъемлемой частью инфраструктуры информационной безопасности. Они поддерживаются всеми ведущими производителями информационных систем и бизнес-приложений, соответствуют требованиям российских регулирующих органов. В дальнейшем доля носителей с неизвлекаемым закрытым ключом будет только расти.

ЛИТЕРАТУРА

1. Скляров Д.В. Искусство защиты и взлома информации. М.: Изд. дом «Питер», 2004. 288 с.

2. Сигнал-КОМ – криптографическая защита информации. USB-ключи eToken компании «Аладдин» [Электронный ресурс]. URL: http://www.signal-com.ru/products/usb/etoken (дата посещения: 03. 03. 2013).

3. Аладдин-РД – JaCartaГОСТ. Технические характеристики продукта [Электронный ресурс]. URL: http://www. http://www.aladdin-rd.ru/catalog/jacarta/details (дата посещения: 03. 03. 2014).

ИМИТАЦИОННАЯ МОДЕЛЬ ДИНАМИЧЕСКОЙ ПЕРЕАВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЯ ЗА СЧЕТ УЧЕТА ПОВЕДЕНЧЕСКИХ ХАРАКТЕРИСТИК И ДАННЫХ О МЕСТОПОЛОЖЕНИИ

Л.К. Саморцев, А.А. Смыкалов, курсанты

Научный руководитель Д.О. Маркин, адъюнкт

г. Орел, Академия ФСО России, admin@nikitka.net

Бурное развитие сетей связи мобильных устройств (МУ), мобильного интернета, а также проникновение смартфонов и планшетов в России предъявляет повышенные требования к безопасности информации при использовании их в корпоративных сетях [1]. Преимущества использования МУ как многофункциональных мобильных абонентских терминалов очевидны, однако их свободное использование ограничено, поскольку создает условия для нарушения безопасности информации вследствие различных объективных и субъективных факторов как внутреннего, так и внешнего характера [3].

Поэтому одной из актуальных задач обеспечения достаточного уровня защищенности удаленного доступа к услугам корпоративной сети является создание новых способов защиты информации в корпоративных сетях при использовании МУ. Одной из принципиальных

особенностей эксплуатации мобильных устройств является постоянное перемещение их в пространстве, а также высокая вероятность утраты МУ из-за их миниатюрности. Исходя из этого, одним из наиболее эффективных способов защиты информации при эксплуатации МУ может быть создание нового механизма управления доступом на основе динамической переавторизации пользователя МУ за счет учета данных о местоположении, а также поведенческих характеристик пользователя.

Известны ряд исследований в рамках изучения вопросов управления доступом с учетом данных контекста доступа и информации о местоположении [3], а также с учетом модели поведения пользователя [4]

Очевидно, что закон изменения местоположения мобильного устройства и соответственно результаты динамической переавторизации непосредственно зависят от задач, выполняемых пользователем и его модели поведения. Исходя из этого, актуальной задачей имитационного моделирования является анализ существующих законов распределения на предмет выбора наиболее оптимального закона распределения и значений его параметров, что позволит наиболее точно и адекватно отразить особенности модели поведения и перемещения пользователей мобильных устройств.

Предлагаемая имитационно-аналитическая модель является системой оценки защищенности удаленного доступа к услугам корпоративной сети пользователя мобильного устройства на основе анализа контекста доступа пользователя мобильного устройства.

Алгоритм работы предлагаемой системы имитационного моделирования динамической переавторизации пользователя мобильного устройства на основе анализа контекста доступа представлен на рис. 1.

В качестве исходных данных модели даны: схема помещений; схема расписания пользователя; схема расположения датчиков местоположения различного радиуса действия и типов (RFID, Bluetooth, WiFi, GSM); псевдослучайные модели перемещения пользователей; группа перечней типичных действий, отражающих профиль поведения разных пользователей мобильных устройств; перечень действий, идентифицируемых как аномальные, для пользователей мобильных устройств; псевдослучайные модели поведения пользователя.

В качестве среды имитационно-аналитического моделирования выбран программный продукт AnyLogic Professional [5], позволяющий реализовать модель в виде автономного Java-приложения, использовать элементы и визуализации результатов моделирования, осуществлять статистическую обработку результатов и их графическую интерпретацию.

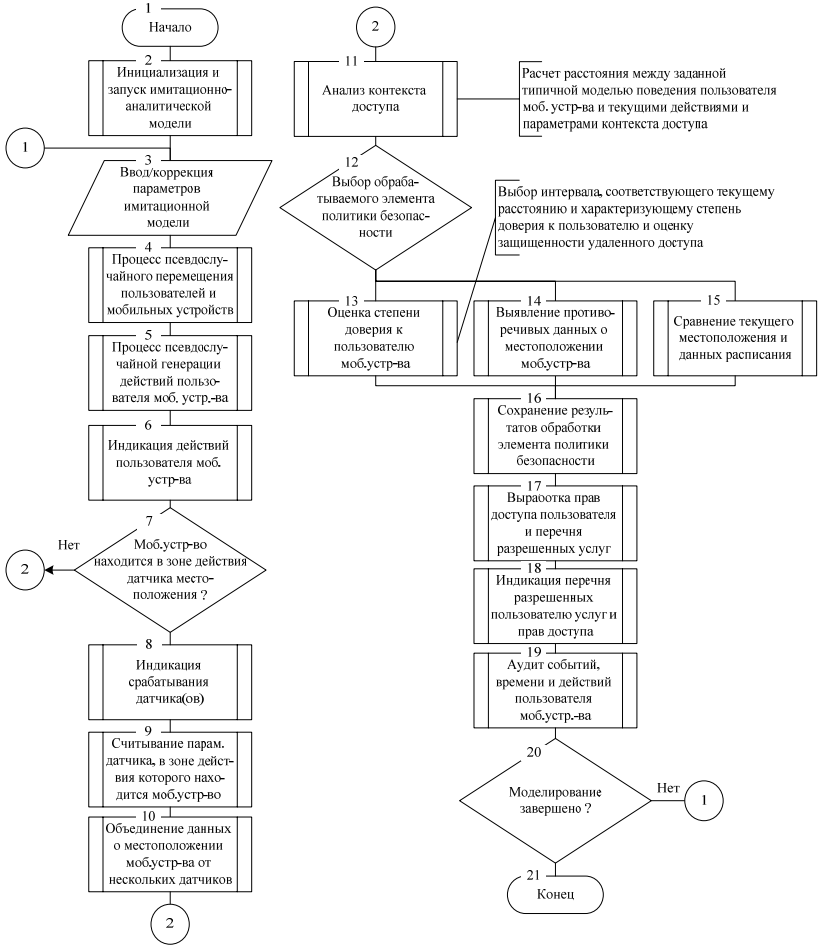


Рис. 1. Алгоритм имитационного моделирования динамической переавторизации пользователя мобильного устройства

Результатом имитационно-аналитического моделирования будут являться выявленные закономерности и зависимости динамически формируемой политики безопасности от изменяющихся параметров контекста доступа, которые после проверки предложенной модели на адекватность, точность и чувствительность можно будет использовать в создании практических приложений, реализующих методы управления доступом на основе аутентификации и динамической переавторизации в мобильных устройствах, с помощью которых осуществляется доступ к информационным ресурсам корпоративных сетей.

ЛИТЕРАТУРА

1. Российский рынок мобильной коммерции 2012 : Отчет Департамента консалтинга «РосБизнесКонсалтинг». М., 2012. 91 с.

2. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введ. 2006.12.27. М.: Федеральное агентство по техническому регулированию и метрологии, 2007. 8 с. (Национальный стандарт Российской Федерации).

3. Rocha C.C. A2BeST: An Adaptive Authentication Service Based on Mobile User`s Behavior Spatio-Temporal Context / C.C. Rocha, J.C.D. Lima, M.A.R. Dantas // IEEE Press. 2011. № 11. P. 771–774.

4. Shi E. Implicit Authentication through Learning User Behavior / E. Shi etc. Berlin : ISC, LNCS 6531. 2011. № 2010. P. 99–113.

5. Инструмент имитационного моделирования AnyLogic [Электронный ресурс]. The AnyLogic Company. СПб., 1991. Режим доступа: http://www.anylogic.ru/overview. (дата обращения: 11.12.2013).

ОБНАРУЖЕНИЕ УГРОЗЫ СЛАБОЙ ПАРОЛЬНОЙ ЗАЩИТЫ В КОРПОРАТИВНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

Р.В. Сёмин, магистр каф. информатики и вычислительного эксперимента ЮФУ

Научный руководитель В.Н. Брагилевский, ЮФУ,
соруководитель В.А. Новосядлый, к.ф.-м.н.,
ФГАНУ НИИ «Спецвузавтоматика»
г. Ростов-на-Дону, ЮФУ, rommero.semin@gmail.com

На настоящий момент угрозам информационной безопасности в компьютерных сетях уделяется большое внимание. Обеспечение информационной безопасности носит комплексный характер и содержит в себе как технические, так и организационные меры. По результатам «Trustwave 2013 Global Security Report» [1] наиболее часто несанкционированный доступ к информации получается удаленно, в том числе через SQL-инъекцию. Основная цель атак – данные кредитных карт и адреса электронной почты. Проведенный анализ паролей, полученных в результате тестов на проникновение, показывает, что слабые пароли, наподобие «Welcome1», «Password1», «Hello123», все еще часто используются. Аналогичные выводы делаются и в отчете Министерства внутренней безопасности США [2].

Таким образом, можно сделать вывод, что угрозы слабой парольной защиты являлись и до сих пор являются одними из наиболее часто упоминаемых и встречающихся в компьютерных сетях. Этой угрозе были подвержены такие известные компьютерные системы, как LinkedIn [3], Steam [4] и Hotmail, Yahoo, Gmail [5].

Надёжный канал, обеспечивающий конфиденциальность передаваемой информации, система авторизации, предотвращающая несанкционированный доступ, – всё это не позволяет обеспечить безопасность информации, если имеет место неграмотная политика паролей пользователей. Для уменьшения этой угрозы применяется периодический аудит безопасности. К сожалению, в большинстве случаев аудит ограничивается проверкой параметров парольной политики (требования к длине пароля, наличию в нём специальных символов и т.д.). Подобный аудит не обнаруживает угрозу слабой парольной защиты там, где парольная политика не действует или не может быть применена. Например, вычислительные средства, не входящие в домен, домашние ПК, коммутационное оборудование, пароли на шифрованные разделы и файлы и т.д.

Активный аудит парольной политики. Аудит требований парольной политики является частью пассивного аудита [6]. Сложность его проведения невысока и на данный момент разработано достаточно много комплексов пассивного аудита, как свободно распространяемых (Watcher, websecuritytool.codeplex.com; Open-AudIT, www.open-audit.org), так и коммерческих (Nipper Studio, www.titania.com/nipperstudio; The Tenable Passive Vulnerability Scanner, www.tenable.com/products/passive-vulnerability-scanner). Для того чтобы устранить отмеченный во введении недостаток пассивного аудита применяется так называемый «активный аудит», основной частью которого является Penetration Testing, или Испытание на проникновение [7].

Для выполнения активного аудита парольной защиты компьютерной системы выработан комплекс шагов:

1. Определение перечня проверяемых узлов компьютерной сети.
2. Определение перечня проверяемых сервисов.
3. Обнаружение доступных сервисов из списка на проверяемых узлах.
4. Активная проверка существования угрозы слабой парольной защиты на обнаруженном сервисе.

Отдельным вопросом является определение того, какую парольную защиту следует относить к слабым. В рамках данной работы будем считать защиту слабой, если нам удалось подобрать учётные данные для доступа к сервису с использованием словарей.

К средствам, позволяющим выполнять активный аудит парольной защиты, относятся такие программные компоненты, как nmap и ncrack (nmap.org), zmap (zmap.io), THC-hydra (www.thc.org/thc-hydra), Metasploit (www.metasploit.com), patator (code.google.com/p/patator), nessus (www.tenable.com/products/nessus).

