ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ
ПРИГЛАШАЕТ

50 ЛЕТ
ТУСУР

Лицензия серия А №282322 от 21.05.08

РАДИОТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ (РТФ), dekanat-rtf@tusur.ru
РАДИОКОНСТРУКТОРСКИЙ ФАКУЛЬТЕТ (РКФ), rkf@main.tusur.ru
ФАКУЛЬТЕТ ЭЛЕКТРОННОЙ ТЕХНИКИ (ФЭТ), dekanat-fet@tusur.ru
ФАКУЛЬТЕТ СИСТЕМ УПРАВЛЕНИЯ (ФСУ), dekanat-fsu@tusur.ru
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ (ФВС), fvs@fet.tusur.ru
ГУМАНИТАРНЫЙ ФАКУЛЬТЕТ (ГФ), tis@main.tusur.ru
ЭКОНОМИЧЕСКИЙ ФАКУЛЬТЕТ (ЭФ), dekanat-ef@tusur.ru
ЗАОЧНЫЙ И ВЕЧЕРНИЙ ФАКУЛЬТЕТ (ЗиВФ), zvf@main.tusur.ru
ФАКУЛЬТЕТ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ (ФИТ), in@sbi.tusur.ru
ФАКУЛЬТЕТ МОДЕЛИРОВАНИЯ СИСТЕМ (ФМС), decan@toe.tusur.ru
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ (ЮФ), tib@mail.tomsknet.ru
ФАКУЛЬТЕТ ДИСТАНЦИОННОГО ОБУЧЕНИЯ (ФДО), office@fdo.tusur.ru

г.Томск, пр.Ленина, 40
Сайт: www. tusur.ru Эл. почта: onir@main.tusur.ru
Телефон приемной комиссии: (3822) 513-226

Представитель ТУСУРа

ТУСУР

НАУЧНАЯ СЕССИЯ ТУСУР–2012

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

посвященной 50-летию ТУСУРа

16–18 мая 2012 г. (В пяти частях)

ЧАСТЬ 3

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–2012

Материалы

Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2012», посвященной 50-летию ТУСУРа

16–18 мая 2012 г., г. Томск

В пяти частях

Часть 3

В-Спектр
2012

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

Н 34 **Научная сессия ТУСУР–2012:** Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 16–18 мая 2012 г. – Томск: В-Спектр, 2012: В 5 частях. – Ч. 3. – 300 с.

ISBN 978-5-91191-246-8
ISBN 978-5-91191-249-9 (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 защите информации. Представлены статьи по математическому моделированию в технике, экономике и менеджменте, антикризисному управлению, автоматизации управления в технике и образовании, а также работы, касающиеся социокультурных проблем современности, экологии, мониторинга окружающей среды и безопасности жизнедеятельности.

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

ISBN 978-5-91191-246-8
ISBN 978-5-91191-249-9 (Ч. 3)

© Том. гос. ун-т систем управления
и радиоэлектроники, 2012

Всероссийская научно-техническая конференция студентов и молодых ученых «Научная сессия ТУСУР–2012», *посвященная 50-летию ТУСУРа*

16–18 мая 2012 г.

ПРОГРАММНЫЙ КОМИТЕТ

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

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

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

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

СЕКЦИИ КОНФЕРЕНЦИИ

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

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

Секция 3. Аудиовизуальная техника, бытовая радиоэлектронная аппаратура и сервис. Председатель секции – Пустынский Иван Николаевич, зав. каф. ТУ, проф., д.т.н.; зам. председателя – Костевич Анатолий Геннадьевич, с.н.с. каф. ТУ НИЧ, к.т.н.

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

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

Секция 6. 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, доцент, д.т.н.; зам. председателя – Семенов Эдуард Валерьевич, доцент каф. РЗИ, к.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 – Ворошилин Евгений Павлович, зав. каф. ТОР, к.т.н.; зам. председателя – Белов Владимир Иванович, доцент каф. ТОР, к.т.н.

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

Секция 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 Дмитрииевич, проф., зам. зав. каф. ПрЭ по НР, к.т.н.

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

Подсекция 13.1. Распределённые информационные технологии и системы. Председатель секции – Ехлаков Юрий Поликарпович, проректор по информатизации и управлению ТУСУРа, зав. каф. АОИ, проф., д.т.н.; зам. председателя – Сенченко Павел Васильевич, декан ФСУ, доцент каф. АОИ, к.т.н.

Подсекция 13.2. Современные библиотечные технологии. Председатель секции – Абдрахманова Марина Викторовна, директор библиотеки ТУСУРа; зам. председателя – Карауш Александр Сергеевич, доцент каф. РЗИ, к.т.н.

Секция 14. Информационно-измерительные приборы и устройства. Председатель секции – Черепанов Олег Иванович, проф. каф. ЭСАУ, д.ф.-м.н.; зам. председателя – Шидловский Виктор Станиславович, доцент каф. ЭСАУ, к.т.н.

Секция 15. Вычислительный интеллект. Председатель секции – Ходашинский Илья Александрович, проф. каф. КИБЭВС, д.т.н.; зам. председателя – Лавыгина Анна Владимировна, ст. преп. каф. АОИ, к.т.н.

Секция 16. 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 16.1. Интеллектуальные системы проектирования технических устройств. Председатель секции – Черкашин Михаил Владимирович, декан ФВС, доцент каф. КСУП, к.т.н.

Подсекция 16.2. Адаптация математических моделей для имитации сложных технических систем. Председатель секции – Коцубинский Владислав Петрович, доцент каф. КСУП, к.т.н.

Подсекция 16.3. Инструментальные средства поддержки автоматизированного проектирования и управления. Председатель секции – Рыбалка Евгений Николаевич, ст. преп. каф. КСУП.

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, зав. каф. КИБЭВС, проф., д.т.н.; зам. председателя – Мещеряков Роман Валерьевич, зам. начальника НУ, зам. зав. каф. КИБЭВС по НР, доцент, 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. ФЭ, к.ф.-м.н.

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

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

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

Секция 23. Актуальные проблемы социальной работы в современном обществе. Председатель секции – Грик Николай Антонович, зав. каф. ИСР, проф., д.ист.н.; зам. председателя – Баранова Мария Николаевна, инженер каф. ИСР.

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 – Чекчеева Наталья Валерьевна, зам. директора Института инноватики, к.э.н.

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

Секция 26. Современные информационные технологии. Открытия. Творчество. Проекты. Председатель секции – Смолонская Марина Александровна, ведущий специалист НОУ «Открытый молодежный университет»; зам. председателя –

Бесклубов Станислав Владимирович, ведущий специалист НОУ «Открытый молодежный университет».

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 – 8–14-я секции;
3-й том – 15, 17, 18-я секции;
4-й том – 16, 19, 20-я секции;
5-й том – 21–26-я секции.

СЕКЦИЯ 15

ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ

*Председатель – **Ходашинский И.А.**, профессор каф. КИБЭВС, д.т.н.,*
*зам. председателя – **Лавыгина А.В.**, ст. преп. каф. АОИ, к.т.н.*

СТРУКТУРА ПРОДУКЦИОННОЙ СИСТЕМЫ ВЫБОРА ПРОГРАММНЫХ ПРОДУКТОВ СИСТЕМЫ «1С:ПРЕДПРИЯТИЕ 8»

А.В. Ахаев*, *аспирант каф. КИБЭВС
Научный руководитель И.А. Ходашинский, проф. каф. КИБЭВС, д.т.н.
г. Томск, ТУСУР, AkhaevAV@gmail.com

На сегодняшний момент существует большое количество различных конфигураций программных продуктов фирмы «1С», которые ориентированы на автоматизацию работы предприятий в самых разнообразных областях. Существует проблема выбора такой конфигурации, которая в наибольшей степени будет удовлетворять потребностям заказчика.

Продукционная система. Для решения данной проблемы предлагается продукционная система выбора программных продуктов системы «1С: Предприятие 8» [1]. Система призвана решать следующие задачи: помощь в выборе оптимальной конфигурации как менеджеру по продажам данных программных продуктов, так и заказчику; предоставление необходимой информации по конфигурациям. Структура системы представлена на рис. 1.

Рассмотрим каждую структурную часть системы.

Интерфейс пользователя. Экспертная система будет работать в нескольких режимах: как Web-приложение, исполняемое в среде интернет-браузера (*Windows Internet Explorer*, *Mozilla Firefox*, *Google Chrome* или *Safari*) и как обычное клиентское приложение, исполняемое в операционной системе компьютера. Первый режим предназначен для использования заказчиком (зарегистрированным пользователем), второй – для использования менеджером. В обоих случаях на этапе ввода информации реализуется диалог пользователя с системой в режиме «вопрос – ответ». В системе хранится информация о пользователях, в связи с этим некоторые вопросы могут «опускаться». При получении результатов заказчик имеет некоторые ограничения – ему не-

доступна подсистема анализа функциональных возможностей конфигураций. Доступ можно получить по специальному запросу.

Рис. 1. Структура продукционной системы

База знаний (*БЗ*). Знания в системе представлены в виде продукционных правил. Правила формируются с использованием языка, разработанного специально для рассматриваемой предметной области. В структурную основу данного языка лег язык *OPS*5. Семантической основой языка является классификация, опирающаяся на онтологический подход [1].

Механизм логического вывода (*МЛВ*) Механизм вывода, как и в классической продукционной системе, работает в режиме «распознавание – действие», воспринимая совокупность известных фактов и выстраивая новые заключения.

Подсистема объяснений. Данная подсистема позволяет пользователю после получения результата выяснить, как и почему получено то или иное решение.

Подсистема анализа функциональных возможностей конфигураций. Подсистема предоставляет менеджеру сравнительный анализ функциональных возможностей конфигураций, полученных по результатам работы МЛВ.

Интеллектуальный редактор. Редактор предоставляет инженеру по знаниям (специалисту в представлении знаний) возможность редактировать существующую базу знаний или создавать новую. При редактировании БЗ можно использовать как разработанный конструктор, так и непосредственно язык представления знаний. Также существует возможность редактирования состава вопросов, которые система задает пользователю на этапе ввода информации.

Кроме того, в интеллектуальном редакторе имеется модуль приобретения знаний, предназначенный для поддержания БЗ в актуальном состоянии. В качестве источника знаний выступают информационные

письма фирмы «1С» (инфописьма) о выпуске программных продуктов в виде текстовых документов. Инфописьма обрабатываются с использованием онтологического подхода [2].

Реализация. При построении экспертных систем возможно применение как языков программирования различного уровня, так и оболочек (пустых, скелетных) экспертных систем. Оболочки имеют общую направленность и не учитывают особенности исследуемой предметной области. Прототип продукционной системы реализован на платформе «1С: Предприятие 8» с использованием разработанного языка описания базы знаний.

Платформа поддерживает два варианта работы: файловый и клиент-серверный. Продукционную систему целесообразно использовать в клиент-серверном варианте, так как он предназначен для масштабного использования. Этот вариант реализован на основе трехуровневой архитектуры «клиент-сервер». Информационная база хранится в одной из поддерживаемых систем управления базами данных (СУБД) (Microsoft SQL Server, PostgreSQL, IBM DB2 или Oracle Database), а взаимодействие между клиентским приложением и СУБД осуществляет кластер серверов «1С: Предприятия 8» [3].

Для обеспечения работы экспертной системы в режиме Web-приложения требуется Web-сервер (Apache или IIS), настроенный на работу с платформой «1С: Предприятие 8». Интернет-браузер взаимодействует с Web-сервером по протоколу HTTP. Web-сервер, в свою очередь, взаимодействует с «1С: Предприятием 8».

Для обеспечения работы экспертной системы в обычном клиентском приложении дополнительных настроек не требуется.

Заключение. Таким образом, была предложена технология, предназначенная для выбора программных продуктов системы «1С: Предприятие 8». На основе данной технологии предложен инструмент хранения и обработки знаний – Web-ориентированная продукционная система. Для актуализации знаний системы требуются только инженеры по знаниям, инфописьма и в некоторых случаях эксперты – носители знаний о предметной области.

ЛИТЕРАТУРА

1. Адуева Т.В., Ахаев А.В., Ходашинский И.А. Продукционная система выбора программных продуктов системы «1С: Предприятие 8» // Бизнес-информатика. 2012. №1(19).

2. Гаврилова Т.А. Онтологический подход к управлению знаниями при разработке корпоративных систем автоматизации // Новости искусственного интеллекта. 2003. № 2.

3. Официальный сайт системы программ «1С: Предприятие 8» [Электронный ресурс]. Режим доступа к сайту: http://www.v8.1c.ru

ПЛАНИРОВАНИЕ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ РОБОТОМ-МАНИПУЛЯТОРОМ

Е.В. Батурина*, *студент 5-го курса
Научный руководитель А.Н. Горитов, д.т.н., профессор
г. Томск, ТУСУР, каф. АСУ, Baturina_E.V@mail.ru

Все более важную роль в нашей жизни начинают занимать роботы. Их развитие не останавливается ни на минуту. Роботы помогают людям в производстве, научных лабораториях, получают широкое применение при выполнении спасательных работ в экстремальных ситуациях.

Области робототехники тесно связаны с искусственным интеллектом. Одним из важных направлений искусственного интеллекта является создание интеллектуальных роботов, способных автономно совершать операции по достижению целей, поставленных человеком [1]. Интеллектуальные роботы способны воспринимать и распознавать объекты окружающей среды, формировать ее внутреннее представление, протекающие процессы, изменять обстановку окружающей среды путем манипулирования с ее объектами.

В данной работе описывается функционирование интеллектуального робота, который, получив заявку (задание), самостоятельно определяет последовательность действий для ее выполнения. Имеются контейнеры одного размера, которые располагаются на заданной поверхности друг на друге, образуя стеки. Робот-манипулятор может взять любой свободный контейнер (тот, который не имеет контейнера на своей верхней грани) и переместить его на свободную поверхность или на верхнюю грань любого другого свободного контейнера (рис. 1).

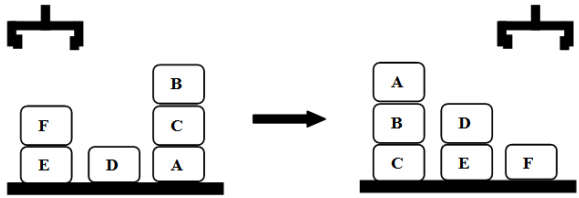


Рис. 1. Пример начального и целевого состояния задачи

Задача состоит в том, чтобы разработать и реализовать метод, минимизирующий число перестановок контейнеров при выполнении заявки, при этом контейнеры должны передаваться на выход в строгом соответствии с имеющимся заданием.

Для решения задачи используются алгоритмы поиск пространства состояний. Совокупность всех возможных состояний образует множе-

ство S. Способы перемещения контейнеров роботом должны быть подчинены некоторым требованиям: контейнеры можно устанавливать друг на друга; для перемещения робот должен выбрать контейнер, лежащий сверху; высота стека из контейнеров ограничена и т.д. На основе требований строится множество F допустимых операторов, которые фактически являются совокупностью разрешенных действий робота. Желаемое расположение контейнеров на поверхности есть целевое состояние. Решением задачи является последовательность действий робота (цепочка операторов F_1, …, F_2), с помощью которой можно переставить контейнеры из некоторого начального расположения (начального состояния S_0) в желаемое (целевое состояние G). Таким образом, задача, определяется тройкой (S_0, F, G).

Описания состояний могут представлять собой строки символов, векторы, двухмерные массивы, деревья, списки и т. п. Наилучшим способом представления является дерево поиска, так как в данной структуре отсутствует возможность образования петель и циклов. Поэтому поиск на деревьях выигрывает в эффективности.

Для построения дерева поиска состояния используются операторы из F, применимые к корню дерева (начальное состояние), строятся вершины первого уровня. Затем, используя операторы из F, применимые к вершинам первого уровня, строятся вершины следующих уровней. Для всех вершин производится проверка соответствия целевому состоянию. От каждой последующей вершины к породившей ее идут указатели, которые позволяют найти путь назад от целевой вершины к начальной [2]. Состояния могут быть достигнуты различными путями. Важно в этом случае выбрать оптимальный путь решения задачи.

Известными алгоритмами поиска пространства состояния являются поиск в ширину, поиск в глубину и эвристический поиск [3, 4]. В результате сравнительного анализа был выбран эвристический поиск, так как он позволяет обеспечивать возможность ранжирования вершин с тем, чтобы выделить ту вершину, которая с наибольшей вероятностью находится на лучшем пути к цели. Основная идея алгоритма заключается в упорядочении списка открытых вершин в соответствии с некоторой мерой, оценивающей «перспективность» вершины или пути, на котором находится данная вершина. Такую меру называют оценочной функцией. Для раскрытия вершины выбирается вершина, имеющая минимальное значение оценочной функции. После каждого шага раскрытия производится переупорядочение вершин в списке в соответствии со значениями оценочной функции. В качестве оценочной функции используется функция $\hat{f}(v) = \hat{g}(v) + \hat{h}(v)$, где $\hat{g}(v)$ – длина пути в дереве состояний от начальной вершины до вершины v; $\hat{h}(v)$ – эвристическая функция – сумма числа контейнеров, расположенных не

на своем месте, и общего числа контейнеров, препятствующих установлению каждого из них на свое место. Препятствующими считаются контейнеры, расположенные сверху какого-либо другого контейнера, который нужно переставить, и контейнеры, расположенные не на своем месте в целевом состоянии.

Используя рассмотренный метод, система управления робота может планировать его действия для выполнения поставленной задачи.

Задача довольно нетривиальная, поэтому для ее решения необходимо затратить определенные усилия.

ЛИТЕРАТУРА

1. Поспелов Г.С. Искусственный интеллект – основа новой информационной технологии. М.: Наука, 1988.

2. Лорьер Ж.-Л. Системы искусственного интеллекта: Пер. с франц. М.: Мир, 1991. 568 с.

3. Нильсон Н. Искусственный интеллект. Методы поиска решения: Пер.с англ. М.: Мир, 1973. 273 с.

4. Рассел С., Норвиг П. Искусственный интеллект: современный подход: 2-е изд.; пер. с англ. М.: Изд. дом «Вильямес», 2006. 1408 с.

ХАОТИЧЕСКИЙ И КВАНТОВЫЙ АЛГОРИТМ РОЯЩИХСЯ ЧАСТИЦ ДЛЯ НАСТРОЙКИ ПАРАМЕТРОВ НЕЧЁТКИХ СИСТЕМ

И.Ю. Белоногов*, *студент 5-го курса

г. Томск, ТУСУР, Igor12345@sibmail.com

К задачам параметрической идентификации параметров нечетких систем относятся нахождение оптимальных значений параметров антецедентов и консеквентов правил. В данной работе рассмотрено решение указанной задачи при помощи модификаций алгоритма роящихся частиц (АРЧ).

Алгоритм роящихся частиц – это метод поиска, основанный на итеративном взаимодействии частиц, образующих рой.

Хаотический метод роящихся частиц. Для этого метода в алгоритм вводится коэффициент *Score:*

$$Score_u(t) = \frac{f(x_{worst}(t)) - f(x_u(t))}{f(x_{worst}(t)) - f(x_{best}(t))},$$

где $x_{worst}(t)$ и $x_{best}(t)$ – векторы, содержащие худшую и лучшую позиции частицы в единицу времени t [1].