Недостатком существующих на данный момент комплексов является их сложность использования, а также узкая направленность на решение конкретных задач, что не позволяет автоматически выполнять весь комплекс шагов, необходимых для активного аудита парольной защиты.

Заключение. Задача создания комплекса, способного проводить активный аудит и выявлять угрозу слабой парольной защиты в автоматическом режиме, является на данный момент весьма актуальной. Такая система позволит упростить процесс аудита, сделав его более наглядным и доступным для конечного пользователя.

ЛИТЕРАТУРА

1. Trustwave 2013 Global Security Report [Электронный ресурс]. 2013. URL: http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf (дата обращения: 01.03.2014).

2. Coburn T. The Federal Government's Track Record on Cybersecurity and Critical Infrastructure [Электронный ресурс] 2014. URL: http://www.hsgac.senate.gov/download/?id=8BC15BCD-4B90-4691-BDBA-C1F0584CA66A (дата обращения: 01.03.2014).

3. LinkedIn passwords leaked by hackers // BBC News Official site [Электронный ресурс]. 2012. URL: http://www.bbc.com/news/technology-18338956 (дата обращения: 01.03.2014).

4. BBC News – Valve's online game service Steam hit by hackers. // BBC News Official site [Электронный ресурс]. 2011. URL: http://www.bbc.co.uk/news/technology-15690187 (дата обращения: 01.03.2014).

5. Fildes J. Scam hits more e-mail accounts // BBC News Official site [Электронный ресурс]. 2009. URL: http://news.bbc.co.uk/2/hi/technology/8292299.stm (дата обращения: 01.03.2014).

6. Sayana S.A. Approach to Auditing Network Security // Information Systems Control Journal. 2003. Vol. 5.

7. Krutz R.L., Vines R.D. Penetration Testing. The CISSP® and CAPCM Prep Guide: Platinum Edition. John Wiley&Sons. 2006.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПРОВЕДЕНИЯ АНАЛИЗА И СРАВНЕНИЯ ТЕСТОВ НА ПРОСТОТУ ЧИСЛА

Ю.В. Шабля, студент каф. КИБЭВС

Научный руководитель Д.В. Кручинин, аспирант каф. КИБЭВС

г. Томск, ТУСУР, shablya-yv@mail.ru

В настоящее время применение простых чисел и их свойств имеет широкое применение в криптографических алгоритмах защиты информации. Многие криптографические алгоритмы используют простые числа, а некоторые даже полностью основаны именно на свойствах простых чисел, например RSA [1], криптографическая сложность

которого заключается в проблеме факторизации больших чисел, то есть разложении на простые множители.

Существует множество тестов проверки натурального числа на простоту, одни из которых выдают точный ответ о простоте исследуемого числа (детерминированные тесты), другие выдают сообщение о простоте числа лишь с определенной вероятностью (вероятностные тесты). Детерминированные тесты на простоту числа хоть и дают достоверный результат, но они значительно уступают вероятностным тестам по скорости работы, поэтому в реальных задачах с применением огромных чисел используются именно вероятностные тесты на простоту. Но в таком случае становится очень важным показатель вероятности ошибки теста на простоту, который показывает долю псевдопростых чисел среди определенных тестом простых чисел.

Различные тесты на простоту также используются и в математических пакетах, таких как Maxima, MathCAD, MathLab, Maple, Mathematica и др. В основном здесь используется вероятностный тест простоты числа Рабина–Миллера, который на практике показывает достаточно хорошую скорость работы и малую вероятность ошибки определения простоты числа.

В связи с таким широким использованием тестов на простоту до сих пор исследуется данная область, и создаются все новые тесты на простоту числа [2, 3]. Чтобы выбрать тест на простоту из всего этого множества тестов простоты, необходим инструмент, который бы позволил сравнить два различных теста. Таковым инструментом является разрабатываемое программное обеспечение по анализу тестов на простоту натуральных чисел.

Функционал программы позволяет сравнивать между собой два различных теста на простоту. Сравнение можно производить как для проверки заданного одного числа, так и для заданного интервала чисел. В ходе анализа теста выводится информация о количественных показателях данных тестов для исследуемого интервала натуральных чисел, таких как вероятность ошибки, время работы, количество простых чисел и так далее. По данным характеристикам приводится сравнение изучаемых тестов простоты. Также программа выдает сравнение двух выбранных тестов в графическом виде.

В программе предусматривается сравнение как уже существующих и использующихся тестов простоты числа (метод пробных делений, тест на основе малой теоремы Ферма, тест Рабина–Миллера и так далее), так и сравнение новых критериев простоты числа, полученных с помощью теории производящих функций [4].

Необходимо также наличие возможности анализа комбинированных тестов простоты числа, то есть состоящих из комбинации двух

тестов. Комбинированные тесты могут обладать совершенно новыми свойствами по сравнению с составляющими их единичными тестами простоты.

Реализация программного обеспечения с указанным функционалом позволит значительно облегчить процесс анализа тестов простоты числа за счет автоматизации данного процесса и представления итоговой информации в удобной форме. Стоит отметить и тот фактор, что аналогов в виде готового программного обеспечения не было обнаружено, поэтому разработка такого программного обеспечения характеризуется своей новизной и актуальностью.

ЛИТЕРАТУРА

1. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and publickey cryptosystems // Communications of the ACM. 1978. Vol. 21, №2. P. 120–126.

2. Agrawal M., Kayal N., Saxena N. Primes is in p // Annals of mathematics. 2004. P. 781–793.

3. Кручинин Д.В., Кручинин В.В. Метод построения алгоритмов проверки простоты натуральных чисел для защиты информации // Доклады ТУСУРа. 2011. №2(24). С. 247–251.

4. Шабля Ю.В., Кручинин Д.В. Критерии простоты числа на основе производящих функций // Электронные средства и системы управления: матер. докл. IX Междунар. науч.-практ. конф. Томск, 2013. С. 38–40.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ГЕОИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ АЭРОВИЗУАЛЬНОГО КОНТРОЛЯ ЗАЩИЩЕННОСТИ ЛИНЕЙНОЙ ЧАСТИ МАГИСТРАЛЬНОГО НЕФТЕПРОВОДА

К.А. Шинкаренко, студент каф. КИБЭВС

г. Томск, ТУСУР, shinkarenko.k@gmail.com

Деятельность компании ОАО «Центрсибнефтепровод» связана с транспортировкой нефти и решением целого комплекса задач, сопутствующих этому процессу. Одной из задач компании является обеспечение контроля защищенности нефтяных магистралей. Для этого периодически осуществляются облеты нефтепроводов с проведением фото- и видеосъемки, а также записывается gps-трек облета. Однако на данный момент в организации отсутствует специализированное программное обеспечение, позволяющее осуществлять обработку и хранение данных, полученных в результате облетов.

Исходя из этого, для обеспечения информационной поддержки процесса охраны линейной части магистрального нефтепровода Служ-

бой безопасности была поставлена задача: создание автоматизированной системы, обеспечивающей просмотр видеофайлов и фотоизображений, полученных в результате облета магистральных нефтепроводов, с привязкой к географическим координатам и отображением на карте. Так как все данные, получаемые в результате облета, являются коммерческой тайной, то к системе были выдвинуты дополнительные требования: необходимо организовать ролевое разграничение доступа к ресурсам автоматизированной системы, также система должна соответствовать требованиям класса защищенности АС от НСД 1Г.

На данный момент реализована подсистема, отвечающая за воспроизведение видео и отображающая на карте gps-трек с маркером, соответствующим текущему местоположению, изображенному на кадре видео. Данные облетов магистрального нефтепровода заносятся в базу данных, из которой впоследствии происходит выборка необходимой информации. В качестве провайдера карт был выбран Bing Maps от Microsoft, так как на этих картах лучше отображены участки земли, на которых располагается нефтепровод. Интерфейс программы показан на рис. 1.

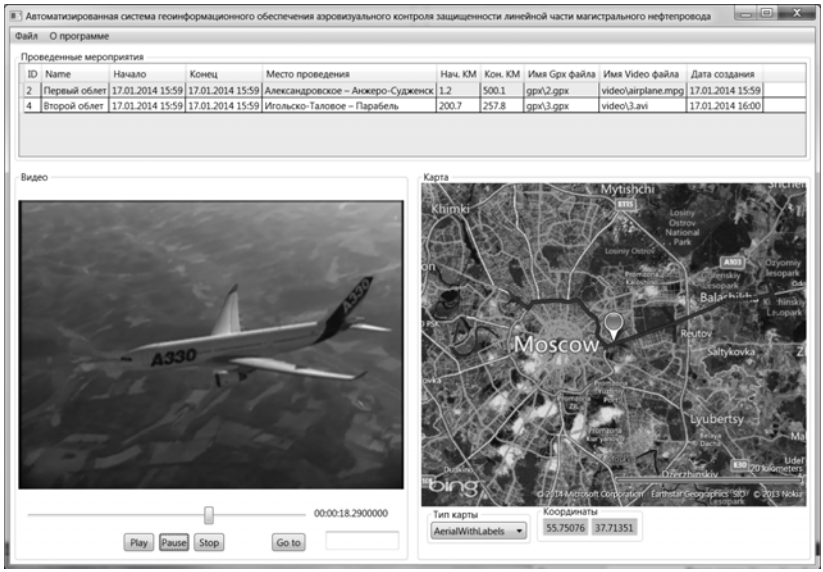


Рис. 1. Интерфейс программы

Окончательная реализация данной автоматизированной системы упростит хранение и обработку информации, способствующей обеспечению охраны линейной части магистрального нефтепровода.

ЛИТЕРАТУРА

1. ОАО «ЦЕНТРСИБНЕФТЕПРОВОД» [Электронный ресурс]. URL: http://csib.tomsk.ru/info/about2 (дата обращения: 2.03.2014).

2. Bing Maps [Электронный ресурс]. URL: http://msdn.microsoft.com/en-us/library/dd877180.aspx (дата обращения: 2.03.14).

АНАЛИЗ ПОДХОДОВ К ПОСТРОЕНИЮ МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.В. Штыгайло, студент каф. КИБЭВС

Научный руководитель А.А. Конев, доцент каф. КИБЭВС

г. Томск, ТУСУР, urbann91@gmail.com

К понятию защиты информации нужно подходить комплексно. Необходимо затронуть все возможные аспекты в области защиты информации. На этапе предпроектного исследования важно определить полный перечень угроз, так как при отсутствии какого-либо элемента вероятность реализации угрозы резко возрастает. Инструментом для формирования перечня угроз служит модель угроз.

Но проблема построения модели угроз является актуальной на сегодняшний день: не существует единого похода к построению модели угроз, отсутствие четких рамок функционирования модели угроз и так далее.

Обобщенно говоря, модель угроз можно представить в виде схемы «черного ящика», где есть входные и выходные данные (рис. 1). То есть на вход схемы подается некая характеристика системы, а на выходе получается готовый перечень угроз. Отсюда следует, что модель угроз должна содержать в себе и работать только с теми параметрами, от которых зависит результирующая угроза. Других параметров быть не должно. Это тривиальное представление данного подхода или абстрактная модель, назначение которой – обеспечить понимание, что же такое модель угроз в целом, и разграничить это понятие от остальных (например, модель нарушителя, оценка рисков и т.д.) для разгрузки модели и устранения избыточности.

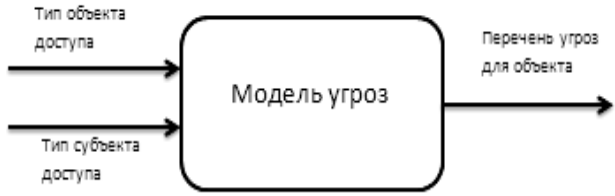


Рис. 1. Модель угроз

Имеется множество подходов, и каждый из них трактует модель угроз по-своему.

Для подтверждения вышесказанного были проанализированы несколько различных подходов, описанные в нормативных документах и в авторефератах кандидатских диссертаций.

1. В качестве первого варианта был рассмотрен документ ФСТЭК России. По данному документу модель угроз представляет следующую структуру:

1) полный перечень угроз;

2) общая характеристика информационной системы;

3) классы уязвимостей;

4) виды деструктивных воздействий на объект доступа;

5) способы реализации деструктивных воздействий.

Примечание. Пункты 3–5 не должны фигурировать при описании модели угроз. Данные параметры основываются на угрозе, а не наоборот, и, следовательно, они не являются входными параметрами, от которых зависят результирующие угрозы.

2. Исходя из материала автореферата О.В. Лукиновой, модель угроз имеет следующий вид:

1) класс уязвимостей;

2) класс нарушителя;

3) класс атак.

Примечание 1. Пункты 1 и 3 не должны использоваться при построении модели угроз, так как при формировании данных двух классов (уязвимостей, атак) базисом является сама угроза, которая в свою очередь – это конечный результат (выходной параметр) модели угроз. Другими словами, сначала выявляют угрозу, затем получают возможные уязвимости и атаки, а не наоборот.

Примечание 2. Пункт 2 описывает тип нарушителя. Данный пункт не должен фигурировать при описании модели угроз. Все, что касается нарушителей (источников угроз), относится к понятию «модель нарушителя».

3. Рекомендация в области стандартизации Банка России предоставляет следующий вид модели угроз:

1) источники угроз информационной безопасности;

2) методы реализации угроз ИБ;

3) объекты, пригодные для реализации угроз ИБ;

4) уязвимости, используемые источниками угроз ИБ;

5) типы возможных потерь;

6) масштабы потенциального ущерба.

Примечание 1. Пункт 1 представляет список источников угроз, в качестве которого выделяется тип нарушителя (внешний или внутрен-

ний). Но так как тип нарушителя характеризуется при построении модели нарушителя, следовательно, данный пункт не относится к модели угроз.

Примечание 2. Пункт 2 включает в себя описание механизмов воздействия, которые нарушитель использует для реализации какой-либо угрозы. То есть данный пункт относится к модели нарушителя.

Примечание 3. Пункт 3 применим к модели угроз, так как является входным параметром модели угроз.

Примечание 4. Пункты 4–6 не являются частью модели угроз. Данные параметры основываются на угрозе, а не наоборот, и, следовательно, они не являются входными параметрами, от которых зависят результирующие угрозы.

4. Автор В.С. Дунин в своей работе представил модель угроз в виде кортежа, состоящего из элементов: S, K, Бс, Бх, П, ИО [4].

Примечание 1: Субъект доступа (S) и информационный объект доступа (ИО) являются входными характеристиками модели угроз. Эти параметры нужны при формировании модели угроз.

Примечание 2. Оборудование в канале связи (K) не влияет на специфику самой угрозы, этот параметр не является входными данными в функции модели угроз. Например, при реализации угрозы как анализ сетевого трафика относительно различных устройств (коммутатор, маршрутизатор, сервер), суть самой угрозы как таковой не меняется. Следовательно, готовая угроза на выходе функции модели угроз никак не зависит от данного параметра на входе.

Примечание 3. Сервисы безопасности (Бс, Бх) не требуются в модели угроз, так как сама специфика угрозы не меняется в зависимости от инструмента защиты.

Проанализировав все источники, можно сделать вывод, что в основном присутствуют схожие недочеты. Установлено, что каждая из рассматриваемых моделей угроз содержит избыточность в виде присутствия модели нарушителя, то есть в модели угроз используются понятия «тип нарушителя», «механизм воздействия на объект» и т.д. – используются параметры модели нарушителя. Помимо этого, типичным недостатком является то, что в рамках последовательности анализа защищенности перечень угроз предшествует этапу выявления уязвимостей и атак, а не наоборот, что во многих подходах не учитывается. Также стоит отметить, что используются те параметры, от которых конечный перечень угроз не зависит. Тем самым появляется избыточность (перегруженность) модели, «стирается» граница между различными моделями (пример, модель: защиты, угрозы, нарушителя). Что усложняет работу эксперта с самой моделью и может отрицательно сказаться на конечном результате.

ЛИТЕРАТУРА

1. Нормативно-методический документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». 15.02.2008 г.

2. Лукинова О.В. Компьютерные модели и алгоритмы управления безопасностью информационных систем: автореф. дис. ... д-ра техн. наук / Институт проблем управления им. В.А. Трапезникова Российской академии наук. М., 2013.

3. РС БР ИББС-2.4-2010. Рекомендации в области стандартизации Банка России.

4. Дунин В.С. Модель угроз информационной безопасности комплексной автоматизированной интеллектуальной системы «Безопасный город»: автореф. дис. ... канд. техн. наук / Воронежский институт МВД России. Воронеж, 2012.

5. Балановская А.В. Модель угроз информационной безопасности промышленного предприятия // Вестник Самарского государственного экономического университета. 2011. № 9 (83).

СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЛАСТНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧЕРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ «РОДДОМ №1» г. ТОМСКА

Д.А. Сорокин, студент каф. КИБЭВС

Научный руководитель В.Г. Миронова, м.н.с. каф. КИБЭВС

г. Томск, ТУСУР, ФБ, densigosor@gmail.com

Защита персональных данных (ПДн) становится все более актуальной задачей в современном мире, особенно это заметно в медицинской сфере в связи с обязательным переходом лечебных учреждений на электронную обработку. Ведь нарушение конфиденциальности, недоступность или нарушение целостности ПДн может нанести гораздо больший вред, чем в случае остальных типов персональных данных.

Сейчас основными информационными системами персональных данных (ИСПДн) в медицинских учреждениях являются:

1) Медицинская информационная система БАРС (МИС БАРС), разрабатываемая компанией БАРС Груп. Предназначена для комплексной автоматизации информационных потоков лечебно-профилактических учреждений (ЛПУ). Хранит и обрабатывает следующие персональные данные:

– ФИО;
– дата рождения;
– место регистрации/проживания/работы;
– паспортные данные;

– данные о семье;
– данные о льготах;
– номер полиса обязательного медицинского обслуживания (ОМС);
– страховой номер индивидуального лицевого счёта;
– номера больничных карт;
– дата времени и результаты записи/посещения врача;
– сведения о госпитализации.

ИСПДн построена по типу «тонкого клиента». Все данные хранятся и обрабатываются на серверах, обслуживаемых ОАО «Ростелеком». Данные жителей Томской области находятся на томских серверах. Передача данных между сервером и «тонким клиентом» осуществляется по сети Интернет в зашифрованном виде. Тонкий клиент – компьютер с установленным браузером Firefox.

2) Корпоративная информационная система ПАРУС (КИС ПАРУС), предназначенная для автоматизированного учета финансово-хозяйственной деятельности государственного учреждения. Хранит и обрабатывает следующие персональные данные:
– паспортные данные;
– ФИО и дата рождения родственников;
– сведения об имуществе;
– дополнительная информация.

ИСПДн построена по типу «тонкого клиента». Все данные хранятся и обрабатываются на локальных серверах медицинских учреждений. Передача данных между сервером и «тонким клиентом» осуществляется по внутренней сети учреждения. Тонкий клиент – компьютер с установленным специальным программным обеспечением КИС ПАРУС.

3) Информационная система комплексного учета и статистики (ИСКУС). Предназначена для регистрации и учета обращений пациента в ЛПУ и создания необходимой отчетности и ведения реестров. Хранит и обрабатывает следующие персональные данные:
– ФИО;
– дата рождения;
– место регистрации/проживания/работы;
– паспортные данные;
– номер полиса ОМС;
– номера больничных карт;
– дата времени и результаты записи/посещения врача;
– сведения о госпитализации.

ИСПДн построена по типу «тонкого клиента». Все данные хранятся и обрабатываются на локальных серверах медицинских учреждений. Передача данных между сервером и «тонким клиентом» осуще-

ствляется по внутренней сети учреждения, так же есть возможность посылать запросы данных полисов ОМС в Томский территориальный фонд ОМС. Тонкий клиент – компьютер с установленным специальным программным обеспечением ИСКУС.

В данный момент мною разрабатывается система защиты ПДн для одного из медучреждений Томской области – ОГБУЗ «Роддом №1». Закончены работы по изучению нормативно-правовых актов в сфере ПДн и обследованию системы, в частности, изучены:

– организационная структура;
– сетевая структура;
– текущие НПА, принятые внутри ЛПУ;
– бизнес-процессы по хранению и обработке ПДн.

Далее в своей работе планируется для каждой ИСПДн:

– создание модели нарушителя;
– создание модели угроз;
– определение требований к СЗИ
– реализация системы защиты.

Итогом данной работы станет создание проекта системы защиты персональных данных, готового к внедрению в ОГБУЗ «Роддом №1».

ОПРЕДЕЛЕНИЕ ХАРАКТЕРИСТИК ПОСКОВОГО СПАМА

И.С. Созинова, студентка, А.С. Романов, доцент к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, irishechka7371@gmail.com

Поисковый спам (далее – спам) – это попытки обмана поисковой системы сервиса и манипулирования ее результатами с целью изменения позиции того или иного веб-сайта в результатах поиска [1].

Отличительная особенность спама – ухудшение качества результатов поисковых запросов. Например, в результатах поискового запроса вторым выдается сайт, в котором минимум информации, большей частью плагиата, с максимальным количеством страниц на сайте, реплицирующих друг друга.

Проблема спама также в том, что она влечет инфляцию индексов в поисковике: чем выше индекс, тем выше цена за поисковую машину.

На сегодняшний день предложены вариации решений проблемы отслеживания спама в поисковых запросах. Но нельзя оставлять без внимания тот факт, что поисковые системы стабильно выдают спам-страницы на выходе в определенном проценте.

Данная работа посвящена изучению отличительных особенностей контента поискового спама и выбору оптимального набора величин, наиболее точно характеризующих веб-страницу как поисковый спам.

В соответствии с существующей таксономией поисковый спам делится на ссылочный и контекстный [2]. В дальнейшем будем говорить только о контекстном спаме.

В зависимости от стандартной html-разметки веб-страницы, можно выделить 5 частей такой веб-страницы: body, title, мета-тег, текст ссылки, URL. Согласно исследованиям каждая из этих частей подвержена воздействиям «черной» оптимизации при продвижении спам-страницы в поисковом рейтинге.

Для манипулирования характеристиками и выбора наиболее оптимального набора были произведены исследование и сравнительный анализ спам-сайтов и релевантных веб-страниц.

В ходе исследования было отобрано 200 релевантных страниц из базы РОМИП BY.WEB-2007 [6], а также отобрано из различных источников 100 веб-страниц, содержащих в себе спам-контент. В большинстве случаев данные страницы являли собой пример классического спама, а также являлись досками объявлений или спам-блогами. Для проведения экспертной оценки страницы на предмет ее принадлежности к спаму был составлен перечень отличительных особенностей:

1) несоответствие заявленной информации содержимому;
2) длина страниц;
3) читабельность и «смотрибельность» страниц, в т.ч.: систематизированность текста, наличие ошибок разного рода (лексические, синтаксические, пунктуационные), большие блоки не разделенного на фрагменты текста, не удобные для чтения с экрана. В оформлении текста сайта не используются пробелы, отступы, списки, выделения и т.д., не учтена специфика веб-текста, шрифты фиксированного размера, фотографии низкого качества;
4) информация давно не обновлялась, сведения устарели;
5) отсутствует авторский текст, размещенные на сайте статьи взяты с других сайтов.

Для чистоты эксперимента было сгенерировано 20 веб-страниц, относящихся к классу дорвеев, при помощи утилиты DoorWay.su [7].

В таблице представлены результаты анализа характеристик спама и релевантных сайтов для выборок веб-страниц.