Этот коэффициент влияет на коэффициент инерции, который теперь должен вычисляться для каждой частицы в отдельности:

$$w_u(t) = w_{low}(t) + (w_{high}(t) - w_{low}(t)) \times (1 - Score_j(t)),$$

где $w_{low}(t)$ и $w_{high}(t)$ – низшая и наивысшая границы инертного веса в единицу времени *t*.

Формулы для расчёта векторов v_i и x_i:

$$\mathbf{v}_i(k+1) = w \cdot \mathbf{v}_i(k) + c_1 \cdot rand \cdot (\mathbf{p}_i(k) - \mathbf{x}_i(k)) + c_2 \cdot Rand \cdot (\mathbf{p}_g(k) - \mathbf{x}_i(k)),$$

$$\mathbf{x}_i(k+1) = \mathbf{x}_i(k) + \mathbf{v}_i(k+1),$$

где i = 1, 2, …, N; $\mathbf{v}_i(k)$ – вектор скорости частицы i на итерации k; $\mathbf{x}_i(k)$ – координаты частицы i на итерации k; c_1, c_2 – эмпирические константы ускорения из интервала [1.4, 2]; $p_i(k)$ – лучшая позиция частицы i на первых k итерациях; $p_g(k)$ – лучшая позиция частицы в рое (задается индексом g) на первых k итерациях; w – эмпирический коэффициент инерции из интервала [0.7, 1.2]; *rand*, *Rand* – случайное число из интервала [0, 1].

Используем хаотические последовательности для сдвига координат частиц [1]:

1. Logistic Map:

$x_{k+1} = 4x_k(1 - x_k)$ с начальным значением $x_0 = 0.2027$.

2. Tent Map:

$$x_{k+1} = G(x_k)$$

$$G(x) = \begin{cases} \frac{x}{0.7}, & if\ f(x < 0.7), \\ \frac{x(1-x)}{0.3}, & otherwise. \end{cases}$$

Начальное значение зафиксировано на $x_0 = 0.27$.

3. Sinusoidal Iterator:

$$x_{k+1} = 2.3x_k^2 sin(\pi x_k) \text{ с } x_0 = 0.7.$$

4. Gauss Map:

$$x_{k+1} = G(x_k) \quad \text{с} \quad G(x) = \begin{cases} 0, & if\ f(x = 0), \\ \frac{1}{x} mod 1, & x \in (0, 1). \end{cases}$$

Хаотический алгоритм роящихся частиц (ХАРЧ).

Шаг 1. Задание параметров алгоритма: $\boldsymbol{v}_i(0) = 0$ c_1, c_2, $w(0)$, N или минимальное значение ошибки.

Шаг 2. Генерация роя случайным образом, k =1.

Шаг 3. Оценка каждой частицы роя путем вычисления ошибки. Если достигнуто условие окончания работы (количество итераций, значение ошибки), то переход на шаг 6.

Шаг 4. Хаотический сдвиг случайной координаты случайной частицы по заданной хаотической последовательности.

Шаг 5. Для каждой частицы определение ее информационного индекса *Score*(*k*+1), коэффициента инерции *w*(*k*+1), вектора скорости $\boldsymbol{v}_i(k+1)$ и новых координат $\boldsymbol{x}_i(k+1)$.

Шаг 6. Расчет новых лучших позиций каждой частицы $\boldsymbol{p}_i(k+1)$. Определение частицы с лучшей позицией в рое $\boldsymbol{p}_g(k+1)$. Определение новых максимальных и минимальных ошибок каждой частицы.

k=*k*+1; переход к шагу 3.

Шаг 7. Окончание работы.

Квантовый метод роящихся частиц. Частицы имеют квантовое поведение и описываются лишь их координатами [2]:

$$x(t+1) = p \pm \beta * |\text{mbest} - x(t)| * \ln\left(\frac{1}{u}\right).$$

$$\text{mbest} = \frac{1}{M}\sum_{i=1}^{M}\boldsymbol{p}_i = \left(\frac{1}{M}\sum_{i=1}^{M}p_{i1}, \frac{1}{M}\sum_{i=1}^{M}p_{i2}, \ldots, \frac{1}{M}\sum_{i=1}^{M}p_{iD}\right),$$

где M – вектор, который является средним арифметическим лучших позиций всех частиц в рое; $p = (p1, p2, ..., pD)$ – вектор, называемый местным привлекателем, где

$$p_d = \varphi * p_{id} + (1-\varphi) * p_{gd}, \quad 0 < \varphi < 1,$$

а β – параметр, который называется коэффициентом сокращения и расширения – вещественное число из интервала [0; 1].

Предложен способ решения проблемы с преждевременной сходимостью квантового метода роящихся частиц – общественный метод. В данном методе рой делится на два подроя по значениям их качеств – обычные частицы и элитные частицы. Если частица относится к обычному подрою, она будет работать по квантовому алгоритму. Элита же работает по своему методу: генерируется мутированный вектор:

$$\boldsymbol{v}_i = \boldsymbol{p}_j + \delta_2, \qquad \delta_N = \frac{\sum_{l=1}^{N}\Delta_l}{N},$$

где $\boldsymbol{x}_{r_1}, \boldsymbol{x}_{r_2}$ $\Delta_l = \boldsymbol{x}_{r_1} - \boldsymbol{x}_{r_2}$, в котором r – частицы, случайно выбранные из обычного подроя. Генерируется пробный вектор $\boldsymbol{u}_i$ смешиванием целевого вектора $\boldsymbol{x}_i$ и соответствующего мутированного вектора $\boldsymbol{v}_i$ под предопределённым перемешивающим значением $Cr \in [0, 1]$. Для d-мерного пространства $\boldsymbol{u}_i$:

$$u_{id} = \begin{cases} v_{id} & \text{if rand()} < \text{Cr or } d = k, \\ x_{id} & \text{otherwise,} \end{cases}$$

где k – это случайное целочисленное значение из интервала $[1, D]$.

Если пробный вектор $\boldsymbol{u}_i$ имеет более лучшие значения ошибки, чем у соответствующего ему целевого вектора $\boldsymbol{x}_i$, он заменяет целевой вектор $\boldsymbol{x}_i$ в следующем поколении, в противном случае целевой вектор $\boldsymbol{x}_i$ остаётся [2].

Квантовый алгоритм роящихся частиц (КАРЧ)

Шаг 1. Задание параметров алгоритма: *Cr*, β(0), *N*, β(N) и минимальное значение ошибки.

Шаг 2. Генерация роя случайным образом, k =1.

Шаг 3. Рассчитать значение *mbest* для всего роя.

Шаг 4. Оценка каждой частицы роя путем вычисления ошибки. Если достигнуто условие окончания работы (количество итераций, значение ошибки), то переход на шаг 6.

Шаг 5. Выбрать элитный подрой.

Шаг 6. Если частица не принадлежит элитному подрою, то для каждой частицы определить ее новый коэффициент сокращения и расширения $\beta(k+1)$ и новые координаты $\boldsymbol{x}_i(k+1)$.

Шаг 7. Если частица принадлежит элитному подрою, то рассчитать существенный вектор разницы Δl, рассчитать мутированный вектор $v_{i,}$ он смешивается с целевым вектором x_i под перемешивающим значением *Cr*.

Шаг 8. Расчет новых лучших позиций каждой частицы $\boldsymbol{p}_i(k+1)$. Определение частицы с лучшей позицией в рое $\boldsymbol{p}_g(k+1)$.

$k = k$ +1; переход к шагу 3.

Шаг 9. Окончание работы.

Эксперимент. Были проведены эксперименты на реальных данных из репозитория KEEL. В таблице представлены результаты работы при решении проблемы ele-1 и сравнение их с данными, взятыми из [3].

Результаты сравнений работы алгоритмов

Алгоритм	Число правил	Ошибка обучения	Ошибка тестовая
КАРЧ	**16**	**335388**	**382578**
ХАРЧ	**16**	**309593**	**394136**
COR-BWAS	22,0	354304	417142
Thrift	46,4	335086	435373
Pittsburgh	17,2	342464	738691
Pitts-DNF min	2,0	767922	760271
Pitts-DNF med	8,2	344636	415266
Pitts-DNF max	14.0	330496	440692

Заключение. Приведенные две модификации, работая с относительно маленьким количеством правил, позволяют достичь неплохих результатов в решении проблемы *ele*-1.

ЛИТЕРАТУРА

1. Zhihua C., Xingjuan C., Jianchao Z. Chaotic Performance-Dependent Particle Swarm Optimization // Division of System Simulation and Computer Application. Taiyuan University of Science and Technology. China. 10 p.

2. Yang K., Maginu K., Nomura H. Cultural algorithm-based quantum-behaved particle swarm optimization // International Journal of Computer Mathematics. 2010. Vol. 87, No. 10. P. 2143–2157.

3. Casillas J., Martinez P., Benitez A. // Learning consistent, complete and compact sets of fuzzy rules in conjunctive normal form for regression problems. 2 September. 2008. P. 451–465.

ЯДРО АВТОМАТИЗИРОВАННОЙ ТЕСТИРУЮЩЕЙ СИСТЕМЫ

В.А. Дель, студент 3-го курса каф. КИБЭВС

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

г. Томск, ТУСУР, ФВС, Rush.vr@gmail.com

«Ядра – чистый изумруд!»
Пушкин А.С.

Проблема автоматизированного тестирования программ неоднократно поднималась, поэтому в данной работе мы не будем рассматривать необходимость создания такой системы. Вместо этого мы рассмотрим математическую модель ядра подобных систем.

Пусть необходимо оценить, является ли конкретное решение корректным. Для этой оценки введем некоторые обозначения:

S – множество решений, т.е. программ, написанных на каком-либо языке программирования; O – множество всех выводов решений; T – множество всех тестовых случаев.

Пусть $s \in S,\ t \in T$.

Введем отображение

$$f : S \times T \to 0.$$

Смысл данного отображения заключается в том, что каждой паре <решение, тест> мы сопоставляем единственный вывод.

Предположим, что для каждого тестового случая существует единственный ответ, и введем следующее отображение

$$A : T \to 0,$$

которое каждому тестовому случаю сопоставляет верный ответ. Здесь стоит заметить, что в данной работе мы рассматриваем только задачи, для которых существует ответ.

Таким образом, исходя из заданного предположения, решение будет являться верным тогда и только тогда, когда будет выполняться условие

$$f(s,t)=A(t)\forall t\in T\,.$$

Итак, мы научились определять, является ли программа корректной в предположении единственности ответа.

Проблема заключается в том, что это предположение не всегда является верным. Существует круг задач, для которых возможно несколько верных вариантов ответа. Причем множество верных ответов может быть как конечным, так и бесконечным.

Доказательством такого странного на первый взгляд утверждения является, например, следующая задача:

Задано натуральное число X, $X < 10^9$. Требуется найти натуральное число Y, удовлетворяющее следующим условиям:

1. $Y > X$.
2. $Y \equiv 1 \bmod 2$.

Очевидно, что такая задача может иметь множество верных ответов. Как же теперь определять, является ли решение корректным?

Для решения данной проблемы изменим отображение *A* следующим образом:

$$A:T\times 0\to\{0,1\}\,.$$

Смысл данного отображения заключается в следующем: паре <тест, ответ> мы сопоставляем «1» тогда и только тогда, когда ответ может являться верным для заданного теста. В противном случае данной паре мы сопоставляем «0».

Таким образом, программа является корректной тогда и только тогда, когда выполняется следующее соотношение:

$$A(t,f(s,t))=1\,.$$

Итак, с математической моделью мы определились. Однако в процессе применения данной модели к реальной системе возникают новые обстоятельства.

Для одной и той же задачи может существовать целое множество различных решений. Эти решения могут быть как оптимальными, так и неоптимальными.

В качестве примера возьмем задачу коммивояжера. У данной задачи есть простое переборное решение, трудоемкость которого составляет O(*n!*) [1], где *n* – число вершин в графе. Для 10 вершин такое решение выполнится за разумное время. Однако уже для 20 вершин такое решение будет работать около 700 лет! Очевидно, необходимо отсечь подобные неоптимальные по времени и памяти решения. Для этого в каждой задаче вводится ограничение используемого времени и используемой памяти. Если программа превышает заданный лимит ресурса, то она завершается и считается неоптимальной.

Итак, в функционал ядра разработанной нами тестирующей системы входят:

1) Сборка решения;
2) Запуск решения на наборе тестов с ограниченными ресурсами;
3) Определение корректности решения.

Сборка решения производится с помощью скрипта build.bat, на вход которому подается имя исходного файла и номер компилятора. На данный момент поддерживаются 5 компиляторов:

- Microsoft Visual C++ 10.0
- GNU C++
- GNU C
- Java 1.7 SE
- Delphi 7

За запуск решения на наборе тестов отвечает инструмент run.exe, являющийся свободным программным обеспечением. Именно этот инструмент позволяет отслеживать количество затраченного времени и используемой памяти.

За определение корректности решения отвечают специальные программы, т.н. верификаторы. Существуют три стандартных верификатора – пословное сравнение, посимвольное сравнение и сравнение вещественных чисел с заданной точностью.

Если же верный ответ не является единственным, то пользователю предоставляется возможность создать свой верификатор на языке программирования C++. Для этого существует специальная библиотека testlib.h, которая предоставляет достаточный для создания верификаторов набор функций.

Таким образом, математическая модель с введенными ограничениями применяется к реальным тестирующим системам, в результате чего мы получаем стабильный инструмент для оценки правильности решений.

Проект ГПО КИБЭВС-1102 – «Программное обеспечение для организации и проведения спортивного программирования».

ЛИТЕРАТУРА

1. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: Построение и анализ. 2-е изд. М.: Вильямс, 2010 С. 90–95.

СИСТЕМА РАСПОЗНАВАНИЯ ГЛАСНЫХ ЗВУКОВ В РЕЧЕВЫХ СИГНАЛАХ

С.А. Елистратов, А.А. Чичерин, М.А. Косенко, студенты 4-го курса
Научные руководители Е.М. Давыдова, доцент;
Е.Ю. Костюченко, доцент
г. Томск, ТУСУР, каф. КИБЭВС, ФВС

Предположена методика распознавания гласных звуков с использованием ИНС.

Целью работы является создание системы для распознавания звуков, область возможного дальнейшего применения обширна. Для распознавания предполагается использование нейронной сети [1, 2] произвольной топологии, представленной на рис. 1. Для построения нейронной сети используется среда MatLab [3].

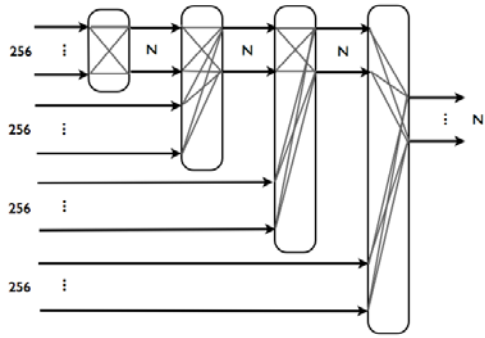


Рис. 1. Архитектура ИНС

Входные параметры формируются наложением маски, выделяющей несущую часть, на спектр сигнала. В связи с большими затратами ресурсов компьютера при работе с нейронной сетью требуется ограничить количество входных параметров. Для этого визуально, по спектру, выделяется значимая часть сигнала, находящаяся после переходного процесса установления звука и используется четыре отсчета маскированного сигнала (рис. 2).

Выходными данными является вектор нулей и единиц, классифицирующий фонему. В данной работе для ограничения количества фонем выбраны только гласные звуки русского языка, произнесенные одним диктором.

В соответствии с теорией [4] после выделения формант звука в одном отсчете (рис. 3) по соотношению частот формант можно определить звук. В данной работе предполагается использовать четыре отсчета для распознавания гласных звуков русского языка.

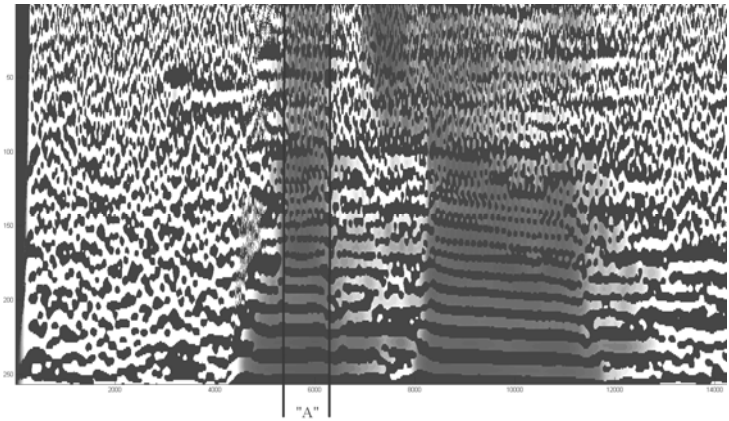


Рис. 2. Значимая часть гласной «А» в слове «Начало»

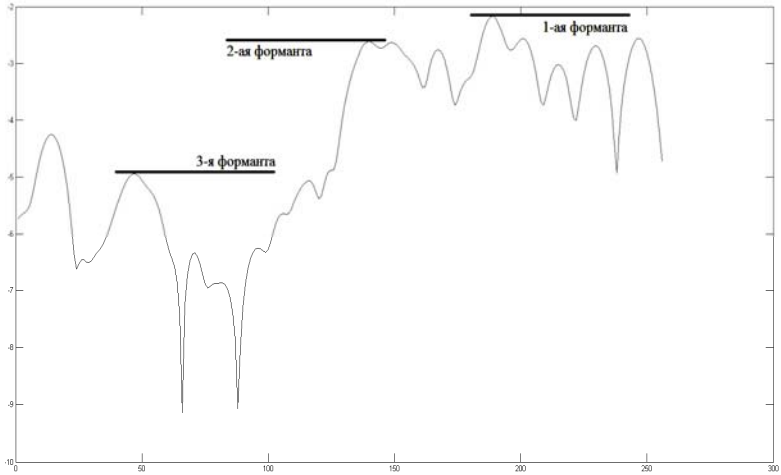


Рис. 3. Форманты звука «О» в слове «Наркоз»

Заключение

В работе предложено использовать нейронную сеть для последовательной обработки различных отсчетов речевого сигнала нейронной сетью с целью уточнения принимаемого решения об идентификации звука на различных уровнях. В настоящее время проводится оценка применимости данного подхода для идентификации звуков в рамках речевого сигнала на примере идентификации гласных. Дальнейшая работа должна показать, на сколько эффективен данный метод распознавания по сравнению с уже существующими. В случае непримени-

мости предложенного подхода возможно дополнение срезов спектра сигнала в заданные моменты времени дополнительной характеристикой, описывающей динамику изменения спектра в течение интервала времени.

Проект ГПО КИБЭВС-1005 – «Система распознавания образов на основе нейронных сетей».

ЛИТЕРАТУРА

1. Хайкин С. Нейронные сети: полный курс. 2-е изд.: пер. с англ. М.: Изд. дом «Вильямс», 2006. 1106 с.