В работах [6, 7] внимание уделялось текстовым характеристикам контента. Проведенное исследование показало, что для классификации веб-страницы существует ряд отличительных особенностей, напрямую относящихся к специфике её создания при помощи html-разметки.

Выявленные характеристики планируется использовать для классификации веб-страниц по принадлежности к поисковому спаму в сочетании с классификатором на основе машины опорных векторов

(SVM), показавшим отличные результаты при решении ряда смежных задач [8].

Средние значения характеристик спама и «неспама»

Характеристики	Среднее арифметическое	
	Релевантные сайты	Спам
Длина текста html	32762,04	37488,25
Доля текста на странице	0,247273	0,128184
Кол-во слов	560,087	715,2
Кол-во ключевых слов на странице	4,869565	1,25
Кол-во ключевых слов на странице (норм)	0,152656	0,003425
Кол-во стоп-слов	159,1304	97,9
Плотность ключевых слов	1,415364	0,3621
Плотность заголовков	5,759727	0,005195
Тег TITLE (50–80 символов)		
Кол-во слов	4,47619	4,9
Плотность слов	4,867238	1,5063
Мета-тег		
Слов в тексте	12,66667	1,1
Плотность слов	2,0356	0,3672
Анкор		
Кол-во ссылок	68,47826	18,1
Без анкоров	8,304348	0,55
Внешние	11,04545	73,5
Внешние без анкоров	2,818182	13,95

ЛИТЕРАТУРА

1. Лицензия на использование поисковой системы Яндекса [Электронный ресурс]. Электронные данные. Режим доступа: http://legal.yandex.ru/termsofuse/, свободный (дата обращения: 5.03.14).

2. Gyongyi Z. Web Spam Taxonomy [Электронный ресурс] // Z. Gyongyi, H. Garcia-Molina. Электронные данные. Chiba: First International Workshop on Adversarial Information Retrieval on the Web (AIRWeb 2005), May 10–14, 2005. Режим доступа: http://infolab.stanford.edu/., свободный (дата обращения: 5.03.2014).

3. Способы генерации текста [Электронный ресрус] // SEO-PPC. Электрон. текст. дан. [Б.м.], 2008. Режим доступа: http://thisishot.org/?page_id=17, свободный (дата обращения: 5.03.2014).

4. Веб-коллекция BY.web 2007 [Электронный ресурс]. Электронная база. Режим доступа: http://romip.ru/ru/collections/by.web-2007.html, свободный (дата обращения: 5.03.2014).

5. Генератор дорвеев [Электронный ресурс]. Электрон. текст. дан. Doorgen.su. Режим доступа: http://doorway.su/manual.html, свободный (дата обращения: 5.03.2014).

6. Павлов А.С. Методы обнаружения поискового спама, порожденного с помощью цепей Маркова / А.С. Павлов, Б.В. Добров / Тр. XI Всерос. науч.

конф. «Электронные библиотеки: перспективные методы и технологии, электронные коллекции». Петрозаводск, 2009. С. 311–317.

7. Павлов А.С. Метод обнаружения массово порожденных неестественных текстов на основе анализа тематической структуры / А.С. Павлов, Б.В. Добров // Тр. XII Всерос. науч. конф. «Электронные библиотеки: перспективные методы и технологии, электронные коллекции». Петрозаводск, 2010. С. 210–218.

8. Романов А.С., Шелупанов А.А., Мещеряков Р.В. Разработка и исследование математических моделей, методик и программных средств информационных процессов при идентификации автора текста. Томск: В-Спектр, 2011. 188 с.

ИСПОЛЬЗОВАНИЕ HYPER-V ДЛЯ ПРОВЕДЕНИЯ ЛАБОРАТОРНЫХ РАБОТ В ИЗОЛИРОВАННОЙ СРЕДЕ

И.В. Степанов, студент

г. Томск, ТУСУР, tusur11b@mail.ru

В наше время достаточно широкое применение получило такое понятие, как виртуализация. Но вот, например, вы – далеко не знаток и не профессионал в ИТ-сфере и мало знакомы с этим понятием виртуализации и его использованием при построении IT-инфраструктур в бизнесе, обучении и многом другом. Вдруг использование виртуализации принесет вам сокращение ваших расходов и, например, даст толчок вашему бизнесу или же, наоборот, затормозит работу и не принесет никакой пользы.

Виртуализация – предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации и обеспечивающее при этом логическую изоляцию вычислительных процессов, выполняемых на одном физическом ресурсе.

Проще говоря, виртуализация – это использование одного физического ресурса для выполнения нескольких задач, которые будут выполняться изолированно и использовать только те ресурсы, которые выделяет им система, на которую они установлены.

Виртуализация делится на три типа:

– виртуализация представлений;

– виртуализация приложений;

– виртуализация серверов.

Самый яркий пример виртуализации представлений – это терминальные службы Windows Server. Терминальный сервер предоставляет свои вычислительные ресурсы клиентам, и клиентское приложение выполняется на сервере, клиент же получает только «картинку», то есть представление. Такая модель доступа позволяет, во-первых, сни-

зить требования к программно-аппаратному обеспечению на стороне клиента, во-вторых, снижает требования к пропускной способности сети, в-третьих, позволяет повысить безопасность.

Виртуализация приложений позволяет запускать отдельное приложение в своей собственной изолированной среде. Такой способ помогает решить множество проблем. Во-первых, опять же безопасность: приложение, запущенное в изолированной среде, не способно нанести вред ОС и другим приложениям. Во-вторых, все виртуализированные приложения можно обновлять централизованно из одного источника. В-третьих, виртуализация приложений позволяет запускать на одном физическом ПК несколько разных приложений, конфликтующих друг с другом, или даже несколько разных версий одного и того же приложения.

Виртуализация серверов – это программная имитация с помощью специального ПО аппаратного обеспечения компьютера: процессор, память, жесткий диск и т.д. Далее, на такой виртуальный компьютер можно установить операционную систему, и она будет на нем работать точно так же, как и на простом, «железном» компьютере. Самое интересное достоинство этой технологии – это возможность запуска нескольких виртуальных компьютеров внутри одного «железного», при этом все виртуальные компьютеры могут работать независимо друг от друга.

В Windows Server 2012 было введено понятие динамической миграции. Динамическая миграция в Windows Server 2012 позволяет переносить данные виртуальной машины, включая файл конфигурации и виртуальные жесткие диски, между любыми поддерживаемыми хранилищами без простоя виртуальной машины. Проще говоря, стало возможным перемещение ВМ с одного сервера Hyper-V на другой, без необходимости завершения работы затрагиваемой ВМ.

Известно, что виртуальные машины используют для своих нужд только те ресурсы, которые мы им выделили. А что если выделенных ресурсов оказалось мало и, например, из-за недостатка оперативной памяти процесс выполнения сложной вычислительной задачи может затянуться на очень длительный период времени? Для этого в Windows Server 2012 было введено понятие динамической памяти. Динамическая память – это новая функция Hyper-V, позволяющая более эффективно использовать физическую память. С использованием динамической памяти Hyper-V рассматривает память как общий ресурс, который может автоматически перераспределяться между выполняющими виртуальными машинами. Динамическая память корректирует объем памяти, доступный для виртуальной машины, на основании изменений

в требованиях к памяти и указанных пользователем значений. Динамическая память позволяет более эффективно использовать ресурсы.

Очевидно, часто при тестировании какого-то ПО, службы или драйвера желательно сохранить состояние ВМ, пробовать разные действия – и каждый раз иметь возможность вернуться в сохраненное состояние. Это сохраненное состояние и есть снимок или снапшот (Snapshot). То есть использование данной функции позволит выполнять любые действия с операционной системой, и если что то пойдет не так, то всегда можно загрузить систему с нужного сохранения.

Из всего вышесказанного можно сделать вывод о том, что виртуализация – это достаточно перспективное направление. В бизнесе при помощи виртуализации можно сократить расходы, а производительность наоборот повысить. Использование виртуальных машин в процессе обучения – это наиболее удобный способ, потому что в виртуальных машинах можно учиться и отрабатывать абсолютно любые навыки и знания без боязни каких-либо последствий. Ведь вы выполняете все действия в изолированной среде и любые ваши действия можно отменить, если что-то пошло не так. Объединение таких машин в виртуальные сети предоставляет возможность использования и применения на практике навыков обеспечения информационной безопасности, обнаружения нарушения целостности или обхода установленных рубежей защиты или изучения вредоносных программ, их поведения при попадании в ОС без опасности ее распространения.

ЛИТЕРАТУРА

1. Виртуализация Hyper-V [Электронный ресурс]. Режим доступа: http://www.itfb.com.ua/virtualization-hyper-v.html (дата обращения: 01.03.2014).

2. Электронная книга «Введение в System Center 2012 R2 [Электронный ресурс]. Режим доступа: https://blogs.technet.com/brutechnews/archive/2014/01/13/171-system-center-2012-r2-187.aspx (дата обращения: 03.03.2014).

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Е.В. Цыбань, студент каф. КИБЭВС

Научный руководитель Р.М. Шарипов, представитель обособленного подразделения ООО «Уральский центр систем безопасности» в г. Сургуте

г. Томск, ТУСУР, boxer2711@mail.ru

Технология облачных вычислений является одним из наиболее перспективных направлений развития информационных технологий, в настоящее время рассматриваемых в качестве альтернативы традици-

онной модели обработки информации. Использование систем облачных вычислений позволяет реализовать возможность удаленной обработки информации, обеспечивает достижение высоких показателей отказоустойчивости и доступности информационной инфраструктуры.

Угрозы информационной безопасности на уровне аппаратной платформы виртуализации включают традиционные угрозы на уровне аппаратной платформы виртуализации, реализация которых осуществляется путем нарушения работы аппаратных компонент серверного оборудования с установленными компонентами виртуальной среды и кражей носителей информации. Данные угрозы связаны с осуществлением угроз физического повреждения технических средств обработки информации, нарушения работы, извлечения или замены аппаратных компонентов системы, а также нарушением работы, отказом или сбоями в работе смежных обеспечивающих систем (электропитание, кондиционирование и пр.). Реализация данных угроз может привести к нарушению целостности и доступности защищаемых ресурсов вследствие остановки ВМ, запущенных на аппаратной платформе, или невозможности восстановления носителей информации.

Угрозы информационной безопасности на уровне системного программного обеспечения виртуализации включают специфические угрозы, связанные с НСД (удаленный доступ или доступ в рамках виртуальной среды) к ресурсам виртуальной машины, сетевые атаки типа «переполнение буфера» (на открытые порты сервера с гипервизором) и «отказ в обслуживании» (в отношении виртуальной машины), а также случайное или умышленное искажение и уничтожение образов виртуальной машины.

Угрозы ИБ на уровне системы управления виртуальной средой включают специфические угрозы, связанные с НСД к консоли управления виртуальной инфраструктурой, интерфейсу системы управления виртуальной среды и настройкам виртуальной машины.

Угрозы ИБ на уровне виртуальной машины включают специфические угрозы, связанные с НСД к виртуальной машине, нарушением изоляции информации, внедрением вредоносных программ на виртуальной машине, проведением сетевых атак между виртуальной машиной и др.

Угрозы ИБ на уровне систем хранения данных включают:

– традиционные угрозы НСД к РС администратора, уничтожения и хищения носителей данных систем хранения данных;

– специфические угрозы, связанные с НСД к управляющим интерфейсам компонент систем хранения данных и кражей разделов систем хранения данных с образами ВМ и данными. Реализация данных угроз может привести к нарушению функционирования компонент

систем хранения данных и работы виртуальной машины, а также НСД к защищаемой информации.

С точки зрения контроля безопасности при использовании средств виртуализации выделяется специфическая угроза, связанная с небезопасным развертыванием виртуальной машины, реализация которой напрямую не приводит к нарушению безопасности защищаемой информации, но может создать возможности для реализации других угроз информационной безопасности.

Таким образом, в данной статье были рассмотрены основные угрозы по уровням технологии облачных вычислений и их краткое описание.

ЛИТЕРАТУРА

1. Liu F. NIST Cloud Computing Reference Architecture [Электронный ресурс] / F. Liu, J. Tong // NIST Special Publication. Режим доступа: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505, свободный. Заглавие с экрана.

2. Peter R. Stephenson. A Formal Model for Information Risk Analysis Using Colored Petri Nets. Colored Petri Nets (CPN), 2004.

3. Badger L. DRAFT Cloud Computing Synopsis and Recommendations [Электронный ресурс] / L. Badger, T. Grance // NIST Special Publication. Режим доступа: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf, свободный. Заглавие с экрана.

ЗАДАЧА ЭНЕРГОЭФФЕКТИВНОГО УПРАВЛЕНИЯ ГРУППОЙ ВОДОДОБЫВАЮЩИХ НАСОСОВ И ЕЕ РЕШЕНИЕ НЕЙРОСЕТЬЮ ХОПФИЛДА

Е.О. Иванов, аспирант каф. АОИ,
Д.И. Цыбусов, А.А. Даниленко, студенты
г. Томск, ТУСУР, egor.o.ivanov@yandex.ru, demonbusov1@yandex.ru, danilenkoprogaleksandr@gmail.com

Проект ГПО АОИ-1301 – «Энергосберегающее ситуационное нейросетевое управление»

Имеется группа вододобывающих насосов, работающих на заполнение резервуара. Каждый насос характеризуется своей подачей Q_i ($м^3$/ч) и потребляемой мощностью N_i (кВт), поэтому различно значение удельной стоимости перекачки единицы воды $C_i = N_i / Q_i$.

Обычно насосы вводятся в избыточном количестве, поэтому все включенные насосы обладают суммарной подачей Q_z, большей, чем реальная потребность [1].

Сложность предсказания количества требуемой воды приводит к применению простейших экономически и технологически не выгодных алгоритмов управления: включение и выключение насосов при достижении уровня воды в резервуаре определенных отметок.

Выгодней поддерживать уровень воды в резервуаре на определенной отметке путем включения насосов, суммарно подающих количество воды, равное потребляемому. При этом целесообразно использовать средний интервал времени управления, например час.

Для определения предполагаемого значения оттока из резервуара предполагается использовать краткосрочное прогнозирование с помощью многослойных нейронных сетей.

Зная прогноз водопотребления на час вперед и расхождение уровня воды в резервуаре с необходимым, можно определить суммарное количество воды, которое необходимо подать в резервуар в течение следующего часа.

Возникает задача определения, какие насосы следует включить, а какие выключить для определения оптимального распределения нагрузки. Таким образом, приходим к многокритериальной задаче оптимизации: снижение стоимости и соответствие требуемой производительности.

Нейросетевая постановка задачи. Обозначим: $x_i \in \{0,1\}$ – состояние насоса в текущий момент времени, где 1 соответствует состоянию «включен», 0 – «выключен», общее количество насосов обозначим n. Таким образом, при $x_i = 0$ выключенный насос не будет увеличивать суммарную удельную стоимость, а включенный ($x_i = 1$) – будет на величину C_i. Тогда решением задачи будет поиск вектора состояний всех насосов X, который будет минимизировать их суммарную удельную стоимость и отклонение от суммарной необходимой подачи Q_z.

Представим задачу в терминах сети Хопфилда с бинарными состояниями нейронов $x_i \in \{0,1\}$ и функцией энергии $E = E(t)$ дискретной сети с дискретным временем:

$$E = \alpha(\sum_i x_i Q_i - Q_z)^2 + \beta \sum_i x_i c_i \ ,$$

где α и β – неотрицательные вещественные константы, определяющие вклад критериев оптимальности в энергию сети.

Построив уравнение динамики сети согласно [2] и сопоставив с динамикой сети Хопфилда, находим матрицу весов w_{ij} формула (1) и вектор порогов u_i – формула (2):

$$w_{ij} = -2\alpha Q_i^2 \delta_{ij} - 2\alpha Q_j Q_i (1 - \delta_{ij}) \, , \qquad (1)$$

$$u_i = -2\alpha Q_z Q_i + \beta c_i, \qquad (2)$$

где δ_{ij} – символ Кронекера.

Моделирование. В качестве задачи для моделирования рассматривалась группа из 18 насосов (реальные данные).

Алгоритм на основе сети Хопфилда сравнивался с двумя простейшими алгоритмами: включение насосов в порядке возрастания их мощностей, пока не возникнет приближение к желаемой суммарной подаче, и включение насосов в порядке возрастания удельной стоимости добычи кубометра воды.

Для сравнения алгоритмов было реализовано приложение в среде Lazarus на языке Object Pascal. А также для отображения работы алгоритмов была написана графическая модель водозабора 1-го уровня с использованием графической библиотеки «Andorra 2d».

Так как получение решения задачи необходимо выполнять ежечасно, в процессе моделирования оценивалась не скорость получения решения, а его качество.

Моделирование выполнялось многократно. Модель Хопфилда запускалась на вычисления с коэффициентами $\alpha = 1{,}0$ и $\beta = 0{,}24$, подобранные экспериментально с расчетом на минимальное расхождение в количестве воды.

Проведем анализ результатов моделирования (таблица) различных подходов на одинаковых данных.

Результаты моделирования

Алгоритм	Сумма N	Сумма C	Среднее
Хопфилд	206820	374680	0,552
Минимизация N_i	234160	375610	0,623
Минимизация C_i	199190	376910	0,528

Во 2-м столбце представлена суммарная мощность, потребленная всеми включенными насосами за все время моделирования. В 3-м столбце находится суммарное значение подачи каждого из алгоритмов. По условию суммарная необходимая подача всех насосов составляла 374100 м$^{3.}$ Как видим, сеть Хопфилда сгенерировала наилучшее значение. Последний столбец показывает среднюю удельную стоимость каждого кубометра воды. Здесь сеть Хопфилда показала приемлемые, но не лучшие результаты. Но вместе с тем сеть Хопфилда оставляет много места для маневра: подбирая значения коэффициентов, можно регулировать «вес» каждого из критериев оптимальности.

Заключение Таким образом, представленная дискретная сеть Хопфилда, решающая задачу оптимизации работы группы насосов, показала хорошие результаты моделирования. Получение более каче-

ственных решений задачи может быть достигнуто переходом на непрерывную модель функционирования сети Хопфилда, путем включения частотного управления.

ЛИТЕРАТУРА

1. Замятин Н.В., Иванов Е.О. Задача энергоэффективного управления группой вододобывающих насосов и ее решение нейросетью Хопфилда // Доклады ТУСУРа. 2013. № 4 (30). С. 168–172.

2. Меламед И.И. Нейронные сети и комбинаторная оптимизация // Автоматика и телемеханика. 1994. Вып. 11. С. 1–38.

СИСТЕМА ЗАЩИТЫ РАСПРЕДЕЛЕННОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

М.А. Турунтаев, студент, А.И. Кураленко, аспирант

г. Томск, ТУСУР, РТФ, каф. РЗИ, ten10shin@gmail.com

Построение системы защиты информации распределенного удостоверяющего центра (РУЦ) – очень сложный и трудоемкий процесс [1], связанный с тем, что точки выдачи сертификатов территориально разнесены от центра сертификации (ЦС) и регистрации (ЦР). Поэтому при создании системы защиты информации надо опираться не только на требования, предъявляемые законодательством [2–4], но и на актуальные угрозы безопасности информации.

В данной работе описано построение системы защиты РУЦ на базе программно-аппаратного комплекса «КриптоПро УЦ», состоящего из ЦС, ЦР и 2 АРМ Администраторов ЦР, которые территориально разнесены от ЦР (рис. 1).

Согласно с [3] в качестве возможного источника угрозы будут выступать нарушители категории H_1 и H_2. Возможности нарушителя также определены в [3].

Определение перечня актуальных угроз является одной из основных задач построения системы защиты информации. На основе актуальных угроз будут выбираться необходимые средства и меры защиты. Далее будет приведен способ определения актуальных угроз с помощью модифицированного SWOT-анализа.

SWOT-анализ – метод стратегического планирования, заключающийся в выявлении факторов внутренней и внешней среды организации: Strengths (сильные стороны), Weaknesses (слабые стороны), Opportunities (возможности) и Threats (угрозы) [5].

SWOT-анализ для определения актуальных угроз будет представлен в следующем виде (таблица):

1. Слабые стороны (W) будут представлены в качестве уязвимых звеньев.

2. Возможности (O) – возможности нарушителя.

3. Угрозы (T) – угрозы информационной безопасности.

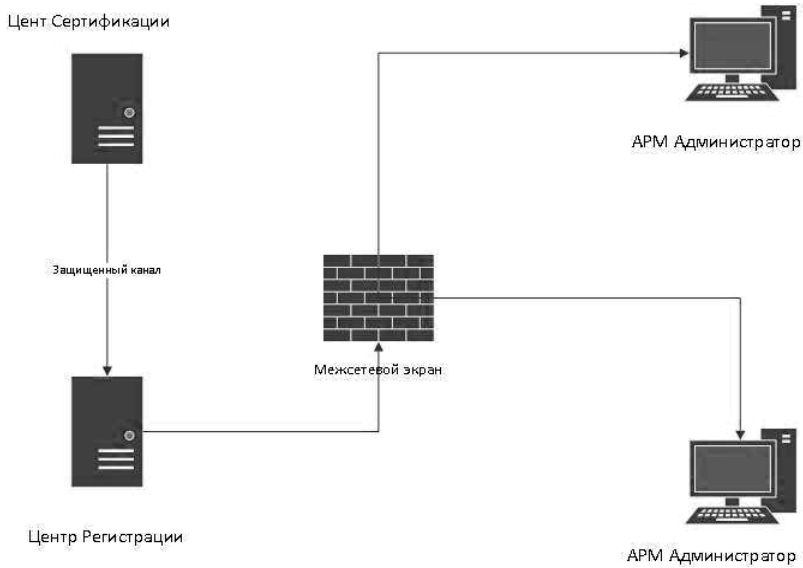


Рис. 1. Топология РУЦ

Поле СЛВ показывает, за счет каких возможностей нарушитель может воспользоваться уязвимостью.

Поле СЛУ показывает, через какие уязвимости может быть реализована угроза (отношение уязвимостей и угроз).

Матрица SWOT анализа

SWOT-анализ		Возможности (O) (возможности нарушителя)				Угрозы (T) (базовая модель угроз)			
		O_1	O_2	…	O_n	T_1	T_2	…	T_n
Слабые стороны (W) (уязвимости)	W_1	СЛВ				СЛУ			
	W_2								
	…								
	W_n								

В результате анализа были получены актуальные угрозы, например:

- угрозы физического доступа;

- угрозы проникновения в операционную систему с применением программных или программно-аппаратных средств;
- и т.д.

Система защиты должна обеспечивать конфиденциальность, целостность и доступность информации посредством организационных и технических мер защиты. Требования к системе защите РУЦ определены на основе актуальных угроз и требований [3, 4, 6].

На основе требований построена система защиты РУЦ, включающая следующие технические средства защиты:

- модуль доверенной загрузки и систему защиты АС от НСД Аккорд-АМДЗ и Аккорд-Win32;
- межсетевой экран и криптошлюз VipNet Coordinator HW100 перед ЦР и ЦС и VipNet client 3.2 на АРМ Администратора ЦР;
- антивирусную защиту объектов на основе «Антивируса» Касперского Endpoint Security.

Разработаны организационно-распорядительные документы в соответствии с определенными ранее требованиями к системе защиты такие, как регламент работы РУЦ; должностные инструкции по работе и т.п.

В результате работы построена система защиты РУЦ на основе КриптоПро УЦ. Для достижения этой цели определена модель нарушителя, с помощью модифицированного SWOT-анализа построена модель угроз, определены требования к системе защиты, реализованы технические и организационные меры защиты РУЦ.