2. Нейронные сети [Электронный ресурс]. Режим доступа: http://www.aiportal.ru/articles/neural-networks/1/, свободный.

3. Ануфриев И.Е., Смирнов А.Б., Смирнова Е.Н., MATLAB 7. СПб.: БХВ-Петербург, 2005. 1104 с.

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

ПРИЛОЖЕНИЯ ТЕОРИИ КЛЕТОЧНЫХ АВТОМАТОВ В ОБРАБОТКЕ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

О.О. Евсютин, аспирант

г. Томск, ТУСУР, каф. КИБЭВС, eoo@keva.tusur.ru

Обработка цифровых изображений в современном мире представлена достаточно широким спектром различных методов, предназначенных для решения задач улучшения, восстановления, сжатия, морфологического анализа изображений, а также распознавания образов [1].

Для решения большинства из перечисленных задач может быть использован математический аппарат теории клеточных автоматов.

Базовым понятием в контексте улучшения и восстановления цифровых изображений является понятие фильтрации, когда значение каждого элемента изображения заменяется новым, зависящим от значений соседних элементов, принадлежащих некоторой окрестности. Для этого задается матрица малого размера, называемая маской фильтра, значения элементов которой обычно представляют собой весовые коэффициенты при суммируемых элементах выделенной окрестности изображения.

Схема фильтрации цифрового изображения представлена на рис. 1.

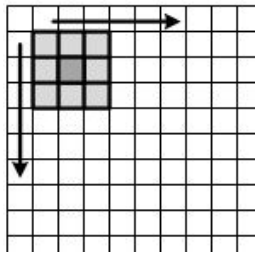


Рис. 1. Фильтрация цифрового изображения

Аналогичным образом организована работа клеточного автомата: значение каждой клетки решетки изменяется в зависимости от значений соседних клеток, принадлежащих окрестности заданного размера, согласно некоторой функции или правилу развития. Обновление значений всех клеток решетки происходит одновременно в каждый момент времени [2].

Таким образом, существующие методы фильтрации цифровых изображений могут быть описаны в терминах динамики клеточных автоматов, а также могут быть получены новые фильтры, построенные на основе клеточных автоматов [3].

Другим важным направлением в рассматриваемой области является сжатие цифровых изображений. Здесь, в свою очередь, ключевым является понятие декоррелирующего преобразования, устраняющего пространственную избыточность между элементами цифрового изображения для их последующего статистического сжатия. Базисы таких преобразований могут быть получены с помощью динамики клеточных автоматов посредством задания множества вещественных коэффициентов, соответствующих элементам базисных векторов, и установления соответствия между целочисленными значениями клеток решетки и указанными коэффициентами. Тогда отдельно взятые состояния развития клеточного автомата будут соответствовать векторам искомого базиса при условии наличия между ними взаимной ортогональности [4].

Клеточные автоматы используются и на стыке таких областей, как обработка цифровых изображений и искусственный интеллект, а именно при решении задачи распознавания образов. Так в [5] рассматривается подход к распознаванию текста посредством выделения структурных признаков символов из их изображений на основе набора клеточных автоматов. Причем клеточные автоматы могут быть задействованы на различных этапах процесса распознавания текста: как для непосредственного выделения признаков символов и их классификации, так и на предшествующих этапах разбиения изображения на текстовые блоки и выделения в данных блоках текстовых строк и отдельных символов.

Приложениям клеточных автоматов в обработке цифровых изображений посвящено достаточно много научных работ, однако попрежнему остаются нерешенные вопросы, дающие возможность для новых исследований.

ЛИТЕРАТУРА

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

2. Тоффоли Т., Марголус Н. Машины клеточных автоматов. М.: Мир, 1991. 284 с.

3. Моисеенко С.В., Оплачко Е.О. Фильтрация шума в цифровом изображении на основе клеточного автомата // Научная сессия ТУСУР–2011: Матер. Всерос. научн.-техн. конф. студентов, аспирантов и молодых ученых, Томск, 4–6 мая 2011 г. Ч. 3. Томск: В-Спектр, 2011. С. 62–65.

4. Евсютин О.О. Декоррелирующие клеточные преобразования // Тр. 54-й науч. конф. МФТИ «Проблемы фундаментальных и прикладных естественных и технических наук в современном информационном обществе». Управление и прикладная математика. Т. 2. М.: МФТИ, 2011. С. 69–70.

5. Суясов Д.И. Выделение структурных признаков изображений символов на основе клеточных автоматов с метками // Информационно-управляющие системы. 2010. №4 (47). С. 39–45.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ ТРАНСПОРТНЫМ РОБОТОМ (НА ПРИМЕРЕ LEGO-РОБОТА)

И.Н. Гаращенко, А.К. Шмакова, Н.Ю. Кудаев, Т.Р. Зубаиров, С.А. Катков, Е.О. Сесова, М.Ю. Пушкарев, студенты каф. АСУ

Научный руководитель А.Н. Горитов, проф., д.т.н.

г. Томск, ТУСУР, ФСУ, shmakova-nastya@yandex.ru

В настоящее время активно ведется проектирование и конструирование мобильных транспортных роботов и разработка программного обеспечения для решения задач различного типа, таких как ориентирование на местности, обход препятствий, транспортировка ресурсов в условиях, непригодных для человека и т.п. Всё это может использоваться в различных областях человеческой деятельности: в пожаротушении, в разминировании местности, при борьбе с террористическими актами, в ядерной и химической промышленности, а также в космической сфере. Как правило, для решения этих задач используются транспортные роботы с определенными колесными базами, формулами (4×2, 3×2, гусеничные и др.), характеристиками колес. Универсального программного обеспечения для работы со всеми основными типами не было найдено.

Целью данной работы является создание универсального программного обеспечения для дистанционного управления транспортным роботом.

Программа должна при заданных входных данных (тип робота, расстояние между колесами, радиус колес, размеры поля, нарисованная траектория и т.п.) рассчитать углы поворота колес и длины прямых траекторий. На рис. 1 представлена структура программы, где проме-

жуточные данные – это данные, полученные на основе входных данных (скорость вращения колес, углы поворота колес и т.п.) и обрабатывающиеся в модульной части программы, где данные запаковываются в форме, понятной роботу, и отправляются через определенный интерфейс (Bluetooth, радио-канал, Wi-Fi и др.). Робот в свою очередь, получив определенную команду, должен либо проехать соответствующее расстояние, либо повернуть на соответствующий угол.

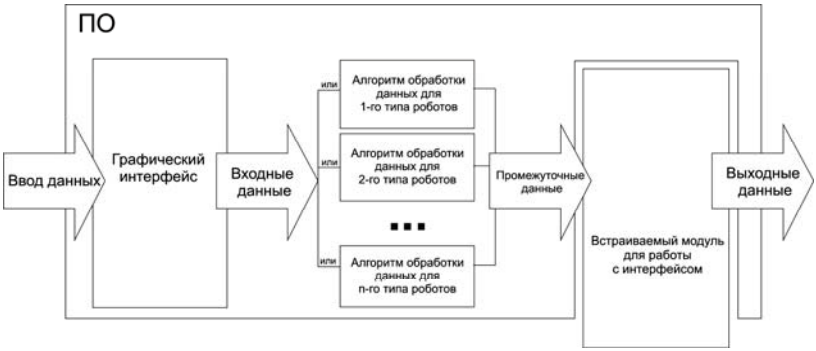


Рис. 1. Структура программы

В ходе выполнения работы были поставлены следующие задачи:

1. Исследование зависимости радиуса колеса и расстояния между колесами от угла поворота (для колесной формулы 3×2 – два колеса из трех ведущие).

2. Разработка и реализация алгоритма движения по заданной траектории.

3. Разработка и реализация алгоритма обработки и передачи данных по каналу Bluetooth на основе класса System.IO.Ports.SerialPort, предоставленного .NET Framework 4.0.

4. Разработка и реализация графического интерфейса программы.

Учитывая тот факт, что длина дуги колеса равна длине дуги траектории поворота, и используя формулу длины дуги окружности, была выведена формула (1), выражающая зависимость радиуса колеса и расстояния между колесами робота от угла поворота:

$$\beta - \frac{L}{2R}\alpha, \qquad (1)$$

где L – расстояние между серединами колес, R – радиус колеса, α – угол поворота робота, β – угол поворота колеса.

Траектория следования представляет собой набор точек (рис. 2) на координатной сетке.

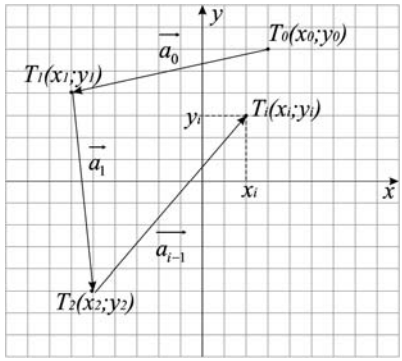


Рис. 2. Траектория следования

Основная идея алгоритма движения по заданной траектории заключается в следующем:

1. Входной набор точек необходимо преобразовать по формулам (2), учитывая ширину карты w и высоту – h в см:

$$x_i' = \frac{x_i}{2 \cdot x_{\max}} \cdot w; \quad y_i' = \frac{y_i}{2 \cdot y_{\max}} \cdot h; \quad i = \overline{1,n}. \tag{2}$$

2. Полученный набор точек преобразуем в набор векторов по формуле (3):

$$\overrightarrow{a_i}\left\{x_{a_i}; y_{a_i}\right\} = \left\{x_{i+1}' - x_i'; y_{i+1}' - y_i'\right\}, i = \overline{1,n}. \tag{3}$$

3. Для движения вперед на определенное число единиц вычисляем длину вектора по формуле (4):

$$\left|\overrightarrow{a_i}\left\{x_{a_i}; y_{a_i}\right\}\right| = \sqrt{x_{a_i}^2 + y_{a_i}^2}, i = \overline{1,n}. \tag{4}$$

4. Чтобы получить угол поворота робота, вычислим угол между векторами, используя формулу (5):

$$\left(\overrightarrow{a_i}\,\hat{}\,\overrightarrow{a_{i+1}}\right) = \arccos\frac{x_{a_i} \cdot x_{a_{i+1}} + y_{a_i} \cdot y_{a_{i+1}}}{\sqrt{x_{a_i}^2 + y_{a_i}^2} \cdot \sqrt{x_{a_{i+1}}^2 + y_{a_{i+1}}^2}}, i = \overline{1,n}. \tag{5}$$

5. Для определения в какую сторону поворачивать роботу, вычислим векторное произведение векторов по формуле (6); если оно положительно, то в правую, если отрицательно – в левую:

$$\overrightarrow{a_i} \times \overrightarrow{a_{i+1}} = x_{a_i} \cdot y_{a_{i+1}} - x_{a_{i+1}} \cdot y_{a_i}, i = \overline{1,n}. \tag{6}$$

Программа написана в среде Visual Studio 2008 на языке C#.

Для работы с графикой была использована библиотека *Tao*.

Минимальные системные требования:

1. .NET Framework 4.0.
2. Библиотека *Tao*.
3. ОС Windows XP, место на диске 50 Мб;
4. Bluetooth адаптер.

Для сборки тестовой конструкции робота был выбран конструктор LEGO Mindstorms NXT 2.0, так как он обладает рядом достоинств: доступность, универсальность, простота в сборке и управлении, поддержка Bluetooth.

Заключение

В ходе данной работы было разработано ПО, позволяющее управлять транспортным роботом LEGO Mindstorms NXT 2.0 по каналу Bluetooth. В дальнейшем планируется сделать ПО более универсальным, а именно, сделать его модульным и увеличить количество поддерживаемых типов транспортных роботов.

Проект ГПО АСУ-1003 – «Управление интеллектуальными робототехническими системами».

ЭФФЕКТ ПЕРЕОБУЧЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ МОДИФИЦИРОВАННОГО АЛГОРИТМА ПЧЕЛИНОЙ КОЛОНИИ ДЛЯ НЕЧЕТКОГО АППРОКСИМАТОРА

И.В. Горбунов, аспирант

Научный руководитель И.А. Ходашинский, проф.

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

Постановка задачи. Одним из объектов исследования в прикладной статистике является задача обучения по прецедентам: задана обучающая выборка пар объект–ответ; требуется восстановить функциональную зависимость ответов от объектов, т. е. построить алгоритм, способный выдавать адекватный ответ для произвольного объекта [1]. Одним из таких алгоритмов является модифицированный алгоритм пчелиной колонии (МАПК), который служит для параметрической идентификации параметров *нечеткой системы* (*НС*). Данный алгоритм наиболее полно описан в статье [2]. МАПК настраивает базу правил нечеткой системы типа *синглтон*, представленную ниже.

Синглтон осуществляет отображение $f:\Re^n \to \Re$:

$$f(\mathbf{x}) = \sum_{i=1}^{R} \mu_{A1i}(x_1)\cdot\mu_{A2i}(x_2)\cdot\ldots\cdot\mu_{Ani}(x_n)\cdot r_i \Big/ \sum_{i=1}^{R} \mu_{A1i}(x_1)\cdot\mu_{A2i}(x_2)\cdot\ldots\cdot\mu_{Ani}(x_n),$$

где $\mathbf{x}$ – входной вектор; R – число правил; n – количество входных переменных; μ_{Aij} – функция принадлежности.

Нечеткая система может быть представлена как

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

где $\boldsymbol{\theta} = \|\theta_1,\ldots,\theta_N\|$ – вектор параметров; y – скалярный выход системы [3].

Пары объект–ответ представлены в *таблице наблюдений*, ТО = $\{(\boldsymbol{x}_p; t_p), p = 1, ..., m\}$. Критерием оптимизации служит *ошибка обучения*. В данной работе в качестве ошибки обучения используется *средняя квадратичная ошибка* (*СКО*) между ответом в таблице наблюдения и выходом нечеткой системы. В данном случае СКО рассчитывается по формуле (1):

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

Проблема данного подхода заключается в том, что по значению ошибки обучения нельзя достоверно судить об эффективности и адекватности полученной системы для объектов, не вошедших в таблицу наблюдений. СКО для этих объектов, как правило, больше значения ошибки обучения, это явление называется *эффектом переобучения* (*переподгонка*) [4, 5]. В эксперименте будет определена *переобученность* НС настраиваемой МАПК для различных наборов данных и отслежена динамика изменения переобученности НС от количества итераций МАПК.

Эксперимент

Для проведения эксперимента таблицу наблюдений разбивают на q равных по размеру, не пересекающихся блоков, согласно методу *контроль по q-блокам* (*q-fold CV*) [5], частному случаю *скользящего контроля* (*кросс–валидации*). Таким образом: $\mathbf{TO}=\mathbf{TO}_1 \cup \mathbf{TO}_2 \cup \ldots \cup \mathbf{TO}_q$ и $\mathbf{TO}_i \cap \mathbf{TO}_j$, $i \neq j$.

Каждый блок по очереди становится контрольным, при этом в обучающую выборку попадаются остальные q–1 блоков. Тогда переобученность рассчитывается по формуле (2):

$$CV(\boldsymbol{\theta}, \mathbf{TO}) = \frac{1}{q} \sum_{i=1}^{q} \text{СКО}(\boldsymbol{\theta}, \mathbf{TO}_i) - \text{СКО}(\boldsymbol{\theta}, \mathbf{TO} \setminus \mathbf{TO}_i). \quad (2)$$

Более подробно о скользящем контроле написано в [6].

Эксперимент проводился на уже разделённых на части наборах данных из репозитория KEEL [7]. Для всех наборов q = 5. МАПК использовался со следующими параметрами: начальная температура 70, коэффициент охлаждения 0,95, алгоритм формирования популяции – бинарные турниры, размер улья – 50, процент пчел разведчиков – 50,

число итераций – 1000. Для каждого контрольного блока тест выполнялся 10 раз.

В табл. 1, указана относительная переобученность для наборов данных: DEE -5, Diabetes, ELE2, в процентах, для этого абсолютные значения были разделены на максимальное значение консеквента в каждом наборе данных и переведены в проценты.

Таблица 1

Переобученность после 1000-й итерации МАПК

Набор данных	СКО($\boldsymbol{\theta}$,**TO****TO**$_i$), %	СКО($\boldsymbol{\theta}$,**TO**$_i$), %	CV($\boldsymbol{\theta}$,**TO**), %
DEE-5	0,793%	2,279%	1,486%
Diabetes	1,069%	6,714%	5,645%
ELE-2	0,066%	0,163%	0,097%

В табл. 2 представлена частотная оценка вероятности обучения, то есть отношения количества экспериментов, в которых СКО($\boldsymbol{\theta}$,**TO**$_i$) – – СКО($\boldsymbol{\theta}$,**TO****TO**$_i$)>3%, в отношении к полному количеству экспериментов как для случаев возникновения в процессе обучения, так и наличия эффекта после 1000-й итерации МАПК.

Таблица 2

Частотная оценка вероятности переобученности после 1000-й итерации

Набор данных	$\mathbf{Q}_\varepsilon$, % (локальный)	$\mathbf{Q}_\varepsilon$, % (1000)
DEE-5	0	0
Diabetes	14	8
ELE-2	0	0

На рис. 1 представлена типичная работа алгоритма без преодоления 3% барьера переобучения. На рис. 2 представлен случай возникновения локального эффекта переобучения. На рис. 3 представлен один из случаев переобучения, полученных во время эксперимента.

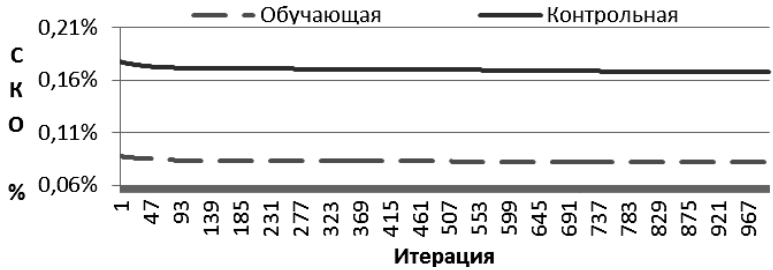


Рис. 1. Работа МАПК без эффекта переобучения

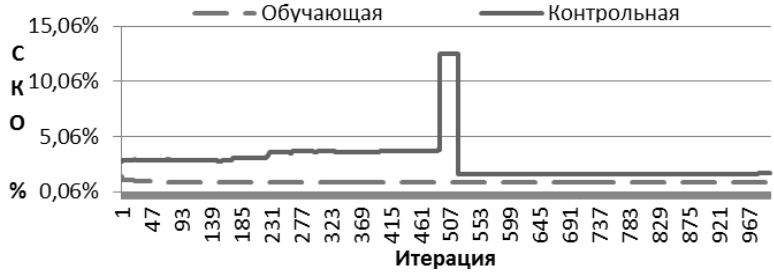


Рис. 2. Локальный эффект переобучения МАПК

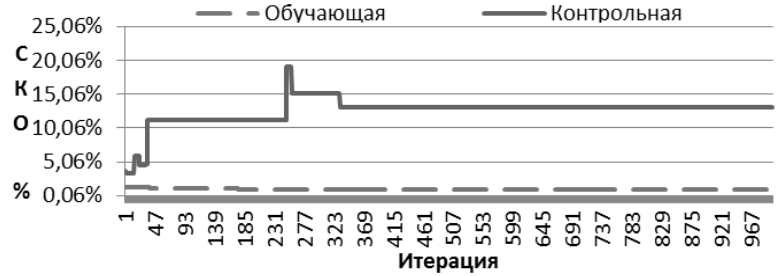


Рис. 3. Эффект переобучения в работу МАПК

Анализ полученных результатов. По результатам эксперимента очевидно, что МАПК подвержен эффекту обучения. Возможность свести эффект переобучения к локальному не гарантирована, но присутствует. Справедливости ради стоит заметить, что эффект проявил себя при эксперименте на наборе данных, размер которого не превышает 41 прецедент при двух входных параметров, т.е. очень малом количестве известных фактов о моделируемой закономерности.

ЛИТЕРАТУРА

1. Воронцов К.В. Комбинаторная теория надёжности обучения по прецедентам: дис. … д-ра физ.-мат. наук: 05-13-17 / Вычислительный центр РАН, 2010. 271 с.

2. Ходашинский И.А., Горбунов И.В., Дудин П.А. Алгоритмы муравьиной и пчелиной колонии для обучения нечетких систем // Доклады Томского государственного университета систем управления и радиоэлектроники. 2009. Т. 20, №2. С. 157–161.

3. Зайцев А.А., Ходашинский И.А., Дудин П.А., Синьков Д.С. Методы вычислительного интеллекта в прогнозировании эффективности немедикаментозного лечения // Матер. V Междунар. науч. конф. (заочной) «Системный анализ в медицине» (САМ 2011) 25–26 мая 2011 г. Благовещенск, 2011. С. 25–28.

4. Vapnik V.N. Statistical learning theory. N.Y.: John Wiley & Sons, Inc., 1998.

5. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning. Springer-Verlag. pages 2008. 763 p

6. Kohavi R. A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection. 14th International Joint Conference on Artificial Intelligence, Palais de Congres Montreal, Quebec. Canada, 1995. C. 1137–1145.

7. Data-mining software Tool: data, set repository [Электронный ресурс]. Режим доступа к сайту: http://www.keel.es.

ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СРЕДСТВ АНАЛИЗА ДАННЫХ В ВЕБ-ПРОЕКТЕ

Ч.А. Ламожапов, С.А. Волков, Р.А. Гурьев, М.А. Харин, студенты

Научный руководитель А.С. Романов, к.т.н.

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

Цель данной работы заключается в исследовании возможности классификации текстов по гендерному признаку автора.

В рамках этой цели требуется разрешить вопрос выбора достоверных характеристик для классификации, которые бы отражали различия в текстах людей разных полов. В этой работе были использованы классификаторы SVM и RVM, а также признаки текста: биграммы (BI), униграммы (UNI), части речи (MORPH), окончания слов (END).

Метод опорных векторов (SVM, support vector machines) – это вид алгоритмов классификации, в основном обучаемых с учителем. Одна из особенностей данных алгоритмов – постоянное уменьшение ошибки. Метод основан на построении одной или нескольких гиперплоскостей или нескольких, разделяющих представления объектов в пространстве на классы [1].

Метод релевантных векторов (RVM, Relevance Vector Machine) [2] позволяет оценить вероятности, принадлежности объекта данному классу. Данный метод в отличие от SVM не гарантирует постоянного уменьшения ошибки обучения.

В ходе работы были разработаны программный комплекс в виде консольных приложений и веб-интерфейс, для него была собрана база образцов для обучения и тестирования. База представляет собой несколько тысяч коротких сообщений. Они собрана из сообщений пользователей twitter.com, т.к. пользователи данного сервиса обмениваются открыто сообщениями и используют в основном неофициальную речь. Длина сообщения ограничена 140 символами.

Программный комплекс состоит из ядра, написанного на языке программирования Python, и веб-интерфейса, написанного на языке программирования PHP. Посредством веб-интерфейса конфигурирует-

ся режим работы ядра. Ядро извлекает из текста набор характеристик и компонует из них вектор для классификаторов. Классификаторы используются как инструмент принятия решения о гендерной принадлежности автора. Сумма их предположений выдаётся как ответ (рис. 1).

Тестирование проводилось через веб-интерфейс (табл. 1, 2). Выбиралась пара текстов из базы данных. Выбирались классификатор и характеристика. Программа выдавала положительный ответ, если обучение прошло успешно. Далее на других текстах проводился анализ. Итогом работы программы являлась вероятность того, что программа сможет определить пол автора по тексту.

Таблица 1

Результаты тестирования четырёх характеристик по количеству строк

Количество строк	Характеристика (классификатор SVM)				Характеристика (классификатор RVM)			
	UNI, %	BI, %	MORPH, %	END, %	UNI, %	BI, %	MORPH, %	END, %
1	48,77	41,23	39,17	39,43	42,17	35,55	34,63	33,99
2	51,11	46,13	46,18	44,07	42,75	32,74	37,13	44,17
5	51,17	61,96	48,13	49,88	47,13	41,55	41,55	48,91
10	54,42	61,11	66,66	61,11	49,11	43,14	45,98	53,14
25	59,87	52,38	52,38	52,38	51,01	52,24	52,24	52,24
50	59,88	52,38	52,38	52,38	51,01	52,24	52,24	52,24
100	64,77	54,12	54,12	54,12	62,13	53,87	53,87	53,87
250	63,06	54,92	54,92	54,92	64,11	54,33	54,33	54,33
500	62,19	58,38	58,38	58,38	62,11	57,39	57,39	57,39
1000	65,44	59,91	57,89	51,32	62,88	47,13	51,18	49,99

Таблица 2

Результаты тестирования различных комбинаций четырёх характеристик по количеству строк

Характеристики, %	Количество строк (классификатор SVM)			Количество строк (классификатор RVM)		
	10	100	1000	10	100	1000
UNI + BI	51,11	51,18	51,32	52,12	59,97	45,12
UNI + MORPH	64,44	51,18	62,96	62,23	59,97	60,13
UNI + END	58,88	51,18	51,32	67,02	59,97	45,12
BI + MORPH	51,11	54,12	51,32	62,12	42,17	45,12
BI + END	51,11	54,12	51,32	62,12	42,17	45,12
MORPH + END	52,22	54,12	51,32	63,17	42,17	45,12
UNI + BI + MORPH	64,44	54,12	62,96	62,23	42,17	60,63
BI + MORPH + END	52,22	54,12	51,32	53,17	42,17	45,12
MORPH + END + UNI	56,66	54,12	63,06	41,11	42,17	60,13
END + UNI + BI	68,88	54,12	51,32	67,01	42,17	45,12
UNI + BI + MORPH + END	64,44	54,12	51,32	62,23	42,17	45,12

По результатам тестов можно сделать выводы, что характеристика UNI в сочетании с классификатором SVM позволяет определить пол автора с наибольшей точностью, равной в данных экспериментах 65,44%. При малом количестве строк более высокий процент выдают комбинации: END+UNI+BI и классификатора SVM – 68,88, UNI+END и классификатора RVM – 67,02. При большом количестве строк наилучших результатов можно добиться с помощью комбинации MORPH+END+UNI и классификатора SVM – 63,06, UNI+BI+MORPH и классификатора RVM – 60,63. Дальнейшие исследования будут связаны с повышением точности классификаторов с помощью увеличения признаков.

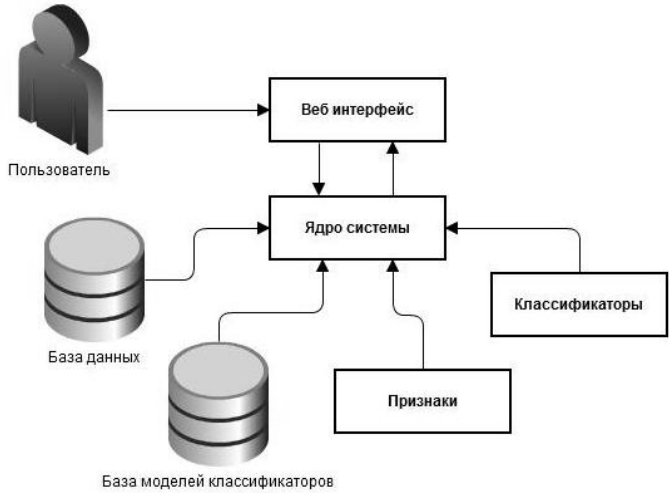


Рис. 1. Структурная схема программного комплекса

ЛИТЕРАТУРА

1. Воронцов К.В. Лекции по методу опорных векторов / К.В. Воронцов // ВЦ РАН, М.: URL: http://www.ccas.ru/voron/download/SVM.pdf (дата обращения: 03.03.12).

2. Christopher M. Bishop. Pattern recognition and machine learning, 2006, C.353-357. URL: http://www.cmlab.csie.ntu.edu.tw/~hsu771217/Pattern Recognition and Machine Learning.pdf (дата обращения: 03.03.12).

3. Romanov A.S., Meshcheriakov R.V. 2011. Gender Identification of the author of a short message. “Dialog 2011” (Computational Linguistics and Intelligent Technologies: Proceedings of the International Conference «Dialog 2011») P. 620–626. URL: http://www.dialog-21.ru/digests/dialog2011/materials/en/pdf/55.pdf (дата обращения: 03.03.12).

АЛГОРИТМЫ И ПРОГРАММНЫЕ СРЕДСТВА ВЫДЕЛЕНИЯ ИНФОРМАТИВНЫХ ПРИЗНАКОВ В ЗАДАЧАХ КЛАССИФИКАЦИИ

Е.Н. Гусакова, студент 5-го курса; И.А. Ходашинский, проф.
г. Томск, ТУСУР, каф. КИБЭВС, ФВС

Программное обеспечение для обнаружения сетевых вторжений защищает компьютерную сеть от неавторизованных пользователей, включая, возможно, инсайдеров. Задача обучения обнаружителя вторжений заключается в том, чтобы построить предсказательную модель (т.е. классификатор, способный различать между «плохими» соединениями, называемыми вторжениями или атаками, и «хорошими» нормальными соединениями).

В лаборатории MIT Lincoln была подготовлена программа «1998 DARPA. Оценка обнаружения вторжений», которая в течение девяти дней собирала данные о соединениях по различным параметрам. Сырые тренировочные данные были около 4 Гб сжатого бинарного TCP-дампа за 7 недель сетевого трафика. Эти данные сгруппированы в 5 млн записей о соединениях [1].

Соединение – это последовательность TCP-пакетов, начинающихся и заканчивающихся в некоторые хорошо определенные моменты, между которыми данные переходят между исходным и целевым IP-адресами по определенному протоколу. Каждое соединение было помечено либо как нормальное, либо как атака, с точным указанием одного определенного типа атаки. Каждая запись о соединении состоит из 100 байт. Данные были собраны в файл. Всего в файле 41 характеристика сетевых вторжений по 22 различным атакам и нормальному соединению.

Предобработка. Из исходного блока данных была сформирована случайная выборка меньшего размера: по 500 записей по каждой атаке.

После того как была сформирована подвыборка, была проведена нормализация всех признаков. Нормализация необходима по той причине, что все признаки имеют различные шкалы принимаемых значений: какие-то признаки принимают дискретные значения (тип протокола, флаг), другие принимают дискретные значения (только 0 и 1), большинство же меняется от 0 до нескольких тысяч. Так как изначально нам неизвестно, какие признаки более информативны, а какие нет, мы должны рассматривать их все как равносильные (т.е. максимальная разница между двумя записями по одному признаку не должна быть больше максимальной разницы по другому признаку).

Признаки, значения которых расположены на номинальной шкале (тип протокола, например), были исключены из набора.

После нормализации всех признаков подвыборка была разделена на две части: обучающая и тестовая выборки для алгоритма классификации *k* ближайших соседей.

Метод *k* ближайших соседей (англ. *k*-nearest neighbor algorithm, *kNN*) – метод автоматической классификации объектов. Основным принципом метода ближайших соседей является то, что объект присваивается тому классу, который является наиболее распространённым среди соседей данного элемента [2].

Соседи берутся, исходя из множества объектов, классы которых уже известны, и, исходя из ключевого для данного метода значения *k*, определяется, какой класс наиболее многочислен среди них.

Для применения данного алгоритма из исходных данных было сформировано две подвыборки: обучающая (400 записей по каждой атаке) и тестовая (100 записей по каждой атаке). При программной реализации алгоритма количество записей в тестовой и обучающей выборке передается в функцию параметром, а потому может варьироваться для сравнения результатов и вычисления оптимального объема подвыборок.

Количество соседей изначально было выбрано равным пяти, но так же передается в качестве параметра для определения их оптимального количества.

Результативность алгоритма (количество правильно и неправильно классифицированных записей) так же очень сильно зависит от выбора способа расчета расстояния между двумя записями. В программной реализации алгоритма пользователь имеет возможность выбрать, каким способом следует рассчитывать расстояние. Для выбора предоставляются следующие четыре варианта: Евклидово расстояние, квадрат Евклидова расстояния, Манхеттенское расстояние, расстояние Чебышева.

Ближайшими соседями считаются записи, расстояние до которых минимально.

После того как вычислены *k* ближайших соседей, анализируется их мода. Класс, который встречается чаще всего среди *k* ближайших соседей, и присваивается классифицируемой записи из тестовой выборки.

После анализа последней записи из тестовой выборки производится подсчет процента правильно классифицированных записей.

Анализ результатов. Минимальный процент ошибок достигается при расчете по формуле Евклидова расстояния. В этом случае ошибка достигает не более 15%, минимальный процент ошибок – 10%. Расчет расстояния как квадрата Евклидова расстояния дает более высокий процент ошибок: от 13 до 17%. Если использовать формулу Манхеттенского расстояния, процент ошибки получается достаточно большой –

свыше 26,5%. При расчете расстояния по формуле Чебышева процент ошибок максимален: количество правильно классифицированных записей не превышает 24%.

После этого была выдвинута гипотеза, что если при исключении одной из характеристик набор соседей не меняется, то данная характеристика не является информативной и ее можно исключить. Для проверки данной гипотезы каждая из характеристик поочередно исключалась из набора и алгоритм поиска ближайших соседей повторялся. Каждый раз вновь полученный набор соседей сравнивался с набором соседей, полученным при полном наборе характеристик. Для проверки данной гипотезы использовались генетические алгоритмы.

В данном случае фитнес-функция формировалась на основе результатов, полученных в ходе выполнения алгоритма k ближайших соседей, в зависимости от того, отличаются ли соседи до и после отбрасывания признака: фитнес-функция минимальна, если соседи не изменились. Для вывода новой популяции использовался простой механизм рулетки. Условием остановки было выбрано выведение 10000 популяций.

В результате выполнения генетического алгоритма на заданном наборе данных была получена популяция наиболее приспособленных хромосом, по которым был сделан вывод о неинформативности следующих признаков: srv_diff_host_rate (процент соединений к другим хостам); srv_count (количество соединений к тому же сервису, что и в текущем соединении, в последние 2 с); num_outbound_cmds (количество внешних команд в FTP-сессии); su_attempted (была ли опробована команда «su root»).

ЛИТЕРАТУРА

1. KDD-CUP-99 [Электронный ресурс]. Режим доступа: http://kdd.ics.uci.edu/databases/kddcup99/task.html

2. Метод k ближайших соседей [Электронный ресурс]. Режим доступа: http://www.spc-consulting.ru/dms/MachineLearning/MachineLearning/Overviews/KNea

3. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М.: Горячая Линия – Телеком, 452 с.

НЕЧЕТКИЙ РЕГУЛЯТОР КАК СРЕДСТВО УПРАВЛЕНИЯ КОМПЕНСИРУЮЩИМИ УСТРОЙСТВАМИ В АКТИВНО-АДАПТИВНОЙ СЕТИ

А.Н. Качалов, аспирант каф. УИ

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

г. Томск, ТУСУР, kachalov@sibmail.com

В электроэнергетической сфере промышленности на сегодняшний момент остро стоит вопрос о повышении эффективности ее работы

путем сохранения баланса реактивной мощности в сети. Средством компенсации могут являться такие устройства, как конденсаторные батареи, синхронные двигатели, синхронные компенсаторы, тиристорные компенсаторы, статический синхронный компенсатор серии STATCOM, унифицированный контроллер Power Flow (Unified Power Flow Controller), SEN-трансформаторы [1].

Основу компенсирующих устройств (КУ) составляют накопительные элементы (емкости, индуктивности), реакторно-тиристорные и конденсаторно-тиристорные блоки. КУ за счет тиристорного управления обладают исключительным быстродействием и осуществляют безынерционное плавное регулирование от 1 до 100% за 300 мс) реактивной мощности во всем диапозоне, от мощности, отдаваемой конденсаторами, до мощности потребляемой индуктивностью [2].

Интеллектуальное управление множеством таким устройств в активно-адаптивной сети дает возможность эффективного регулирования сдвига фазы тока относительно напряжения, что непосредственно влияет на пропускную способность линий электропередач и величину уменьшения амплитуды напряжения в сети. В основу интеллектуального управления был выбран нечеткий регулятор, т.к. он по результатам экспертных оценок обеспечивает минимальное время стабилизации напряжения по сравнению с ПИ- и ПИД-регулятором [3].

Нечеткий регулятор управляющего воздействия для КУ имеет в виде входных значений величину отклонения напряжения в сети *dU* от нормы (100%) в диапазоне от 0 до 200% и условную величину потребления реактивной мощности *Qgm* потребителем в диапазоне от –1 до 1. Выходное значение есть условная величина регулирующего воздействия *Um* в диапазоне от –1 до 1, которая непосредственно переконвертируется по весовому коэффициенту в МВАр генерации или потребления реактивной мощности компенсирующей установкой. Всего в нечетком регуляторе используется 11 правил с центром области как методом дефазификации.

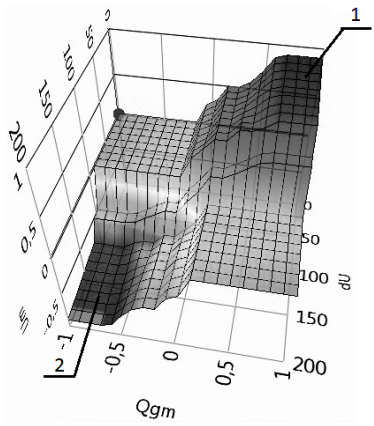


Рис. 1. 3D-модель взаимосвязи входных и выходных переменных

Результат управления нечеткой модели, представленный на рис. 1, демонстрирует две ключевые области: *1* – область высокого регулирующего воздействия конденсаторами, при высоком внешнем потреблении реактивной энергии и значительном уменьшении напряжения в сети; *2* – область высокого регулирующего воздействия шунтирующими реакторами, при высокой внешней генерации реактивной энергии и значительном увеличении напряжения в сети.

Нечеткий регулятор позволяет быстро спроектировать модель управления прикладным процессом, но является ли построенная модель эталоном? Вероятнее всего нет, и для ее бесконечного приближения к эталонной модели необходимы методы самообучения.

ЛИТЕРАТУРА

1. Зачепа Ю.В., Василькова Т.С. Анализ систем компенсации реактивной мощности в условиях автономных генераторных установок // ELECTRO-MECHANICAL AND ENERGY SAVING UP SYSTEMS. 2010. № 4. P. 71–78.