ЛИТЕРАТУРА

1. Кураленко А.И. Оценка защищенности системы обеспечения безопасности информации удостоверяющего центра // Системы высокой доступности. 2013. №3. С. 128–130.

2. Специальные требования и рекомендации по технической защите конфиденциальной информации. М.: Гостехкомиссия РФ, 2003.

3. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, (утв. руководством 8 Центра ФСБ России 21 февр. 2008 г. № 149/54-144).

4. Приказ ФСБ РФ от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

5. Майсак О.С. SWOT-анализ: объект, факторы, стратегии. Проблема поиска связей между факторами // Прикаспийский журнал: управление и высокие технологии. 2013. № 1. С. 151–157.

6. ЖТЯИ.00067 02 90 01 КриптоПро УЦ. Общее описание.

КИБЕРВОСПИТАНИЕ ДЖИХАДИСТОВ: АНАЛИЗ

И.С. Васильева, студентка
Научный руководитель О.Н. Мызников, доцент
г. Краснодар, КубГТУ, ИКСИБ, inna1523@mail.ru

Всемирная паутина является домом для десятков сайтов, которые предоставляют информацию о том, как построить химическое и взрывоопасное оружие. Многие из этих сайтов размещают различные руководства (Энциклопедия Джихада, справочник Моджахеда, настольная книга террориста и т.п.), которые могут быть использованы не только террористическими организациями, но и «одинокими волками» для подготовки террористического акта в поддержку своих идей. Удивительно, насколько легкодоступна эта информация. Поиск по ключевым словам «террорист» и «руководство» в поисковой системе Google выдаст тысячи страниц, на которых есть или сами руководства, или ссылки на них – кибервоспитание джихадистов.

Террористические организации, действующие во имя джихада, используют Интернет в военной подготовке за счет циркуляции военных руководств по вооружению, тактике ведения боя, производству взрывчатых веществ и т.п. Другим типом онлайн – деятельности является использование методов взлома сайтов («электронный джихад»). В рамках этой деятельности исламистские хакеры атакуют сайты тех, кого они считают своими врагами, с целью саботирования сайтов. Они также пытаются взломать стратегические, экономические и военные сети с целью причинения существенного ущерба инфраструктурам. Многие исламистские сайты и форумы имеют специальные разделы, посвященные теме электронного джихада. Основное применение джихадистами Интернета – воспитание новых джихадистов и пропаганда Ислама. Кибервоспитание рассматривается этими организациями в качестве неотъемлемой части их «священной войны» и в качестве еще одного фронта джихада в дополнение к своей военной, экономической и политической активности. На самом деле они характеризуют Интернет или другую информационную деятельность как джихад, который может быть осуществлен теми, кто не может участвовать в боевых действиях на поле боя.

Наиболее эффективный и непосредственный способ борьбы с этим явлением – это во-первых, разоблачение экстремистских сайтов через средства массовой информации, и, таким образом, информирование провайдеров и общественности в целом об их содержании, а во-вторых, проведение правовых мер против интернет-провайдеров, которые продолжают обслуживать экстремистские сайты и форумы. И на последнем этапе – полное удаление сайта и контента из Интернета.

Опыт учит нас, что воздействие само по себе эффективное средство против экстремистских сайтов. Действенным средством против деятельности экстремистов в Интернете было бы создание единой (мировой) базы данных, которая будет собирать всю информацию об исламистских/джихадистских сайтах и отправлять ее для дальнейшего разбирательства правоохранительным органам стран-участниц. Однако какие бы блага не несла эта база, она может стать и опасным оружием, поэтому помимо всех организационных мероприятий нужно провести эффективные защитные меры (с оригинальным шифрованием).

По большей части анализ джихадистских сайтов не направлен на поиск дискуссий о планировании атак, но, изучив их, мы можем узнать идеологию и формирование в общине выбора цели во имя джихада, а также «увидеть» и проследить набор новобранцев.

Наличие джихада в киберпространстве наиболее ощущается в идеологической дискуссии. Интернет имеет важное значение для идеологического развития движения, а также фактического распространения этой идеологии для потенциальных новобранцев и сторонников. Такие свободно доступные дискуссии образуют окно в джихад, что упрощает его изучение как на «низком» уровне, так и на «высшем» уровне (уровень лидеров).

Один из лучших способов узнать о террористической организации – это чтение статей, руководств и других документов, предоставляемые на их сайтах и написанных их лидерами для поддержки и дисциплины всей организации. Многие из таких документов могут быть перехвачены военнослужащими и сотрудниками правоохранительных органов и дать представление о том, как работает организация. Источники легкодоступны в Интернете. Чем больше будет доступ к этим документам, тем больше преимуществ можно достигнуть для борьбы с терроризмом. Аналитики, получив доступ к подобной базе данных, смогут понять ключевую идеологию, стратегию и мотивацию движения. Интересно то, что такой анализ чаще проводят аналитики частного или академического сектора.

Интернет используется не только для идеологического обсуждения и распространения идей, но и для тактических дискуссий. Анализ тактической информации может дать исчерпывающие данные об организации: к примеру, анализ оружия, которое использует организация, может дать информацию о том, почему они выбрали то или иное оружие, узнать их предположения относительно эффективности этого оружия.

Как уже упоминалось, джихад в значительной мере опирается на сети для распространения информации от высших эшелонов к низшим. Заявления лидеров движения можно считать полезным вкладом для

анализа разведывательных данных. Контекстный анализ таких заявлений может дать некоторый намек о намерениях, хотя большая часть этих заявлений состоит из огромного количества бахвальства, обмана и ложной информации. Поэтому контекстный анализ может быть очень полезным, такой анализ может определить мнение заявителя и то, что хотят услышать сторонники движения.

Особое внимание следует уделить языку, на что делается упор, и даже дизайну сайтов. Используемые языки могут сказать, кого джихадисты хотят привлечь в свои ряды. В некоторых случаях это указывает на предполагаемые уязвимости среди целевой группы. Также можно вычленить информацию о том, кого бы они могли завербовать (узконаправленных специалистов).

Еще одним предметом анализа может быть структура и дизайн сайта. Эти сайты – часто работа одних из лучших и квалифицированных джихадистов-новобранцев нового поколения (так как требуются знания новых современных технологий).

Джихад, как и любое другое крупное общественное движение, зависит от широкой поддержки. Положительное общественное мнение внутри их круга является обязательным не только для привлечения новых рекрутов/кадров, но и для поддержки. Одной из ключевых ценностей мусульманских обществ являются социальное единство и гармония. Эффективной контратакой было бы использование их же атак против них.

Тот факт, что почти все «сырье» для анализа можно достать в Интернете, не должен быть недооценен спецслужбами. Сегодняшние бои ведутся все больше и больше в сфере общественного мнения, а не на поле боя. Террористы и те, кто с ними борются, «воюют» за ту же аудиторию. В этом типе войны, Интернет является как полем боя, так и оружием. Для джихадистов, это палка о двух концах: чем больше их зависимость от Интернета, тем больше их распространение и эффективность действий, но и тем больше они уязвимы.

Дальнейшее изучение контента позволит разработать методику анализа скрытых групп в Интернете (социальных сетях) и расширение рекомендательной базы по борьбе с терроризмом.

ЛИТЕРАТУРА

1. Авдеев Ю.И. Особенности современного международного терроризма и некоторые правовые проблемы борьбы с ним. М.: Век, 2008.

2. Denning D.E. Cyberterrorism, Global Dialogue, 2000.

РЕКОМЕНДАЦИИ ПО БОРЬБЕ С КИБЕРТЕРРОРИЗМОМ

И.С. Васильева, студентка
Научный руководитель О.Н. Мызников, доцент
г. Краснодар, КубГТУ, ИКСИБ, inna1523@mail.ru

Что может сделать правительство, частный сектор и гражданское общество для предотвращения кибертеррористических атак? Сегодня более чем когда-либо прежде мир объединяется за счет использования технологии. С появлением Интернета жизнь в целом стала легче, но мы открыли и новую эру беспрецедентной угрозы безопасности. Между 2006–2013 гг. число нападений увеличилось на 850% (по статистическим данным). Нынешнее поколение террористов становится все моложе и искуснее в работе с новыми технологиями. Целесообразно предложить некоторые рекомендации для органов власти, частного сектора и гражданского общества по борьбе с кибертерроризмом.

1) *Создать и принять всеобъемлющую киберстратегию; разработать четкие обязанности для государственных учреждений; организовать частные и промышленные ответственные органы.*

Эта рекомендация частично зависят от того, что правительство хоть и подтвердило факт существования кибертерроризма как угрозы национальной безопасности, однако фактических действий и стратегий по борьбе с этим видом терроризма нет. В настоящее время всеобъемлющей российской киберстратегии не существует, так же как и законодательной базы. Для начала нужно разработать краткие документы, обозначающие определенные роли и обязанности учреждений, уровни доступа к информации, установить критерии и методы для отслеживания прогресса и внедрения практик. Кроме того, правительство должно донести до частного сектора, что они в полной мере ответственны за обеспечение высокого уровня кибербезопасности, особенно по отношению к критическим инфраструктурам.

Нужно произвести аудит как государственного, так и частного секторов на соответствие требованиям по обеспечению безопасности, оценить их потенциал по предотвращению кибертеррористических атак разных уровней. Системы, имеющие решающее значение для поддержания и регулирования критических инфраструктур страны, должны стоять в начале списка, так как атака, направленная на них, может поставить под угрозу национальную безопасность. К примеру, такие меры уже введены в действие в Китае и Японии, правительства этих стран смогли наладить диалог между органами власти и бизнесом, промышленностью на разных уровнях, что в свою очередь гарантирует оперативные оборонные действия. Российская Федерация и ее

союзники должны учиться таким подходам, для того чтобы успешно защищать нацию от угроз кибертерроризма.

2) *Правительство должно привлечь гражданское общество в качестве заинтересованной стороны в повышении устойчивости к кибертеррористическим атакам.*

В настоящее время население РФ относится с недоверием к способностям правительства справиться с кибертеррористическими атаками, в то время как, например, 60 процентов населения Китая считает, что правительство способно успешно бороться с кибертерроризмом. Следовательно, помимо законодательной базы нужно создать что-то вроде гражданской культуры, которая будет рассматривать кибербезопасность как приоритетную область развития страны.

Рекламные ролики и билборды с просьбой граждан сообщать о подозрительной деятельности оказались бы весьма эффективными. Поэтому логично будет создать нечто подобное для эффективного реагирования на инциденты и подозрительную активность в киберпространстве, – системы, которые будут информировать граждан о многочисленных угрозах, присутствующих в киберпространстве, и поощрять использование мер по обеспечению кибербезопасности. Правительство должно распространять идею всеобщей кибербезопасности через социальные медиа, СМИ и т.п., начать обучение основам информационной безопасности в образовательных учреждениях, дабы подчеркнуть важность кибербезопасности в раннем возрасте.

3) *Создание международных норм управления Интернетом и борьбы с международным черным рынком.*

Субъект, государственный орган или международная организация не могут и не должны иметь полный контроль над Интернетом. Однако для того чтобы предотвратить злоупотребление Интернетом, в частности, террористами, которые активно распространяют экстремистскую информацию, нанимают хакеров и других профессионалов, увеличивают свой капитал, а также планируют и исполняют атаки, можно прибегнуть к международному сотрудничеству, которое может дать больше возможностей для регулирования и сдерживания Интернета.

4) *Нужно построить гораздо более прочную оборону, интегрированную систему комплексной аварийной готовности и реагирования, а также улучшить процессы их использования.*

Нужно обеспечить своевременную индикацию и предупреждение кибератак. Обнаружение вторжений стало особо развиваться и исследоваться в последнее время. Не удивительно, что системы обнаружения и оповещения довольно сложны и, к сожалению, склонны к ложным срабатываниям. В случае нападения должна быть разработана

система управления инцидентами, смягчения атак и ограничения ущерба.