2. Мастерова О.В., Тюлькин М.В. Исследование эффективности реализации пилотного проекта по установке статического тиристорного компенсатора на подстанции Новоанжерская 500 Кв // Известия Томского политехнического университета. 2010. Т. 317. № 4. С. 100–103.

3. Karuppanan P., Mahapatra K. K. PI, PID and Fuzzy Logic Controller for Reactive Power and Harmonic Compensation // International J. of Recent Trends in Engineering and Technology. 2010. Vol. 3, №3. P. 88–92.

ТЕСТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА RUBY ON RAILS

А.А. Ханефт*, *студент 3-го курса

г. Томск, *ТУСУР*, *каф. АСУ, ФСУ*, *a.khaneft@mail.ru*

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

В настоящее время многие организации, которые создают программное обеспечение, до 50% средств, выделенных на разработку программ, тратят на их тестирование. Но несмотря на огромные капиталовложения, знаний о сути тестирования явно не хватает и большинство программных продуктов ненадежны даже после основательного тестирования. Заметим, что тестирование программ активно применяется и в соревнованиях по спортивному программированию [1].

Тестирование – процесс, подтверждающий правильность программы и демонстрирующий, что ошибок в программе нет. Основной недостаток такого определения заключается в том, что оно неверно. На самом деле невозможно продемонстрировать отсутствие ошибок в программе. Поэтому определение описывает невыполнимую задачу, а

так как тестирование зачастую все же выполняется с успехом, по крайней мере, с некоторым успехом, то такое определение логически некорректно.

Правильное определение таково: тестирование – это любая деятельность, направленная на обнаружение ошибок в программном продукте. Тестирование проводится для того, чтобы обнаружить ошибки в программе и повысить ее надежность и ценность.

Примерная схема тестирования приведена на рис. 1.

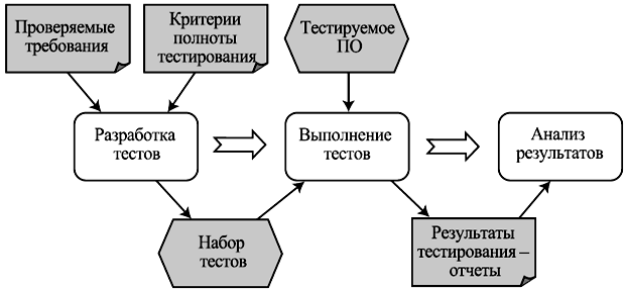


Рис. 1. Схема процесса тестирования программного продукта

Тестирование Web-приложений является неотъемлемой частью процесса их разработки (рис. 1). Существуют различные уровни тестирования:

1) модульное;
2) интеграционное;
3) системное;
4) приемочное.

В рамках модульного тестирования проверяются минимально возможные компоненты, например отдельные классы или функции. Интеграционное тестирование предназначено для проверки связи между компонентами. Задачей системного тестирования является проверка как функциональных, так и нефункциональных требований к системе в целом. Приемочное тестирование проверяет поведение системы на предмет удовлетворения требований заказчика.

Основными целями написания тестов для нашего приложения на Ruby on Rails [2] являются:

- простой запуск тестов позволит убедиться, что наш код придерживается нужной функциональности даже после большой переделки кода;
- симулировать запросы браузера, таким образом, можно тестировать отклик своего приложения без необхо-димости тестирования с использованием браузера.

Проект ГПО АСУ-1101 – «Программное обеспечение для организации и проведения спортивного программирования».

ЛИТЕРАТУРА

1. Командный чемпионат мира по программированию ACM 2011/2012. Северо-Восточный Европейский регион / Под ред. В.Н. Васильева, В.Г. Парфенова. Санкт-Петербург: НИУ ИТМО, 2011. 254 с.

2. Sam Ruby, Dave Thomas, David Hansson. Agile Web Development with Rails. Fourth Edition. R.:The Pragmatic Bookshelf, 2011. 474 c.

ПРИМЕНЕНИЕ МЕТОДА ЦВЕТОВЫХ ГИСТОГРАММ ДЛЯ КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ С ЦЕНТРАЛЬНЫМ ПОЗИЦИОНИРОВАНИЕМ ОБЪЕКТА

И.А. Кривцов*, *студент каф. АСУ

Научный руководитель И. В. Бойченко, доцент, к.т.н.

г. Томск, ТУСУР, ФСУ, IgorKrivtsov@mail.ru

В процессе реализации проекта ГПО «Электронная тень» необходимо было решить задачу объединения схожих групп изображений по классам.

Поскольку классификация изображений обычно используется не самостоятельно, а как часть некоторой системы (например, системы машинного зрения), то с практической точки зрения качество работы метода оценивается исходя из работы системы в целом. Поэтому один и тот же метод классификации может оказаться пригодным для одной задачи и несоответствующим для другой. Это обосновывает необходимость работы с методами машинного обучения и калибровки параметров алгоритмов обучения.

Как правило, системы распознавания изображений строятся по следующей схеме:

- предобработка изображения (необязательный шаг);
- сбор признаков;
- обучение классификатора;
- классификация.

В качестве признаков будем использовать гистограммы яркости пикселей изображения по цветовым каналам [1].

В качестве входных данных для эксперимента возьмем 4 набора изображений с сайта Лаборатории компьютерной графики при ВМК МГУ [2].

Проект выполнен в системе MATLAB, т.к. эта система содержит массу библиотечных функций для обработки изображений.

Классификатор с признаками на основе цветовых гистограмм

После загрузки из файла изображение проходит предобработку путем изменения размера к высоте 128 пикселей с сохранением пропорций изображения, нормализации значений его элементов к интервалу [0;1] и преобразования цветового пространства из системы RGB в HSV (используется функция rgb2hsv).

Мотивацией к изменению размера является желание ускорить вычисление признаков на изображении.

После предобработки изображения вычисляются признаки. В качестве признаков используется цветовая гистограмма всего изображения либо его прямоугольной части (используется функция histc). Гистограммой трехканального HSV изображения является массив 16×3, где 16 – число бинов (столбцов гистограммы). Значения гистограммы нормализуются к интервалу [0; 1]. Мотивацией к нормализации является рекомендация авторов LIBSVM [3] нормализовать обучающие данные.

В качестве частей изображения (рис. 1) берутся его верхняя и нижняя части, центральная часть (отстоящая от краев на 1/3 ширины/высоты изображения), верхняя – левая четверть, верхняя-правая четверть, нижняя – левая четверть и нижняя – правая четверть.

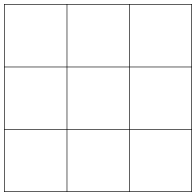


Рис. 1. Логическое разбиение изображения на фрагменты

Мотивацией выделения частей является локализация объектов в данных частях (например, бутоны цветков находятся преимущественно в центральной части изображения, а на изображениях с улицы небо расположено в верхней части). При изменении угла поворота камеры, данная фрагментация позволят дать разный вес для значимости каждого из признаков. Как правило, объект съемки всегда располагается в центральной части изображения, верхняя и нижняя части меняются незначительно, а боковые подвержены изменениям.

Если объединить три канала гистограммы цвета в один вектор 1×48, то получится смешанная гистограмма. Также каждый канал гистограммы можно рассматривать как отдельный признак.

В результате для каждого изображения получаем 32 признака.

Слабый классификатор

Если для каждого из 32 признаков обучить SVM- (support vector machines – это набор схожих алгоритмов вида «обучение с учителем», использующихся для задач классификации) классификатор (функции svmtrain/svmpredict библиотеки LIBSVM [3]), то получим 32 класси-

фикатора, вероятность неверной классификации в которых экспериментально не менее 20%. Поэтому назовем их «слабыми» классификаторами.

Для обучения слабого классификатора необходимо разбить выборку на три: обучающую, валидационную и тестовую.

Для SVM классификатора используется RBF- (функция радиального базиса, значение которой зависит только от нормы аргумента) ядро с двумя параметрами (C, gamma), которые подбираются на валидационной выборке.

Сильный классификатор

Для уменьшения вероятности неверной классификации «слабые» классификаторы обычно объединяют в иерархическую структуру, которую назовем «сильным» классификатором.

Получив на выходах слабых классификаторов некий результат, сформируем из него обучающую выборку для еще одного SVM-классификатора, который назовем «сильным».

Причем не все слабые классификаторы имеют одинаково хорошие результаты классификации, поэтому существует мотивация взять только N наилучших из них, чтобы остальные не портили результат сильному классификатору. Число N определяется экспериментально, последовательно добавляя по одному слабому классификатору и вычисляя результирующую ошибку (процент неверно классифицированных изображений). N берется таким, при котором ошибка наименьшая.

Заключение

В эксперименте на выборке ошибка сильного классификатора оказалась порядка 3%. Применение данной фрагментации изображения обосновано достаточно малой погрешностью и временем, затрачиваемым на вычисления.

Данный проект выполнялся в рамках программы «У.М.Н.И.К.» (проект 13140) и является частью проекта ГПО «Электронная тень».

ЛИТЕРАТУРА

1. Histogram, Image Classification [Электронный ресурс]. Режим доступа: http://olivier.chapelle.cc/pub/tnn99.pdf. Загл. с экрана.

2. Лаборатория компьютерной графики при ВМК МГУ [Электронный ресурс] / Курсы лаборатории компьютерной графики. Режим доступа: http://courses.graphicon.ru/school/mscvs2011/assign. Загл. с экрана.

3. Сайт разработчиков открытого программного обеспечения LIBSVM [Электронный ресурс] / Загрузка библиотеки LIBSVM. Режим доступа: http://www.csie.ntu.edu.tw/~cjlin/libsvm/ Загл. с экрана.

РЕШЕНИЕ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ В НЕЙРОСЕТЕВОМ БАЗИСЕ

К.А. Семенов, А.Е. Утешева, студенты;
А.А. Погуда, ст. преподаватель каф. ИОИД ТГУ
г. Томск, ТУСУР, ФСУ, icetomcat@gmail.com

В настоящее время известно множество численных методов для решения обыкновенных дифференциальных уравнений и систем обыкновенных дифференциальных уравнений. Однако большинство из них являются последовательными, т.е. изначально были созданы для решения на однопроцессорных ЭВМ и не поддавались распараллеливанию. Поэтому они не пригодны для решения задач сверхбольшой размерности в реальном времени.

Нейронная сеть (НС) является высокопараллельным вычислительным устройством, что ведет к увеличению скорости вычислений на современных ЭВМ и суперкомпьютерах.

Обучив НС на примерах некоторого множества дифференциальных уравнений, можно решать похожие уравнения за несколько физических тактов работы сети, т.е. в реальном времени.

На сегодня были рассмотрены обыкновенные дифференциальные уравнения.

В общем виде обыкновенное дифференциальное уравнение может быть представлено так:

$$\phi(x, y(x), y'(x), ..., y^{(n)}(x)) = 0, \quad (1)$$

где ϕ – неявно заданная функция своих аргументов; x – независимая переменная; $y(x)$ – зависимая переменная; $y^{(n)}(x)$ – n-я производная функции y.

Ограничимся рассмотрением только обыкновенных дифференциальных уравнений первого порядка. Тогда уравнение (1) можно записать в виде

$$\phi(x, y(x), y'(x)) = 0. \quad (2)$$

Предположим, что уравнение (2) может быть разрешено относительно производной. Тогда оно имеет вид

$$y' = \phi(x, y) \quad (3)$$

или

$$y' = \phi(y). \quad (4)$$

С целью сокращения объема вычислений и математических выкладок будем рассматривать только (4), поскольку все сказанное относится и к (3).

Предположим, что дифференциальное уравнение имеет решение на отрезке $D = [x_1, x_2]$. Пусть $y^*(x)$ – точное решение, т.е. такая функ-

ция, которая удовлетворяет (4). Итерационный алгоритм можно описать следующими соотношениями:

$$y^k(x) = y^k; \varepsilon = |y^*(x) - y^k(x)|,$$

где y^k – k-е приближение решения; ε^k – ошибка на k-м шаге.

Предположим, что

$$(y^k)' = \phi_k(y^k), \tag{5}$$

$$y^{k+1} = g_k(y^k). \tag{6}$$

Введем ошибку e^k, определяемую выражением

$$e^k = |\phi(y) - \phi_k(y^k)| = \int_D (\phi(y) - \phi_k(y^k))^2 dy. \tag{7}$$

Выражения (5) и (6) описывают итерационный процесс решения дифференциального уравнения. $g_k(y^k)$ следует выбирать таким образом, чтобы выполнялось условие

$$\lim_{k\to\infty} e^k = 0.$$

Аппроксимируем функцию $g_k(y^k)$ кусочно-линейной функцией $G(y)$. Поскольку вид функции $g_k(\cdot)$ не известен, то будем считать, что функция G кроме своего аргумента y зависит еще от вектора параметров:

$$\alpha = (c_1, c_2, \ldots, c_{N-1}, d_1, d_2, \ldots, d_{N-1}),$$

где N – число точек разбиений отрезка D; c_i и d_i – параметры линейной функции $(c_i y + d_i)$, аппроксимирующей участок $y_i \le y \le y_{i+1}$ функции $g_k(\cdot)$.

Очевидно, что

$$\lim_{N\to\infty} |g_k(y) - G(y)| = 0.$$

Поэтому вместо $g_k(y)$ можно вычислять $G(y)$.

Для вычисления функции $G(y)$ используем двухслойную НС с линейной функцией активации.

Первый слой будет состоять из N нейронов, на вход которым подается y^k, второй слой состоит всего из одного нейрона, а на выходе получаем y^{k+1}.

Неизвестный вектор параметров функции G будем искать из условия минимума ошибки (7).

Примечательно, что эта задача эквивалентна обучению НС. В начале обучения предполагаем случайными весовые коэффициенты сети. На вход сети подается вектор y^k, состоящий из функций $y^k(x)$ в L точках $x_1, x_2, \ldots, x_L$:

$$y^k = (y_1{}^k(x), \ldots, y_L{}^k(x)).$$

Вектор y^k представляет собой L обучающих примеров и подается на вход сети поэлементно.

По входу вычисляется выход: $y^{k+1} \approx G(y^k, \alpha)$.

Формулируем ошибку $e^k = |\phi(y) - \phi_k(y^k)|$, которую в данном случае можно представить в дискретной форме:

$$e^k = \frac{1}{L}\sum_{i=1}^{L}(\phi(y_i) - \phi_{k+1}(y_i^{k+1}))^2 \to \min_{\alpha}.$$

Затем обучаем НС. Если в результате обучения достигается приемлемое значение ошибки, то считаем $y^*(x) = y^{k+1}(x)$ и заканчиваем итерационный процесс. В противном случае увиличиваем k на единицу и продолжаем процесс до тех пор, пока не будет достигнут.

В качестве начального решения $y^0(x)$ рекомендуется выбирать решение линеаризованного уравнения для исходного (4), т.к. решение линеаризованного уравнения и точное решение имеют одинаковые знаки при одинаковых аргументах.

В данной работе был рассмотрен алгоритм решения обыкновенного дифференциального уравнения первого порядка, разрешенного относительно первой производной. Но эту идею решения можно использовать и для уравнений высших порядков и систем обыкновенных дифференциальных уравнений.

ЛИТЕРАТУРА

1. Комарцова Л.Г. Нейрокомпьютеры: Учеб. пособие для вузов: 2-е изд., перераб. и доп. М.: Изд-во МГТУ им. Н. Э. Баумана, 2004. 400 с.

2. Агеев А.Д., Балухто А.Н., Бычков А.В. и др. Нейроматематика. Кн. 6: учеб. пособие для вузов / Общ. ред. А.И. Галушкина. М.: ИПРЖР, 2002. 448 с.

ПРОЕКТИРОВАНИЕ WEB-САЙТА «СИБИРСКОГО МЕДИЦИНСКОГО ЖУРНАЛА»

О.А. Серебренникова, студентка, каф. АОИ

г. Томск, ТУСУР, avayrin@gmail.com

Работа над созданием сайта включает в себя не только работы по программированию и разработке его дизайна. Одной из важных задач является разработка структуры проекта в целом как информационной, так и функциональной его составляющих. Цель данной работы на примере проекта сайта «Сибирского медицинского журнала» ФГБУ «НИИ кардиологии» СО РАМН – обозначить основные этапы проектирования и рассмотреть нечеткую систему как инструмент адаптации информационной структуры Web-сайта.

Процесс проектирования можно подразделить на 3 основные части:

1. Концептуальное проектирование.
2. Логическое проектирование.
3. Физическое проектирование.

Концептуальное проектирование служит для указания целей, задач сайта и определения аудитории, на которую он рассчитан, – выявление заинтересованных сторон и их требований, которые в соответствии с методологией RUP (Rational Unified Process) можно представить, как в табл. 1, а также составление бизнес-правил проекта (табл. 2) [1].

Таблица 1

Запросы заинтересованных сторон

Запросы заинтересованных сторон	Приоритет	Происхождение
Улучшить контроль за научной деятельностью сотрудников	Низкий	Руковод. одела межд. связей
Повысить доступность материалов, опубликованных в журнале	Средний	Читательская аудитория
Расширить читательскую аудиторию	Средний	Руковод. одела межд. связей
Повысить индексы цитируемости сотрудников	Высокий	Руковод. одела межд. связей
Повысить привлекательность журнала в научной среде	Средний	Руковод. одела межд. связей
Увеличить прибыль за счет новых способов рекламы	Средний	Руковод. одела межд. связей
Повысить рейтинг ФГБУ «НИИ кардиологии» СО РАМН среди научных организаций РФ	Средний	Руковод. одела межд. связей

Бизнес-правила отражают логику, на основании которой строится взаимодействие заинтересованных сторон, выявленных ранее, а также правила функционирования системы, для которой проектируется сайт [2]. Примеры таких бизнес-правил, характеризующих правила работы «Сибирского медицинского журнала», приведены в табл. 2.

Таблица 2

Бизнес-правила проекта

Бизнес-правила	Вид бизнес-правила
К каждой статье публикуется аннотация на русском и английском языках	Факт
Каждой статье соответствует список литературы в романском алфавите	Факт
Заглавие статьи публикуется на английском и русском языках	Факт
У журнала есть Международный стандартный номер	Факт
Журнал возлавляет редакционный совет	Факт
Существуют специальные правила оформления статей	Факт

На этапе логического проектирования следует описать структуру сайта и разработать прототип – схемы основных разделов (рис. 2).

Технологии, которые будут применяться на сайте, и используемое программное обеспечение определяются на этапе физического проектирования.

После завершения третьего этапа следует вернуться к концептуальному проектированию и проверить, не нужно ли внести изменения в связи с переосмыслением проекта на других стадиях.

На этапе проектирования важно заложить систему управления сайтом.