Следующей линией обороны является внутреннее обособление (дробление) программ и информационных файлов для защиты от несанкционированного доступа, а также сдерживание. В этом случае цель заключается в ограничении проникновения и повреждения, т.е. защите важных активов от повторной атаки и сборе информации, что облегчит, восстановит данные и усовершенствует контрмеры.

Особое внимание необходимо уделить сохранению и сбору информации во время кибертеррористической атаки. Это поможет в дальнейшем расследовании инцидента, что облегчит работу правоохранительным органам, а предприятию – учесть этот опыт в будущем. Чем сложнее атака, тем сложней разработать систему с подобными функциями.

Существующие контрмеры носят лишь рекомендательный характер. Решение, какие действия будут предприняты, должны быть сделаны согласно тому, кто нападает. В отличие от обычного террориста, который имеет характерные черты и может быть идентифицирован среди общей массы людей, ситуация с кибертеррористами абсолютно противоположна и требует индивидуального подхода.

ЛИТЕРАТУРА

1. Авдеев Ю.И. Особенности современного международного терроризма и некоторые правовые проблемы борьбы с ним. М.: Век, 2008.

2. Васенин В.А. Информационная безопасность и компьютерный терроризм. 2004. http://www.crime-research.ru

3. Гришко А.Я. Личность террориста: Криминологический портрет. Рязань: Академия права и управления Федеральной службы исполнения наказаний, 2006.

4. Denning D.E. Cyberterrorism // Global Dialogue. 2000.

ИСПОЛЬЗОВАНИЕ DLP-СИСТЕМ С ТОЧКИ ЗРЕНИЯ ЗАКОНОДАТЕЛЬСТВА РФ

Е.И. Вискунов, студент каф. КИБЭВС

Научный руководитель А.Ю. Корнилов, начальник отдела ИТ

г. Томск, ООО «ТОМТЕЛ», evgeniy.viskunov@live.com

Одна из основных проблем, являющихся следствием внедрения DLP-системы в существующую сеть предприятия, – это законность её использования по отношению к сотрудникам. В связи с тем, что DLP-системы позволяют осуществлять перехват информации, передающейся по различным каналам, таким как электронная почта, skype, IM-

мессенджеры и др., возникает вопрос законности этого перехвата. Конкретизированного решения на данный момент до сих пор не существует, но с каждым годом вносится всё больше ясности.

Чаще всего при возникновении вопроса о законности использования средств мониторинга, противники приводят в качестве аргументов отдельные статьи из Конституции и УК РФ. В частности, в ст. 23 Конституции РФ определяется, что:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения [1].

Аналогичная мысль прописана в гл. 9, ст. 63 ФЗ от 07.07.03 №126-ФЗ «О связи» [2].

Исходя из вышесказанного, в случае нарушений к компании можно применить ч. 2 ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» [2].

В свою очередь у компаний есть аргументы в свою защиту:

1. Часть 2 ст. 209 ГК РФ гласит: «Собственник вправе по своему усмотрению совершать в отношении принадлежащего ему имущества любые действия, не противоречащие закону и иным правовым актам и не нарушающие права и охраняемые законом интересы других лиц, в том числе отчуждать свое имущество в собственность другим лицам, передавать им, оставаясь собственником, права владения, пользования и распоряжения имуществом, отдавать имущество в залог и обременять его другими способами, распоряжаться им иным образом». Этот пункт означает, что работодатель вправе контролировать работников на предмет использования оборудования компании по целевому назначению [3].

2. Статья 22 ТК РФ, по которой работодатель обязан «обеспечивать работников оборудованием, инструментами, технической документацией и иными средствами, необходимыми для исполнения ими трудовых обязанностей». И ст. 189 ТК РФ, по которой «работодатель обязан в соответствии с трудовым законодательством и иными нормативными правовыми актами, содержащими нормы трудового права, коллективным договором, соглашениями, локальными нормативными актами, трудовым договором создавать условия, необходимые для соблюдения работниками дисциплины труда». Работник же по ст. 21 обязан «добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором; соблюдать правила внутреннего трудового распорядка; соблюдать трудовую дисциплину; выполнять установленные нормы труда». При этом из ст. 189 «Дисциплина тру-

да» определяется как «обязательное для всех работников подчинение правилам поведения, определенным в соответствии с настоящим Кодексом, иными федеральными законами, коллективным договором, соглашениями, локальными нормативными актами, трудовым договором» [4].

Исходя из этого, можно сделать вывод, что для правомерности использования DLP-систем в корпоративной сети необходимо, чтобы её использование было закреплено в локальном нормативном акте либо в нормативном правовом акте.

В тех случаях, когда сотрудник знает, что работодатель имеет доступ к содержанию отправленных и полученных сообщений и выразил согласие на совершение подобных действий, они не должны квалифицироваться как нарушение конституционного права работника. К тому же, согласно требованию ст. 22 ТК РФ, работодатель обязан «знакомить работников под роспись с принимаемыми локальными нормативными актами, непосредственно связанными с их трудовой деятельностью».

Исходя из этого, будет верным заручиться письменным согласием работника, прописав несколько дополнительных пунктов в трудовом договоре. Например, такие:

1. Работники извещены о том, что в случае использования ими оборудования работодателя в личных целях (указать возможные), в силу специфики работы системы, работодатель может непреднамеренно получать доступ к передаваемым сведениям, при этом работник дает согласие на подобный доступ.

2. Работники извещены о том, что они не должны использовать оборудование работодателя (в рабочее и нерабочее время) для целей, не связанных с выполнением их прямых должностных обязанностей, указанных в должностных инструкциях.

3. Работодатель может контролировать использование сотрудниками оборудования (персональных компьютеров) и ПО, принадлежащих работодателю, при помощи «системы мониторинга».

Или можно сформулировать данные пункты в более конкретизированной форме, что поможет избежать недопонимания со стороны работников.

ЛИТЕРАТУРА

1. Конституция РФ от 12.12.1993 [Электронный ресурс]. Режим доступа: http://www.consultant.ru/popular/cons/ (дата обращения: 17.02.2014).

2. Федеральный Закон от 07.07.03 №126-ФЗ (ред. от 28.12.2013) «О связи» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/popular/communication/ (дата обращения: 18.02.2014).

3. Гражданский кодекс РФ (ч. 1) от 30.11.1994 №51-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/popular/gkrf1/ (дата обращения: 19.02.2014).

4. Трудовой кодекс РФ от 30.12.2001 №197-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/popular/tkrf/ (дата обращения: 20.02.2014).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ

А.А. Воронова, Ю.Е. Иванова, О.Ю. Тензик, студентки каф. АСУ

Научный руководитель Т.А. Ельцова, доцент, к.ф.-м.н.

г. Томск, ТУСУР, каф. математики, le_say@sibmail.com

Быстро развивающиеся компьютерные информационные технологии вносят заметные изменения в нашу жизнь. Информация стала товаром, который можно купить, продать, обменять. И от степени безопасности информационных технологий в настоящее время зависит благополучие, а порой и жизнь людей. Такова плата за усложнение и повсеместное распространение автоматизированных систем обработки информации.

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации. На практике важнейшими являются три аспекта информационной безопасности:

1) доступность,

2) целостность,

3) конфиденциальность.

Нарушения этих аспектов могут быть вызваны различными опасными воздействиями на информационную систему, которая представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, связанных между собой. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.

Компоненты автоматизированной информационной системы можно разбить на следующие группы:

1) аппаратные средства,

2) программное обеспечение,

3) данные (хранимые временно и постоянно),

4) обслуживающий персонал и пользователи.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. И информа-

ция подвергается различным воздействиям на всех этапах цикла жизни системы.

Формирование режима информационной безопасности – проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1) законодательный,

2) морально-этический,

3) административный,

4) физический,

5) аппаратно-программный.

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты. Объекты защиты целесообразно разделять на группы так, чтобы нарушение защиты в одной из групп не влияло на безопасность других.

Целью работы является рассмотрение информационной безопасности мобильных устройств и компьютерных данных. А также разработка и реализация модификаций шифров Рабина и Blowfish.

В общем случае алгоритм шифрования Blowfish представляет собой сеть Фейстеля, но с некоторыми особенностями генерации и использования раундовых ключей (P_0, P_1…). Для начала допустим, что функция итерации F в алгоритме Blowfish – это некоторый «черный ящик», который принимает на входе и выдает на выходе 32-битное число. При этом 32-битные раундовые ключи Pn:

1) вычисляются по некоторому правилу от исходного ключа (длиной до 448 бит);

2) не являются аргументами для функции итерации F;

3) непосредственно складываются по модулю 2 (XOR) с «левым блоком». Результат этой операции является входящим 32-битным аргументом для функции F. В алгоритме Blowfish при шифровании выполняется 16 раундов (внутри сети Фейстеля), а 17-й и 18-й ключи складываются с левым и правым выходным блоком последнего раунда. Такое количество раундов было выбрано, поскольку именно оно определяет длину возможного ключа (рис. 1).

Функция раунда или итерации использует лишь несколько логических операций над матрицей подстановок. Матрицы подстановок S_1–S_4 используются для того, чтобы линейно преобразовать входящие 32 бита данных в значение из матрицы подстановки. А сами значения в матрицах подстановки вычисляются на этапе расширения ключа.

Формула функции:

$$F(X_1, X_2, X_3, X_4) = (((S_1[X_1\} + S_2[X_2])\mathrm{mod}2^{32} \oplus S_3[X_3]) + S_4[X_4])\ \mathrm{mod}2^{32}.$$

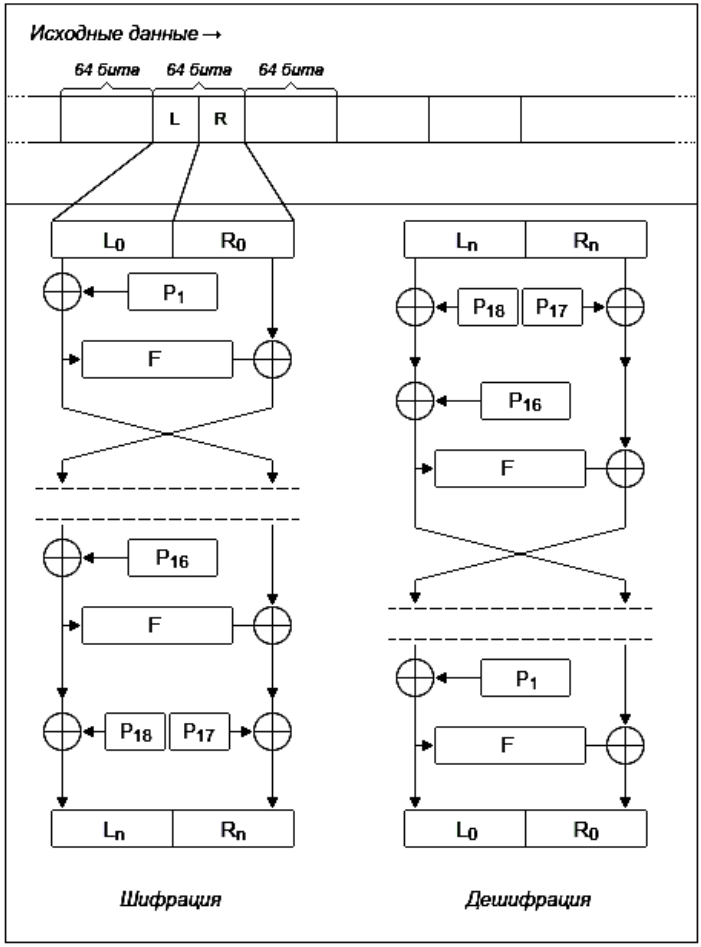


Рис. 1. Реализация сети Фейстеля для алгоритма Blowfish

Итак:

1) входящий 32-битный блок делится на четыре 8-битных блока, назовем их X_1, X_2, X_3, X_4 (рис. 2), каждый из которых является индексом массива таблицы замен S_1–S_4;

2) значения $S_1[X_1]$ и $S_2[X_2]$ складываются по модулю 2^{32}, затем результат складывается по модулю 2 (XOR) с $S_3[X_3]$ и, наконец, складываются с $S_4[X_4]$ опять же по модулю 2^{32};

3) результат вычислений и будет значением функции $F(X_1–X_4)$.

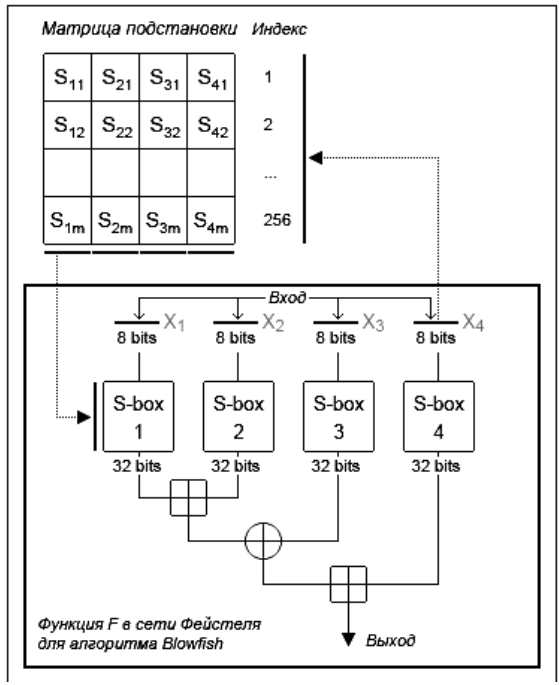


Рис. 2. Функция *F* в сети Фейстеля для алгоритма Blowfish

ЛИТЕРАТУРА

1. Смарт Н. Криптография. М.: Техносфера, 2005. 528 с.
2. Шнайер Б. Прикладная криптография. М.: Триумф, 2002. 816 с.
3. Галатенко В.А. Стандарты информационной безопасности. М.: Интернет-университет информационных технологий, 2006. 264 с.
4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов. М.: Горячая линия-Телеком, 2004. 280 с.

АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ЗАНИМАЮЩЕГОСЯ АНАЛИЗОМ РИСКОВ И ПРОВЕРКОЙ НА СООТВЕТСТВИЕ СТАНДАРТАМ

А.А. Войченко, студент каф. КИБЭВС
Научный руководитель А.А. Конев, доцент каф. КИБЭВС
г. Томск, ТУСУР, alexgarf@yandex.ru

Инструментальные средства анализа рисков позволяют автоматизировать работу специалистов в области защиты информации, осуще-

ствляющих оценку или переоценку информационных рисков предприятия.

В России в настоящее время чаще всего используются разнообразные «бумажные» методики, достоинствами которых являются гибкость и адаптивность. Как правило, разработкой данных методик занимаются компании – системные и специализированные интеграторы в области защиты информации. По понятным причинам методики обычно не публикуются, поскольку относятся к «Know how» компании. В силу закрытости данных методик судить об их качестве, объективности и возможностях достаточно сложно.

Специализированное ПО, реализующее методики анализа рисков, может относиться к категории программных продуктов (продается на рынке) либо являться собственностью ведомства или организации и не продаваться. Если ПО разрабатывается как программный продукт, оно должно быть в достаточной степени универсальным. Ведомственные варианты ПО адаптированы под особенности постановок задач анализа и управления рисками, и позволяют учесть специфику информационных технологий организации.

Предлагаемое на рынке ПО ориентировано в основном на уровень информационной безопасности, несколько превышающий базовый уровень защищенности. Таким образом, инструментарий рассчитан в основном на потребности организаций 3–4-й степени зрелости.

В 2005 г. был принят Международный стандарт ISO/IEC 27001:2005, за основу которого был взят Британский стандарт BS 7799. В результате большинство инструментальных средств (ПО анализа риска) было в последнее время модифицировано таким образом, чтобы обеспечить соответствие требованиям именно этого стандарта.

Для подтверждения вышесказанного были проанализированы несколько различных ПО, занимающихся анализом рисков и проверкой на соответствие стандартам, такие как:

1. DigitalSecurityOffice ГРИФ 2006.
2. COBRA.
3. CRAMM.
4. Callio Secura 17799.
5. Proteus Enterprise.
6. RA2 the art of risk.
7. RiskWatch.
8. vsRisk.
9. RiskAdvisor.
10. DigitalSecurityOffice КОНДОР 2006.

Проанализировав все источники, можно сделать вывод, что недостатки, свойственные многим программным продуктам, предназна-

ченным для управления рисками, ограничивают их практическое применение. Помимо этого, обнаружить продукт, лишенный всех недостатков и в то же время полностью соответствующий требованиям международных стандартов, достаточно сложно. Не говоря уже о том, что многие продукты, позиционируемые разработчиками как средства для оценки или управления рисками, на самом деле таковыми не являются, т.к. не реализуют ни методологии оценки рисков, ни алгоритма их вычисления, а предоставляют лишь средства представления и хранения данных о рисках, оставляя анализ и оценивание рисков, по существу, на откуп пользователю.

Многие известные продукты либо не позволяют проводить полноценной оценки рисков, а скорее являются средствами для анализа несоответствий требованиям стандарта ISO 27001, либо включают в себя слабые средства оценки рисков, не полностью соответствующие требованиям ISO 27001, хотя в них много другого функционала, либо являются слишком сложными в использовании, дорогими и некастомизируемыми.

ЛИТЕРАТУРА

1. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.

2. Петренко С.А. Анализ рисков в области защиты информации. СПб.: ООО «Издательский Дом «Афина», 2009. 153 с.

3. Петренко С.А., Панасенко С.П. Криптографические методы защиты информации для корпоративных систем // Экспресс-Электроника. 2002. № 2–3. С. 60–67.

4. Петренко С.А. Управление информационными рисками компании // Экспресс-Электроника. 2002. № 2–3. С. 106–113.

5. Программные продукты для анализа рисков [Электронный ресурс]. Режим доступа: http://www.iso27000.ru/informacionnye-rubriki/upravlenie-riskami/programmnye-produkty-dlya-analiza-riskov

6. Компьютерные программы, предназначенные для анализа рисков [Электронный ресурс]. Режим доступа: http://www.cfin.ru/forum/showthread.php?t=58613.

РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ

А.Ю. Якимук, студент каф. КИБЭВС

Научный руководитель В.Г. Миронова, м.н.с. каф. КИБЭВС

г. Томск, ТУСУР, ФБ, каф. КИБЭВС yakimuk-alex@mail.ru

В современном мире сложно представить организацию, в которой в силу выполнения должностных обязательств сотрудникам не приходится иметь дело с информацией ограниченного доступа. Это могут

быть и персональные данные работников или клиентов, и сведения о коммерческой деятельности организации, и многое другое. Знание данной информации при определенных условиях может предоставить некоторые преимущества или выгоды, и потому не удивительно, что они могут стать предметом интереса злоумышленников.

Для оказания противодействия возможному нарушению конфиденциальности сведений в организации принято вводить режим защиты информации. Это даст основания рассчитывать на то, что информация будет известна лишь тем лицам, которые были допущены до нее, а в случае нарушения режима – на судебную защиту. В ином случае суд признает информацию открытой, и претензии по поводу разглашения окажутся безосновательными. Чтобы такого не произошло, необходимо своевременно ввести режим конфиденциальности в организации.

В Федеральном законе №98 «О коммерческой тайне» отдельно рассказывается о том, как должна быть организована защита информации, попадающей под действие этого закона. Однако, кроме этого, существует еще 5 групп сведений, доступ к которым ограничен, и не существует конкретной методики по введению режима защиты данных видов тайны. В частности, для служебной тайны не существует отдельного закона, регулирующего работу с ней. Однако если прочесть обсуждения работников, столкнувшихся с проблемой введения режима конфиденциальности, то можно понять, что введение режима служебной тайны или любой другой во многом схоже с введением режима коммерческой.

Введение режима конфиденциальности в первую очередь потребует создания перечня сведений ограниченного доступа и публикации его в составе приказа об обеспечении охраны информации ограниченного доступа, ряда должностных инструкций и других документов, направленных на поддержание конфиденциальности в организации. Отдельный документ должен содержать порядок получения допуска к защищаемой информации и методов контроля по соблюдению введенного режима [1].

Инструкция по обеспечению конфиденциальности информации будет самым содержательным актом, поскольку этот документ включает в себе все аспекты по поддержанию режима. В этой инструкции необходимо регламентировать методику снятия и присвоения грифа сведениям ограниченного доступа, ограничения и обязанности сотрудников, порядок допуска сотрудников к охраняемым сведениям и правила обращения с документами, содержащими их, методику контроля соблюдения режима конфиденциальности и ответственность за ее нарушение.

Во-вторых, необходимо, чтобы сотрудники, выполняющие работы с информацией ограниченного доступа, быть ознакомлены с перечнем

сведений, разглашение которых запрещено с точки зрения законодательства и устанавливаемой политики компании, вводимыми режимом конфиденциальности условиями работы и мерами ответственности за их нарушение.

Тот факт, что сотрудник был ознакомлен и дал согласие работать в соответствии с вводимыми изменениями, должен закрепляться документально в соответствующем соглашении. Каждый сотрудник должен подтвердить тот факт, что он прочел правила работы с защищаемой информацией и предупрежден об ответственности в случае нарушения их конфиденциальности. В свою очередь, от работодателя потребуется создать достаточные условия для осуществления сотрудниками должностных обязательств в рамках устанавливаемого режима.

Все документы, которые содержат информацию ограниченного доступа, должны пройти маркировку и получить соответствующий гриф, ссылающийся на обладателя сведений и сотрудника, на которого ложится обязанность обеспечения сохранности информации.

Следующим этапом можно организовать ограничение доступа к конфиденциальным сведениям. Это потребует проведения учета лиц, которым был предоставлен доступ к сведениям ограниченного доступа или они были получены до введения режима конфиденциальности. Попутно назначаются сотрудники, которые будут отвечать за сохранность информации и контролировать соблюдение режима конфиденциальности [2].

В случае выполнения всех вышеуказанных процедур считается, что режим конфиденциальности принят. Это, разумеется, не значит, что конфиденциальность сведений будет гарантирована. Однако, это позволяет рассчитывать на соблюдение режима конфиденциальности в организации или судебную защиту и возмещение возможного ущерба в случае его нарушения.

ЛИТЕРАТУРА

1. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне». КонсультантПлюс [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_116684/, свободный.

2. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. СПб.: Юридический центр Пресс, 2001. 789 с.

СОДЕРЖАНИЕ

СЕКЦИЯ 16

ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ

*Председатель секции – **Ходашинский И.А.**, профессор каф. КИБЭВС, д.т.н., зам. председателя – **Костюченко Е.Ю.**, доцент каф. КИБЭВС, к.т.н.*

СЕКЦИЯ 17

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 18

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 – **Конев А.А.**, доцент каф. КИБЭВС, к.т.н.*

ДЛЯ ЗАМЕТОК

Научное издание

Материалы
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2014»

14–16 мая 2014 г., г. Томск

В пяти частях

Часть 3

Корректор – **В.Г. Лихачева**
Верстка **В.М. Бочкаревой**

Издательство «В-Спектр»
Сдано на верстку 01.04.2014. Подписано к печати 30.04.2014.
Формат 60×84 1/16. Печать трафаретная. Печ. л. 16,6.
Тираж 500 экз. Заказ 11.

Издательство «В-Спектр»
ИП Бочкарева В.М. ИНН 701701817754
634055, г. Томск, пр. Академический, 13–24, т. 49-09-91.
E-mail: bvm@sibmail.com