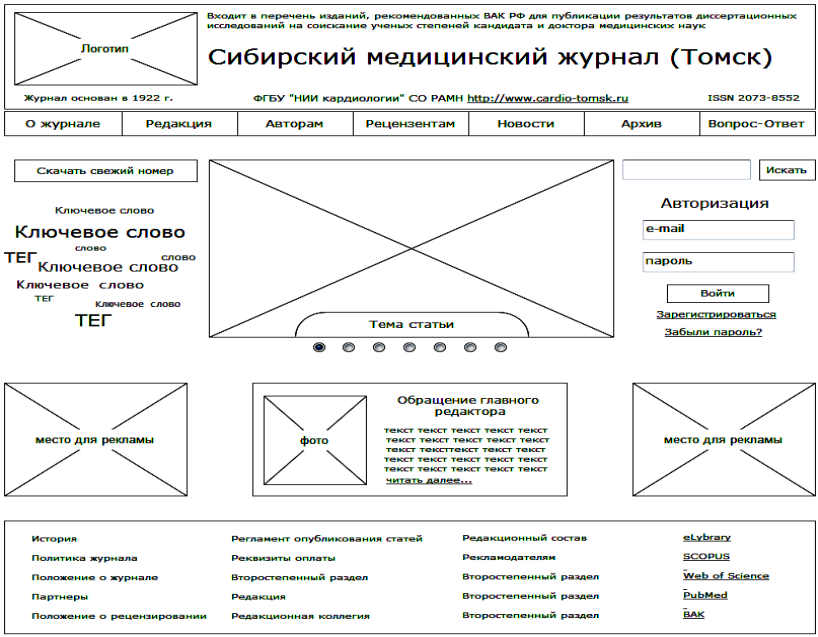


Рис 1. Схема главной страницы

Использование нечеткой системы может решить проблему эффективности информационной структуры сайта, а именно на основе статистических данных принимать решение, к примеру в контексте предметной области «Сибирского медицинского журнала», какие разделы более интересны конкретному пользователю по сравнению с другими темами. Так, во время очередного посещения сайта данному пользователю в первую очередь будут предложены новые медицинские статьи по интересующим его темам.

Заключение. Таким образом, проектирование позволяет определить границы системы, разработать наиболее оптимальную структуру web-сайта.

ЛИТЕРАТУРА

1. Крачтен Ф. Введение в Rational Unified Process. 2-е изд. М.: Изд. дом «Вильямс», 2002. 240 с.

2. Соловьев Д.А. Курс лекций по дисциплине «Проектирование ПАСОИУ» для студентов специальности 220200. Томск: ТУСУР, 2003. 25 с.

АЛГОРИТМ APRIORI. ЗАДАЧА ГЕНЕРАЦИИ АССОЦИАТИВНЫХ ПРАВИЛ ДЛЯ ПРОДВИЖЕНИЯ ТОВАРОВ В ИНТЕРЕНТ-МАГАЗИНЕ

Д.С. Синьков, аспирант

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

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

Впервые задача поиска ассоциативных правил (association rule mining) была предложена для нахождения типичных шаблонов покупок, совершаемых в супермаркетах, поэтому иногда ее еще называют анализом рыночной корзины (market basket analysis). Рыночная корзина – это набор товаров, приобретенных покупателем в рамках одной отдельно взятой транзакции [1].

Транзакция – это множество событий, которые произошли одновременно. Регистрируя все бизнес-операции в течение всего времени своей деятельности, торговые компании накапливают огромные собрания транзакций. Каждая такая транзакция представляет собой набор товаров, купленных покупателем за один визит. Полученные в результате анализа шаблоны включают перечень товаров и число транзакций, которые содержат данные наборы. Транзакционная или операционная база данных представляет собой двумерную таблицу, которая состоит из номера транзакции и перечня покупок, приобретенных во время этой транзакции [1].

Пусть $\mathbf{I} = \{i_1, i_2, i_3, \ldots i_n\}$ – множество (набор) товаров, называемых элементами. Пусть **D** – множество транзакций, где каждая транзакция **T** – это набор элементов из $\mathbf{I}$, $\mathbf{T} \in \mathbf{I}$. Каждая транзакция представляет собой бинарный вектор, где $t[k]=1$, если i_k элемент присутствует в транзакции, иначе $t[k]=0$. Транзакция **T** содержит **X**, некоторый набор элементов из **I**, если $\mathbf{X} \in \mathbf{T}$. Ассоциативным правилом называется импликация $\mathbf{X} \Rightarrow \mathbf{Y}$, где $\mathbf{X} \in \mathbf{I}$, $\mathbf{Y} \in \mathbf{I}$ и $\mathbf{X} \cap \mathbf{Y} = \varnothing$. Правило $\mathbf{X} \Rightarrow \mathbf{Y}$ имеет поддержку s (support), если s% транзакций из ***D*** содержат $\mathbf{X} \cup \mathbf{Y}$,

$supp(\mathbf{X} \Rightarrow \mathbf{Y}) = supp(\mathbf{X} \cup \mathbf{Y})$. Достоверность правила показывает, какова вероятность того, что из **X** следует **Y**. Правило $\mathbf{X} \Rightarrow \mathbf{Y}$ справедливо с достоверностью (confidence) c, если c% транзакций из $\boldsymbol{D}$, содержащих **X**, также содержат **Y**, $conf(\mathbf{X} \Rightarrow \mathbf{Y}) = supp(\mathbf{X} \cup \mathbf{Y})/supp(\mathbf{X})$ [2].

В работе приводится описание применения алгоритма APRIORI для генерации ассоциативных правил для интернет-магазина ресторана доставки. Также будет рассмотрено применение ассоциативных правил для продвижения товаров магазина.

Алгоритм APRIORI. На первом шаге алгоритма подсчитываются одноэлементные часто встречающиеся наборы. Для этого необходимо пройтись по всему набору данных и подсчитать для них поддержку, т.е. сколько раз встречается в базе.

Следующие шаги будут состоять из двух частей: генерации потенциально часто встречающихся наборов элементов (их называют кандидатами) и подсчета поддержки для кандидатов.

Ниже приведено описание алгоритма.

Вход. Транзакционная база, минимальная поддержка, минимальная достоверность.

Выход. Ассоциативные правила.

Шаг 1. Сгенерировать часто встречающиеся одноэлементные наборы, $k = 1$.

Шаг 2. Для $k > 1$ сгенерировать кандидатов на включение в часто встречающиеся множества.

Шаг 3. Удалить кандидатов, поддержка которых меньше заданной минимальной.

Шаг 4. Если кандидатов на включение в часто встречающиеся множества нет, перейти к шагу 5, иначе $k = k + 1$, перейти к шагу 2.

Шаг 5. Для каждого часто встречающегося набора $\boldsymbol{F_i}$ найти все его непустые подмножества. Для каждого непустого подмножества s сформировать правило $s \Rightarrow (F_i - s)$, если достоверность правила $supp(F_i)/supp(s)$ не меньше заданной.

Шаг 6. Окончание работы.

Описание программного комплекса. За время существования магазина накопилась история покупок пользователей. Задача состоит в том, чтобы сформировать ассоциативные правила по историческим данным и на основании их советовать пользователям сопутствующие товары.

Программный комплекс состоит из 2 частей: интернет-магазин и программа анализа покупательской корзины. Магазин написан на языке PHP (CakePHP), база данных MySQL, программа анализа на языке C#.

После работы программа анализа генерирует файлы products.js и rules.js. Products.js содержит наименования товаров содержащихся в правилах, rules.js содержит массив правил в формате JSON. Данные файлы подключаются на сайт магазина. Далее при добавлении товара в корзину происходит поиск соответствующего правила, и если оно найдено, на сайте появляется сообщение о том, что пользователю, возможно, понравится определенный товар (рис. 1).

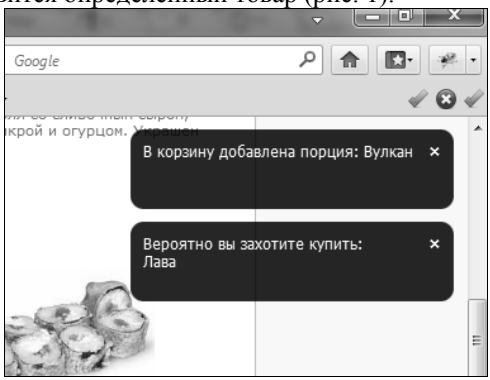


Рис.1. Окно программы анализа, сгенерированные ассоциативные правила

Если найдено несколько правил с одним товаром, то в сообщении выведутся все сопутствующие товары из найденных правил.

ЛИТЕРАТУРА

1. Чубукова И.А. Data Mining [Электронный ресурс]. Режим доступа к сайту: http://www.intuit.ru/department/database/datamining/15.

2. Apriori – масштабируемый алгоритм поиска ассоциативных правил. [Электронный ресурс]. Режим доступа к сайту: http://www.basegroup.ru/library/analysis/association_rules/intro/

СТРУКТУРА СИСТЕМЫ АВТОНОМНОГО ТЕСТИРОВАНИЯ ПРОГРАММ

В.А. Соловьёв*, *студент 3-го курса каф. АСУ

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

г. Томск, ТУСУР, ФСУ, SoVictor_tomsk@hotmail/com

В последнее время олимпиады по спортивному программированию стали популярны среди студентов вузов. Еженедельно различные сайты проводят всё новые и новые соревнования по правилам, предложенным корпорацией ACM [1]. От прочих олимпиад они выгодно отличаются тем, что субъективный фактор в оценке сведён на нет: по-

верка решений участников полностью автоматизирована и возложена на сервер. Помимо этого, за счёт очень быстрой проверки появляется возможность показывать результаты в реальном времени, отображая текущий рейтинг участника.

Такой подход, очевидно, пригоден не только для олимпиад. Автономное тестирование с лёгкостью впишется в учебный процесс, освобождая, с одной стороны, учителя от рутинной работы, а с другой – не оставляя студентам повода для сомнений в объективности оценки. Кроме того, отражение результатов в реальном времени привносит в учебный процесс элементы соревнования, соперничества. Всё, что требуется от преподавателя, – единожды составить набор тестов для каждой задачи, всё остальное возьмёт на себя тестирующая система.

Что же представляет собой эта система? Как уже упоминалось выше, обрабатывает поступившие от участников решения сервер. Его важнейшая часть – ядро тестирующей системы – принимает на вход исходный код программы, проверяет его на соответствующем задаче наборе тестов, сопоставляя полученные результаты с эталоном, и выносит вердикт, полностью отражающий результат прохождения программой тестов (рис. 1).

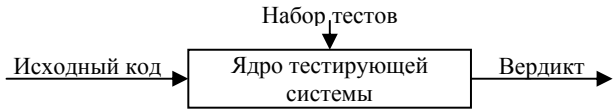


Рис. 1 Диаграмма процесса тестирования

Пользователь через сайт посылает своё решение задачи серверу, сервер запрашивает набор тестов у БД, решение проверяется тестирующей системой, после чего, на основе вердикта, сервер формирует возвращаемые сайту результаты (рис. 2).

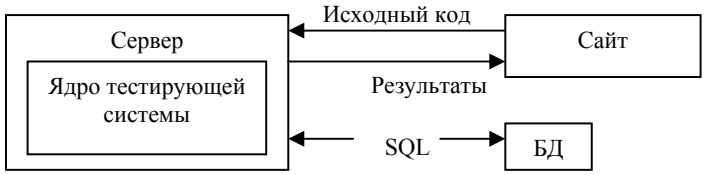


Рис. 2 Упрощённая схема системы тестирования программ

Учитывается не только то, как прошла тесты данная попытка решения, но и сколько попыток было до неё, сколько времени прошло с начала олимпиады (или, например, с начала пары, в случае учебного процесса). Сайт в свою очередь использует эти результаты для построения итоговой таблицы.

Информация о пользователях, олимпиадах, задачах и попытках их сдачи сохраняется в базе данных. Возможен подсчёт различных статистических данных.

При работе над проектом использовался фреймворк Ruby on rails, поддерживающий развивающийся язык программирования Ruby [2] для Web-разработки, языки C++ и BATCH для ядра системы. Для хранения данных использована СУБД PostgreSQL. Использование новых инструментов позволяет добиться большего быстродействия на фоне аналогов, обеспечить лёгкость разработки и сопровождения, а также сделать работу с системой максимально удобной для пользователя.

Помимо прочих достоинств, описанная система позволяет уже после завершения олимпиады симулировать участие в ней. Все данные о посланных решениях хранятся в базе данных. В ходе симуляции, по мере того как проходит время с её начала, попытки участников извлекаются из базы данных и учитываются при построении итоговой таблицы наряду с попытками нового пользователя. В спортивном программировании это позволяет оценить свои возможности, потягавшись с участниками уже прошедших олимпиад, в учебном процессе – оценить способности студента, отсутствовавшего во время тестирования после его окончания. Отметим, что данная возможность нашей системы не реализована в большинстве существующих аналогов.

Проект ГПО АСУ-1101 – «Программное обеспечение для организации и проведения спортивного программирования».

ЛИТЕРАТУРА

1. Командный чемпионат мира по программированию ACM 2011/2012. Северо-Восточный Европейский регион / Под ред. В.Н. Васильева, В.Г. Парфенова. СПб.: НИУ ИТМО, 2011. 254 с.

2. Sam Ruby, Dave Thomas, David Hansson. Agile Web Development with Rails. Fourth Edition. R.: The Pragmatic Bookshelf, 2011. 474 p.

АВТОМАТИЧЕСКИЙ СБОР, ОБРАБОТКА И РУБРИКАЦИЯ НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ

А.В. Ямшанов, студент каф. КСУП

Научный руководитель Р.В. Мещеряков, доцент каф. КИБЭВСв, к.т.н.

г. Томск, ТУСУР, jav@kcup.tusur.ru

На протяжении многих веков информация была одним из важнейших ресурсов человечества, желание владеть информацией становилось поводом для войн, а тот, кто мог изменять информацию, мог изменять мир. Современный мир не становится исключением, разве что кровавые кровопролития переросли в информационную войны, где

стали проявляться в виде гонки технологий, гонки вооружений, биржи и т.д.

Уникально быстрый скачок в развитии Интернета дал не только большое количество информации и большое количество свободы для этой информации, но также и большое количество проблем, таких как (это лишь краткая часть списка):

− стремительно увеличивающийся объем информации, которую необходимо обработать;

− сложность подтверждения достоверности информации;

− увеличивающаяся сложность автоматического поиска необходимой информации вследствие её уменьшающейся формализованности.

Проблема автоматического поиска существует уже давно, и множество задач успешно решается внутри таких корпораций, как Google или Yandex, которые достаточно успешно начали предлагать не результаты, основываясь не только на том что вы задаёте в поисковом запросе, но и на портрете вашего интернет-эго, делая поиск действительно персонализированным [1].

По сути, из такой специализации, но ещё более узкой, чем уже решаемая поисковыми системами, вытекает наша задача. Требуется ещё одно решение, причём менее универсальное. Рассмотрим предпосылку предлагаемой для решения задачи.

Этой предпосылкой являются большие временные затраты на поиск и поддержание актуальности базы существующих в мире программ грантов и планирующихся научных конференций. Задача не нова и успешно решается. Для её выполнения необходимо несколько шагов (рис. 1).

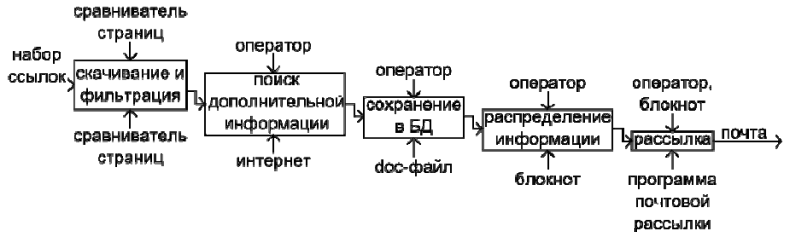


Рис. 1. Диаграмма существующего процесса

• По заранее заданной базе ссылок получить множество страниц, найти на них новые правки и отфильтровать эти правки по какому-либо заданному критерию.

• По уже уменьшенной базе новых и интересующих правок найти необходимую нам дополнительную информацию (например, скачать pdf/doc с правилами конференции), складывая их в общую базу.

• Основываясь на базе полной информации о интересующих нас конференциях/грантах и базе о тех, кому эта информация интересна, распределить найденную информацию.

Однако есть множество факторов, которые сильно ограничивают уже существующее решение проблемы:

1. Оператор – механизм. Почти во всех происходящих процессах оператор является не только средством контроля, но и механизмом необходимым для протекания процесса. Он вынужден вручную осуществлять множество рутинных действий, быть связующим механизмом между модулями, хранить большую часть данных в голове и т. д., что делает его если не самым слабым звеном в системе, то самым медленным. Увеличение масштаба поиска линейно увеличит время, затрачиваемое на этот поиск.

2. Закрытость программ. Несмотря на то, что использующиеся программы решают возложенные на них задачи, они бы могли решать их намного эффективнее, если бы их можно было немного модифицировать. Но, к сожалению, такая возможность отсутствует. Разработка своей системы решит эту проблему, а также проблему с лицензированием программ.

Предлагая свое решение этой задачи, мы надеемся решить несколько задач (основной список):

1. Сильно персонализированный поиск. Пользователю должна предлагаться только та информация, которая ему интересна.

2. Предложить удобный инструмент для решения уже существующей задачи с поиском и поддержанием актуальной базы по существующим программам грантов и научным конференциям.

3. Исследовать проблему поиска информации. Написать интеллектуальную систему поиска и обработки информации, основанную на морфологическом разборе текста.

Для эффективного решения этой задачи предлагается использовать следующие средства:

• Итеративная разработка с наращиванием функционала. Это позволит:

− быстро выпустить работающую программу для удовлетворения требования заказчика;

− увидеть дальнейшие тенденции развития программы;

− набрать базу длядальнейшего исследования.

• Разработка программы с использованием методологии IoC/DI [2]. Это позволит:

− итеративно разрабатывать программу, легко меняя программные блоки с одной реализации на другую.

− упростить разработку программы, и сделать её архитектуру более прозрачной.

− легко конфигурировать возможности программы на стадии её реального использования

• Разработка будет вестись на языке Python. Это даст следующие преимущества:

− Python – это язык который обладает почти самым минималистическим синтаксисом и высокой скоростью разработки программы. Таким образом сильно сокращается время разработки прототипа;

− богатая библиотека и активное сообщество. Большинство рутинных задач решено за нас;

− открытая лицензия;

− лёгкое размещение на серверах, облаках, GAE [3].

Таким образом, поставлена задача – на основе существующей системы разработать новую, в основе которой будет заложен морфологический разбор текста и почти полная автоматизация обработки необходимой информации.

ЛИТЕРАТУРА

1. Search plus Your World: Personal results. URL: http://support.google.com/websearch/bin/answer.py?hl=ru&answer=1710607 (дата обращения: 29.02.2012).

2. Inversion of Control Containers and the Dependency Injection pattern. URL: http://martinfowler.com/articles/injection.html (дата обращения: 29.02.2012).

3. Google App Engine. URL: http://code.google.com/intl/ru-RU/appengine/ (дата обращения: 01.02.2012).

МНОГОКРИТЕРИАЛЬНАЯ ОПТИМИЗАЦИЯ, ПОСТРОЕНИЕ ПАРЕТО-ФРОНТА

Н.Н. Земцов, И.С. Корниенко, студенты каф. АОИ

Научный руководитель И.А. Ходашинский

г. Томск, ТУСУР, nike-blitz@yandex.ru, zloi.linux@gmail.com

Постановка задачи. Часто, в связи тем, что количество правил нечеткой системы, при использовании всех возможных комбинаций термов $m = \prod_1^n t_n$, где t_n – количество термов определенных на n-й переменной, мы сталкиваемся с огромной базой правил – эффект «проклятия размерности» (чем шире постановка задачи, тем больше сопутствующих данных). Работа с большим количеством правил повышает время выполнения расчетов в информационной системе и делает очень сложным интерпретацию их человеком. Также изначально, в системе могут присутствовать переменные, которые не оказывают значитель-

ного влияния на вывод, но при этом затрудняют вычисления и понимание структуры системы.

Выбор критерия сложности

Обозначим: n – количество переменных; t_n – количество термов определенных на n-й переменной; $m = \prod_1^n t_n$ – количество правил.

Определим сложность системы C как количество термов, непосредственно участвующих в выводе умноженных на количество правил.

После начальной инициализации системы $C=m+(t_n*n)$ (у нас m правил, если части каждого из которых n переменным поставлены в соответствие термы), то есть максимально полная структура системы.

Будем считать, что при $C = 0$ ошибка $E = +\infty$.

Задача – сформировать группу решений, удовлетворяющих требованиям либо по сложности нечеткой системы, либо по её ошибке.

Заданный критерий определяется выражением

$$Q_C(S) = \begin{cases} C, & \text{при} \quad E < E_{\max}, \\ \infty, & \text{иначе}, \end{cases}$$

где Q_C – критерий оптимальности по параметру «сложность» (C), сложность нечеткой системы со структурой S; E – ошибка нечеткой системы при данной структуре и параметрах; $E_{\max}$ – максимальная на данный момент ошибка нечеткой системы; C – сложность нечеткой системы с текущей структурой; S – структура нечеткой системы, для которой определяется значение критерия.

Данный критерий позволит производить анализ во множестве различных структур нечеткой системы и выбирать наиболее оптимальную структуру, используя сложность нечеткой системы как величину, характеризующую систему целиком.

Нечеткая система оптимальна по заданному критерию Q_C, если значение этого критерия для данной конфигурации системы меньше или равно пороговому значению критерия (устанавливается пользователем/экспертом).

Оптимальность по Парето – такое состояние системы, при котором значение каждого частного критерия, описывающего состояние системы, не может быть улучшено без ухудшения положения других элементов.

Таким образом, по словам самого Парето, «всякое изменение, которое никому не приносит убытков, а некоторым людям приносит пользу (по их собственной оценке), является улучшением». Значит,

признаётся право на все изменения, которые не приносят никому дополнительного вреда [1].

Взаимодействие нечеткой системы и метода настройки

Обозначим структуру нечеткой системы в виде бинарного вектора $X = t_n*n+m$, где t_n – количество термов для n-й переменной; n – количество переменных; m – количество правил.

Значение $x \in X$ может принимать {0; 1}, если 0 – элемент отсутствует в выводе, иначе присутствует. Фактически сложность это количество единиц в X. Тогда построение Парето-фронта сводится к:

Шаг 1. В системе задается параметр i – количество значений в Парето-фронте.

Шаг 2. Нечеткая система передает методу настройки, на какой сложности необходимо настроить систему.

Шаг 3. Настройка методом, возвращаются в систему оптимальные параметры и структура при заданной сложности (одна точка на Парето-фронте).

Шаг 4. $iter = iter+1$; сложность изменяется на следующее значение.

Шаг 5. Если $iter < i$ то переход к шагу 2, иначе шаг 6.

Шаг 6. Вывод Парето-фронта.

Шаг 7. Принятие экспертом решения из Парето-фронта, которое необходимо применить к системе.

Заключение

Предложенное взаимодействие нечеткой системы и метода настройки позволяет построить Парето-фронт с заданным количеством точек и равномерно распределенным по сложности.

ЛИТЕРАТУРА

1. Подиновский В.В., Ногин В.Д. Парето-оптимальные решения многокритериальных задач. М.: Наука, 1982.

СЕКЦИЯ 17

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

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

АВТОМАТИЗАЦИЯ УЧЕТА РАБОЧЕГО ВРЕМЕНИ СОТРУДНИКОВ ТОМСКОГО ЦЕНТРА ОВД

Т.А. Афиркина, студентка 5-го курса
г. Томск, ТУСУР, каф. АСУ

Широкое внедрение информационных технологий во все сферы деятельности связано с их способностью быстро и безошибочно обрабатывать и хранить большие объемы информации. Применение информационных систем на предприятиях позволяет многократно повышать производительность труда сотрудников. Широкий выбор разработанных языков и сред программирования и СУБД позволяет создавать информационные системы с необходимым функционалом, отвечающие всем требованиям заказчика.

До настоящего времени Томский центр обеспечения воздушного движения (ОВД) осуществлял учет рабочего времени сотрудников с минимальным уровнем автоматизации, с использованием пакета офисных программ Microsoft Office. Для учета рабочего времени сотрудников разных подразделений использовались не связанные между собой формы ввода данных, перенос в общую базу осуществлялся вручную, что приводило к частым ошибкам. Кроме того, ранее введенные данные могли изменяться. Следовательно, необходимо было контролировать изменения и вносить их в зависящие данные. Была разработана информационная система, которая позволила автоматизировать данные процессы, облегчив тем самым рутинную работу сотрудников.

Информационная система (ИС) объединила в одном программном продукте весь спектр задач учета рабочего времени на предприятии.

Проектирование системы было начато с изучения предметной области, рассмотрения аналогов, выбора средств реализации проекта, построения функциональной модели системы и концептуальной модели базы данных**.**

При рассмотрении представленных на рынке программных продуктов были выявлены недостатки, не позволяющие внедрить данное

ПО на предприятии: избыточный или недостаточный функционал, необходимость установки дополнительного оборудования или ПО, невозможность импорта данных, невозможность использования на территориально удаленных друг от друга объектах, высокая цена (более 1000 евро).

Основными факторами, влияющими на принятие решения о выборе среды программирования для реализации системы, были следующие:

– возможность создания приложения для ОС Windows;

– возможность доступа, простота, эффективность работы с БД;

– простота создания дружественного интерфейса;

– наличие средств создания печатных выходных форм;

– возможность реализации обмена данными с MS Excel;

– надежность работы среды разработки.

Наиболее оптимальным решением при выборе средства реализации ИС стала платформа «1С: Предприятие 8.0».

Разработанная система обеспечивает хранение постоянной и условно-постоянной однотипной информации, ведет учет отработанного сотрудниками времени, формирует выходные документы. Информационная система выполняет следующие функции:

– составление годовых графиков работы сотрудников;

– составление ежемесячных табелей отработанного времени;

– оперативное получение информации о месячном и годовом балансе рабочего времени каждого сотрудника.

Основные компоненты ИС приведены ниже.

Справочник «*Структурные подразделения»* содержит сведения о подразделениях организации и их иерархической подчиненности.

Справочник «*Должности»* содержит список должностей, имеющихся в организации.

Справочник *«Сотрудники организации»* содержит сведения о сотрудниках организации.

Справочник *«Типовые графики сменности»* содержит информацию о типовых графиках, на основании которых составляются годовые графики рабочего времени сотрудников.

Справочник *«Вид рабочего времени в графике»* содержит перечень условных обозначений затрат рабочего времени, используемых в годовых графиках, и используется для установления соответствия между обозначениями в графике и в табеле учета использования рабочего времени.

Справочник *«Классификатор использования рабочего времени»* содержит перечень условных обозначений затрат рабочего времени, используемых в табеле учета использования рабочего времени.

Документ *«Годовой график рабочего времени»* используется для составления графика работы на год и контроля за соблюдением годового баланса рабочего времени.

Документ *«Табель учета использования рабочего времени»* применяется для учета времени, фактически отработанного и (или) не отработанного каждым работником организации, для контроля за соблюдением работниками установленного режима рабочего времени, для получения данных об отработанном времени, а также для составления статистической отчетности по труду.

Отчеты по использованию рабочего времени сотрудниками организации позволяют предоставить пользователю интересующую его информацию об отработанном времени любого сотрудника, сотрудников определенного подразделения или в целом по центру.

Разработка системы и внедрение ее на предприятии позволило сократить непроизводительный труд от внесения повторяющихся данных, что обеспечило экономическую выгоду и позволило уменьшить степень совершаемых ошибок при вводе и обработке информации.

РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО УСТРОЙСТВА ДЛЯ НАПЫЛЕНИЯ ПРОСВЕТЛЯЮЩИХ ПОКРЫТИЙ

А.В. Андрианова*, *студентка 3-го курса;
И.А. Паргачёв*, *аспирант каф. ЭП
Научный руководитель Л.Я. Серебренников, доцент каф. ЭП, к.т.н.
г. Томск, ТУСУР, ФЭТ,andrianova_anast @mail.ru

Одной из важных задач для электрооптики является нанесение просветляющих покрытий на элементы устройств основанных на нелинейно-оптических кристаллах. Но при изготовлении таких покрытий возникает ряд сложностей, связанных с расчетом распределения толщин слоев по поверхности элемента, недостаточной точности контроля толщины слоев в процессе осаждения, подбором плёнкообразующих материалов [1]. Разработка автоматизированного устройства для напыления просветляющих покрытий сократит участие человека в процессе до выбора длин волн, на которых требуется просветление.

Автоматическое устройство напыления включает в себя блок расчета показателей преломления напыляемых материалов и моделирования процесса напыления. Концепция модели процесса определяется методом контроля толщины оптического покрытия. Наиболее точный на сегодня метод контроля толщины покрытия основан на интенсивности отраженного лазерного пучка от оптической грани кристалла. Использование такого метода контроля толщины покрытия предполагает

задание технологических процессов в виде зависимости интенсивности отраженного пучка от толщины пленки.

На рис. 1 представлен алгоритм работы модуля, рассчитывающего показатели преломления необходимых для напыления материалов и моделирования технологического процесса.

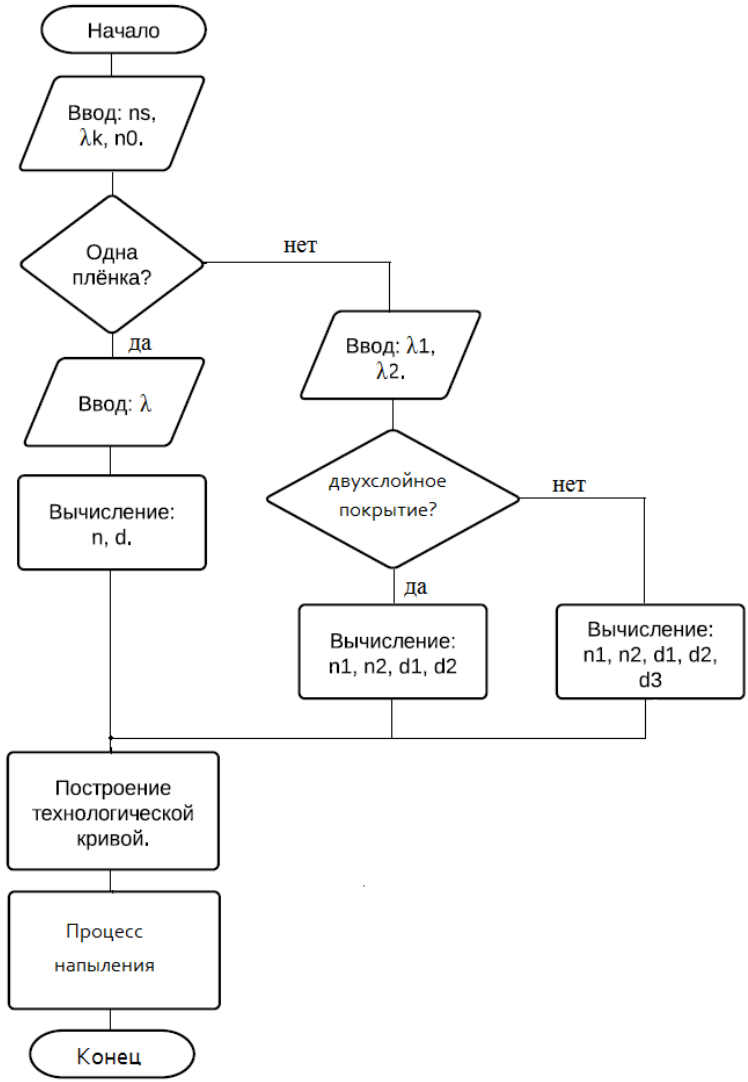


Рис. 1. Алгоритм расчета и построения технологической кривой напыления

На начальном этапе программы вводится значение длины волны контрольного лазера (λ_k), показателя преломления среды (n_s) и кристалла (n_0). Далее следует логический блок, где оператор выбирает количество длин волн, на которых нужно просветление. В случае с однослойным покрытием программа запрашивает ввод значений длины волны (λ) и рассчитывает по формулам Френеля оптимальные значения коэффициента преломления напыляемого материала (n), а также толщину плёнки (d). При расчете многослойного покрытия требуется рассчитать коэффициенты преломления нескольких материалов, последовательность их напыления и толщину каждого слоя. Тип конструкции подбирается с учетом заданных параметров. После расчетов строится технологическая кривая напыления просветляющих покрытий (рис. 2) и передается в блок управления процессом напыления.

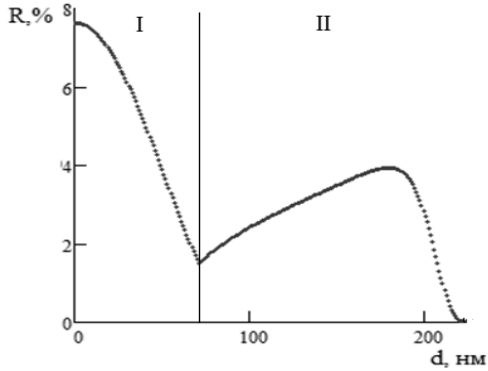


Рис. 2. Теоретическая кривая интенсивности отражения излучения с длиной волны 660 нм от толщины пленок MgF_2 и SiO_2 напыляемых на кристалл KTP

Расчетный модуль будет реализован на одном из языков программирования. На данном этапе проделана основная аналитическая работа: изучены методы расчета параметров просветляющих покрытий, проведен ряд экспериментов по напылению плёнок на кристаллы KTP. Полученные данные являются основой разрабатываемого устройства и оптимизации расчетного блока.

Работа выполнена в рамках Госзадания Минобрнауки РФ на 2012 год (проект 7.2647.2011) и ФЦП «Научные и научно-педагогические кадры инновационной России» (госконтракт № 02.740.11.0553).

ЛИТЕРАТУРА

1. Путилин Э.С. Оптические покрытия: учеб. пособие. СПб.: СПбГУ ИТМО, 2010. 227 с.

ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА И КОНТРОЛЯ ТРАНСПОРТНЫХ СРЕДСТВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ СЛУЖБЫ «ГОСТЕХНАДЗОР» ХМАО–ЮГРЫ

Я.В. Архипов*, *студент кафедры АСУ
Научный руководитель А.И. Исакова, *доцент кафедры АСУ*, *к.т.н.*
г. Томск, *ТУСУР*, *ФСУ*, *drkdobryak@mail.ru*

Средства автоматизации должны внедряться в сферу управления путём создания комплексных автоматизированных систем управления, охватывающих определённые области народного хозяйства, ибо только в этом случае обеспечивается высокая эффективность средств автоматизации. Внедрением таких систем достигается освобождение аппарата центральных и местных органов управления от трудоёмких расчётных работ (если при этом общая численность персонала даже не уменьшается, сами задачи планирования и управления ставятся на качественно высшую ступень); коренное улучшение качества принимаемых решений и обеспечение должной оперативности руководства на всех уровнях управления, что обеспечивается соответствующим агрегированием и фильтрацией избыточной информации техническими средствами [1].

В настоящее время на рынке РФ представлены разнообразные системы автоматизации учета транспортных средств. В большинстве случаев эти системы общего характера без учёта конкретных узконаправленных задач, что накладывает ограничения на внедрение этих систем в специализированные предприятия.

Для службы «Гостехнадзор» ХМАО–Югры, которая занимается учетом и контролем транспортных средств специального назначения, разработана собственная информационная система, которая позволяет решать следующие задачи:

– экономия трудовых ресурсов при выполнении процессов преобразования информации;

– сокращение рутинных операций при выполнении расчетов;

– увеличение уровня качества информации за счет сокращения ручного труда;

– повышение эффективности работы специалистов за счет оперативной обработки информации;

– уменьшение ошибок в расчетах за счет автоматизации.

Разработанная информационная система выполняет функции:

– сбор, хранение, обработка и выдача необходимой информации для выполнения инспектором Гостехнадзора определенных функций;

– создание выходной документации и отчетности.

Для регистрации транспортного средства в службу «Гостехнадзор» предоставляют следующие документы: копию паспорта, ПТС (паспорт технического средства), заявление о постановке на учёт. В итоге владелец транспортного средства получает свидетельство о регистрации.

Для автоматизации формирования путевого листа специального автомобиля нужны данные из свидетельства о регистрации, водительского и служебного удостоверений лица, которому будет выдаваться путевой лист, а также текущие показания одометра на начало поездки и по её завершении для учёта расхода ГСМ.

На основании зарегистрированных транспортных средств инспектор может сформировать отчеты о всех транспортных средствах по владельцам, о зарегистрированных личных транспортных средствах каждой инспекции, а также по группам зарегистрированных транспортных средств в каждой инспекции.

Наиболее оптимальным решением при выборе средства реализации ИС стала типовая конфигурация платформы «1С: Предприятие 8.0».

Таким образом, разработанная ИС содержит 13 справочников, 8 видов документов, 5 отчетов. Система внедрена и проходит опытную эксплуатацию в службе «Гостехнадзор» ХМАО–Югры.

ЛИТЕРАТУРА

1. Академик – Автоматизация управленческих работ [Электронный ресурс]. Режим доступа: http://dic.academic.ru/dic.nsf/bse/Автоматизация управленческих работ.

УСТАНОВКА МИКРОКЛИМАТА ДОМАШНИХ РАСТЕНИЙ

В.Е. Долгушин*, *студент 5-го курса каф. КИБЕВС
Научный руководитель Л.А. Торгонский, *доцент каф. КИБЭВС*
г. Томск, *ТУСУР*, *ФВС*, *Dolgvadim@gmail.com*

Выращивание растений в домашних условиях имеет свои особенности. Для успешного результата необходимо обеспечить благоприятные условия, приближенные к климату естественной среды обитания. Следует учитывать такие параметры, как температура, влажность, длительность светового дня и количество осадков. Миллионы людей по всему миру занимаются домашним выращиванием растений и зачастую прибегают к использованию различных технических решений для создания благоприятного микроклимата и автоматизации установок выращивания.

В настоящее время существует большое разнообразие домашних теплиц и мини-оранжерей, позволяющих создавать необходимые ус-

ловия для успешного развития даже самых прихотливых растений, независимо от особенностей региона. Но представленные для частных лиц на рынке решения не обеспечивают достаточного контроля над параметрами микроклимата, требуют постоянного участия человека в процессе выращивания и являются дорогостоящими установками.

Целью настоящей работы является разработка конструктивных и технических решений по устройству и автоматизации домашней мини оранжереи.

Анализ подобных устройств позволяет заключить что предлагаемая установка должна иметь:

– защиту от воздействий внешней среды;
– регулируемое освещение;
– регулируемый воздухообмен;
– удобную систему контроля и регулировки параметров микроклимата (температура, влажность, длительность светового дня, воздухообмен);
– автоматизацию процесса полива растений.

Исходя из описанных выше требований, предлагается в качестве основы использовать конструкцию установки микроклимата «Гроубокс» (Grow Box) [1], которая представляет собой теплоизолированный шкаф, оборудованный искусственным освещением и вентиляцией. Для обеспечения необходимых параметров микроклимата в этой установке, предлагается использовать устройство управления с микроконтроллером.

Для автоматизации процесса поддержания микроклимата в установке применено устройство управления, структурная схема которого приведена на рис. 1. В устройстве применён набор датчиков, исполнительных устройств, подготовлены и отлажены алгоритмы и программы контроля параметров процесса и управления исполнительными устройствами [2].

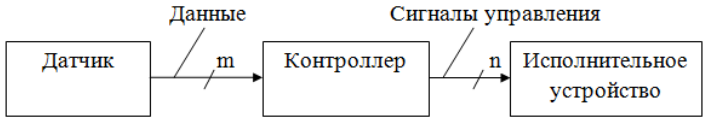


Рис. 1. Структурная схема устройства управления

Контроль и изменение параметров микроклимата осуществляется через персональный компьютер, связанный с устройством управления. Для этого предлагается использовать протокол последовательной передачи SPP (Serial Port Protocol) беспроводной связи bluetooth, что из-

бавит пользователя от необходимости находиться в непосредственной близости к установке [2, 3].

Программное обеспечение ПК должно обеспечивать поиск и связь с устройством управления установки по технологии bluetooth, принимать и наглядно отображать текущие параметры среды установки, вести журнал изменений и предоставлять пользователю возможность задать желаемые параметры микроклимата.

Результаты работы отражают содержание проекта установки микроклимата, в которой при минимальном участии пользователя контролируются и регулируются показатели среды жизнеобеспечения домашних растений.

ЛИТЕРАТУРА

1. Строим сами. Что такое гроубокс, grow box? [Электронный ресурс]. URL: http://diynow.ru/grow-box (дата обращения: 18.02.2010).

2. Голубцов М.С. Микроконтроллеры AVR: от простого к сложному. М.: СОЛОН-Пресс, 2003. 288 с.

3. Беделл П. Сети. Беспроводные технологии. М.: НТ-Пресс, 2008. 448 с.

КРИТЕРИЙ ВЫБОРА БАЗИСОВ ДЕКОРРЕЛИРУЮЩИХ ПРЕОБРАЗОВАНИЙ, ПОЛУЧАЕМЫХ ИЗ СОСТОЯНИЙ РАЗВИТИЯ КЛЕТОЧНОГО АВТОМАТА

О.О. Евсютин*, *аспирант каф. КИБЭВС

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

г. Томск, ТУСУР, eoo@keva.tusur.ru

Изменяя значения параметров клеточного автомата на разбиении и рассматривая различные истории его развития, можно получить достаточно большое количество различных ортогональных базисов [1, 2]. Вследствие этого появляется вопрос: каким образом выбирать базисы декоррелирующих преобразований для последующего использования в составе методов сжатия цифровых изображения из множества получаемых?

Критерий такого отбора можно сформулировать в терминах концентрации энергии [3], осуществляемой декоррелирующим преобразованием, когда большая часть информации исходной последовательности данных сосредоточивается в одной или нескольких низкочастотных составляющих.

Здесь возможны три случая:

- Наиболее значимой является одна низкочастотная составляющая, приближенная к среднему значению преобразуемых элементов данных.

- Наиболее значимыми являются две и более низкочастотные составляющие, приближенные к локальным средним значениям преобразуемых элементов данных. Следует отметить, что данный случай можно разбить на два и более, если ввести некоторое пороговое значение количества низкочастотных составляющих.
- Построенный базис не разделяет элементы данных на частотные составляющие, то есть равномерно распределяет энергию по всем преобразованным элементам данных.

Интерес для исследования представляют базисы, свойства которых соответствуют первым двум случаям, в то время как преобразования, не обладающие способностью к разделению элементов данных на частотные составляющие, нельзя отнести к декоррелирующим.

Таким образом, при исследовании характеристик ортогонального базиса сначала необходимо определить количество низкочастотных составляющих среди преобразованных элементов данных. Это можно сделать с помощью преобразования исследуемым базисом специальным образом выбранной последовательности, обладающей пространственной избыточностью. Кроме того, при исследовании базисов декоррелирующих преобразований наряду с количеством низкочастотных составляющих крайне важным является их расположение среди элементов преобразованной последовательности данных, поскольку оно определяет порядок обхода последовательности при подготовке к непосредственному сжатию.

С учетом всего вышесказанного критерий выбора базиса, построенного из состояний развития клеточного автомата на разбиении, представленный в виде алгоритма, будет выглядеть следующим образом.

Критерий выбора базисов декоррелирующих преобразований

Вход:

натуральное $N \geq 2$;

целое $m \geq 0$;

вектор-строка $F = (f_i)_{i=1}^{N},\ f_i \in \{0,...,m-1\}$;

вектор-строка $H = (h_i)_{i=1}^{N},\ h_i \in \{0,1\}$;

матрица $C = (c_{ij})_{i=1,\,j=1}^{N,N}$;

целое $0 \leq r \leq N$;

целое $k > 0$.

Выход:

Ответ на вопрос: соответствует ли базис, представленный матрицей *C*, задаваемому маской *H* расположению частотных составляющих?

1. Вычислить $s \leftarrow \frac{1}{N}\sum_{i=1}^{N} f_i$.

2. Для i от 1 до N выполнить:

2.1. Вычислить $g_i \leftarrow \frac{1}{N}\sum_{j=1}^{N} f_j \cdot c_{ji}$.

3. Пока $k>0$ и $s>0$ выполнять следующее:

3.1. Вычислить $k \leftarrow k-1$.

3.2. Полагаем $l \leftarrow 0$.

3.3. Для i от 1 до N выполнить:

3.3.1. Вычислить $x \leftarrow \lfloor g_i / s \rfloor$.

3.3.2. Если $x>0$, то вычислить $l \leftarrow l+1$.

3.4. Если $l=0,$ то вычислить $s \leftarrow \lfloor s/2 \rfloor$ и перейти к шагу 3. В противном случае перейти к шагу 4.

4. Если $l=r,$ то перейти к следующему шагу. В противном случае алгоритм заканчивается неудачей, так как количество низкочастотных составляющих отличается от указанного значения.

5. Для i от 1 до N выполнить:

5.1. Если $\lfloor g_i / s \rfloor \neq h_i$, то вернуть отрицательный ответ, так как было обнаружено несовпадение с заданным расположением частотных составляющих. В противном случае продолжить.

6. Расположение частотных составляющих среди элементов преобразованной последовательности данных совпадает с заданным, поэтому вернуть положительный ответ.

Дальнейшее развитие предложенного критерия выбора базисов, получаемых из состояний развития клеточного автомата, может заключаться в добавлении дополнительного условия, учитывающего порядок расположения низкочастотных составляющих в последовательности преобразованных элементов данных с точки зрения соотношений между ними.

ЛИТЕРАТУРА

1. Евсютин О.О., Росошек С.К. Использование клеточных автоматов для решения задач преобразования информации // Доклады ТУСУРа. № 1 (21), Ч. 1. 2010. С. 173–174.

2. Евсютин О.О. Декоррелирующие клеточные преобразования // Тр. 54-й науч. конф. МФТИ «Проблемы фундаментальных и прикладных естественных и технических наук в современном информационном обществе». Управление и прикладная математика. Т. 2. М.: МФТИ, 2011. С. 69–70.

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

ПАРАМЕТРИЧЕСКИЙ СИНТЕЗ РЕГУЛЯТОРА ЛИНЕЙНОЙ ИНТЕРВАЛЬНОЙ СИСТЕМЫ НА ОСНОВЕ НЕЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ

Т.А. Езангина*, *магистрант

Научный руководитель С.А. Гайворонский, доцент, к.т.н.

г. Томск, ТПУ, АиКС, eza-tanya@yandex.ru

В реальных автоматических системах параметры объекта управления, как правило, известны неточно или могут изменяться по заранее неизвестным законам в определенных пределах. Такие параметры относятся к классу интервальных. Для оценки работоспособности системы желательно определить ее наихудшее качество. Такое качество называют робастным и определяют при наихудших сочетаниях интервальных коэффициентов интервального характеристического полинома (ИХП) [1].

При синтезе систем управления объектами с ИХП наиболее целесообразным является критерий, оптимизация настроечных параметров по которому обеспечивает максимальную степень устойчивости систем управления.

Данная работа посвящена определению параметров регулятора, при которых степень устойчивости системы принимает максимальное значение при условии интервальности параметров объекта управления.

Ранее известные методы А.М. Шубладзе и Д.П. Кима основаны на использовании нормированных полиномов и применении к ним достаточных условий оптимальности по степени устойчивости. В данной работе для решения поставленной задачи предлагается применить метод нелинейного программирования.

Пусть характеристический полином имеет вид

$$F(s)=\sum_{i=1}^{n} a_i s^n, \qquad (1)$$

где $s=\eta+iw, \underline{a_i} \le a_i \le \overline{a_i}$.

Данный полином получен из следующей передаточной функции

$$W(p)=\frac{A(s)}{B(s)}, \text{ где } A(s)=\sum_{j=1}^{m} b_j s^m,\ B(s)=\sum_{i=1}^{n} a_i s^n,\ \underline{a_i} \le a_i \le \overline{a_i}, \qquad (2)$$

где $s=\eta+jw$, a, b – вектор коэффициентов системы, $A(\cdot)$ и $B(\cdot)$ некоторые функции от a, b и s.

Утверждение. Для того чтобы замкнутая система обладала максимальной степенью устойчивости, необходимо выполнение следующих условий:

$$\{R(a,\eta,w)=0; I(a,\eta,w)=0; \tag{3}$$

$$\begin{cases}\dfrac{\partial R(a,\eta,w)}{\partial\eta}=0; \dfrac{\partial I(a,\eta,w)}{\partial\eta}=0; \end{cases} \tag{4}$$

$$\begin{cases}\dfrac{\partial^n R(a,\eta,w)}{\partial\eta}=0; \dfrac{\partial^n I(a,\eta,w)}{\partial\eta}=0; \end{cases} \tag{5}$$

Здесь комплексная функция (1) раздела на вещественную $R(a,\eta,w)$ и мнимую $I(a,\eta,w)$ составляющие. Дифференцирование (5) происходит до тех пор, пока не будут определены все искомые параметры a,η,w.

Пусть передаточная функция объекта имеет вид

$$W(s)=\frac{b}{s^3+a_2s^2+a_1s+a_0}, \text{ где } \underline{a_i}\le a_i\le\overline{a_i}.$$

Требуется определить параметры ПД-регулятора $W_p(s)=k_n+k_\partial s$, при которых система обладает максимальной степенью устойчивости.

Запишем характеристический полином синтезируемой системы в виде

$$F(s)=s^3\overline{a_3}+\underline{a_2}s^2+(\underline{a_1}+bk_\partial)s+k_n+\overline{a_0}, \text{ где } s=\eta+jw. \tag{6}$$

При этом выбор нижних или верхних пределов коэффициентов определяется из условия получения максимума степени устойчивости η^* [2], т.е. $\eta^*=\max\eta_i(k)$, $k=[K_n,K_\partial]$.

Подставим (6) в условия (3)–(5) и получим следующую систему:

$$\begin{cases} R(a,\eta,w)=(-\overline{a_3})\eta^3+\underline{a_2}\eta^2-\underline{a_1}\eta-K_\partial b\eta-\underline{a_2}w^2+3\eta\overline{a_3}w^2+\overline{a_0}+K_nb; \\ I(a,\eta,w)=3\eta\overline{a_3}w^2-2\underline{a_2}\eta w-\overline{a_3}w^2-\underline{a_1}w-K_\partial bw; \\ \dfrac{\partial R(a,\eta,w)}{\partial h}=(-3)\overline{a_3}\eta^2+2\underline{a_2}\eta-\underline{a_1}-K_\partial b-\underline{a_2}w^2+3\eta\overline{a_3}w^2; \\ I(a,\eta,w)=6\eta\overline{a_3}w-2\underline{a_2}w. \end{cases}$$

Решив данную систему уравнений, получим параметры настроек регулятора

$$K_\partial=\frac{-(3\overline{a_3}\eta^2-2\underline{a_2}\eta+\underline{a_1})}{b}, \quad K_n=\frac{-(2\overline{a_3}\eta^3-\underline{a_2}\eta+\overline{a_0})}{b}$$

и максимальную степень устойчивости $\eta=\frac{1}{6}\overline{a_3}(2\underline{a_2}^2+2\sqrt{\underline{a_2}^2-3\overline{a_3}\,\underline{a_1}})$.

В работе получены необходимые и достаточные условия робастного качества (максимальной степени устойчивости) системы автоматического управления, определяемые по коэффициентам ее интервального характеристического полинома. На основе этих условий получены выражения для параметров регулятора и значения максимальной степени устойчивости.

Данный подход к параметрическому синтезу регулятора позволяет обеспечить в системе высокие динамические характеристики САУ во всем диапазоне изменения параметров объекта управления, доказывая тем самым эффективность применения данного метода.

ЛИТЕРАТУРА

1. Гусев Ю.М., Ефанов В.Н., Крымский В.Г., Рутковский В.Ю. Анализ и синтез линейных интервальных динамических систем (состояние проблемы). Анализ с использованием интервальных характеристических полиномов // Изв. АН СССР. Техн. кибернетика. 1991. № 1.

2. Петров Б.Н., Сокоов Н.И., Липатов А.В. Системы автоматического управления объектами с переменными параметрами: Инженерные методы анализа и синтеза: М.: Машиностраение, 1986.

МЕТОДИКА ПОСТРОЕНИЯ МОДЕЛЕЙ СЕТЕВЫХ УСТРОЙСТВ

С.Ю. Исхаков*, *аспирант каф. КИБЭВС

Научный руководитель А.А. Шелупанов, *проректор по научной работе*, *проф.*, *д.т.н.*

г. Томск, *ТУСУР*, *каф. КИБЭВС*, *iskhakovsy@oez.tomsk.ru*

Локальная вычислительная сеть (ЛВС) физически состоит из совокупности устройств. Одним из способов моделирования является описание параметров устройств и их значений в текущий момент времени. Далеко не всегда для построения модели объекта необходимы все параметры. В большинстве случаев для построения адекватной в текущем исследовании модели объекта достаточно описать только некоторые из них.

Для построения моделей сетевых устройств необходим методико-алгоритмический аппарат, описывающий процедуру сбора построения моделей устройств на основе необходимых в текущем исследовании параметров. В ходе проводимого исследования [1] разработана методика сбора построения частных моделей сетевых устройств.

Цель методики – предоставить сетевым администраторам алгоритмический аппарат определения текущей конфигурации сети. Методика должна обеспечивать процедуру (рис. 1) [2], которая поддержива-

ет сбор данных всех свойств объектов (информационное обследование), выбор необходимых и достаточных наборов свойств для каждого объекта, построение множества частных моделей объектов, синтез модели, отражающей текущую конфигурацию и состояние сети.

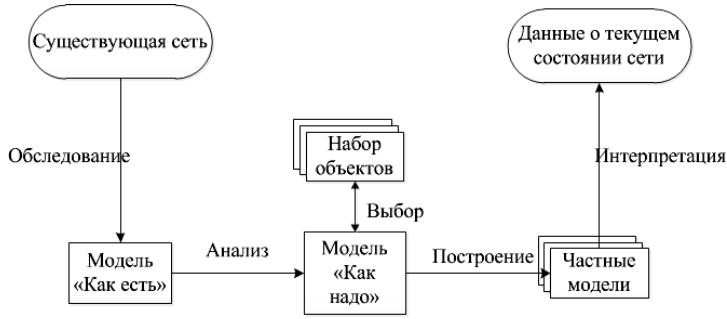


Рис. 1. Сфера действия методики

В общем случае сети принято классифицировать в зависимости от их масштаба как ЛВС, сети городского масштаба и глобальные сети. Сеть любого класса может быть смоделирована с любым уровнем детализации. В самом общем виде сеть – это одиночный узел. Далее каждый узел может быть разбит на составляющие (подсети; сетевые устройства; сервисы, запущенные на сетевых устройствах). Детализация заканчивается на том этапе, на котором дальнейшая детализация не является полезной:

1) Определить необходимый и достаточный уровень детализации модели сети.
2) Выбрать протокол.
3) Настроить СЭ для использования выбранного протокола.
4) Настроить взаимосвязь менеджера и СЭ.
5) Настроить взаимосвязь менеджера и хранилища.
6) Получить общие модели СЭ.
7) Выбрать наборы необходимых атрибутов и получить частные модели СЭ.
8) Интерпретировать полученные данные о текущем состоянии сети.

Основными элементами (концептами) методики являются: сетевой элемент (СЭ), менеджер [3–4], хранилище, протокол, общая модель, частная модель.

Сетевой элемент. В понимании методики это набор программно-аппаратных средств, которые являются частью сети, неделимой при данном уровне детализации. Все типы узлов имеют общие свойства (например, имя), но для каждого типа характерны специфические ат-

рибуты. Для каждого экземпляра конкретного типа могут иметь место специфические параметры.

Менеджер. В понимании методики это программное обеспечение, которое собирает информацию о текущем состоянии СЭ и помещает ее в хранилище.

Хранилище. Это экземпляр базы данных (БД), работающей под управлением определенной системы управления базами данных (СУБД), в котором содержится информация о текущем состоянии СЭ.

Протокол. Концепт соответствует протоколу прикладного уровня модели OSI [2–4], используемого для передачи информации от СЭ к менеджеру.

Общая модель. Это описание всех свойств объекта, которые мы можем получить с помощью используемого протокола.

Частная модель. Это набор свойств объекта, определенный администратором (человеком, использующим методику) и являющийся необходимым и достаточным для представления о текущем состоянии объекта при данном уровне детализации.

Таким образом, данная методика разработана для использования совместно со средствами моделирования сетей для помощи проведения этапа информационного обследования.

Методика способна отражать структуру сети на различных уровнях декомпозиции. Также имеется возможность анализа отдельных сегментов.

Для облегчения создания частных моделей поддерживается фиксация текущего набора свойств объекта и возможность изменения этого набора.

ЛИТЕРАТУРА

1. Исхаков С.Ю. Получение данных с устройств сети, их обработка и представление / С.Ю. Исхаков, Н.С. Козыренко, А.О. Шумская // Матер. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2011», Томск, 4–6 мая 2011 г. Томск: В-Спектр, 2011. Ч. 3. С. 37–39.

2. Гладцын В.А., Яновский В.В. Средства моделирования вычислительных сетей: учеб. пособие. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2001. 128 с.

3. Моделирование и анализ надежности корпоративной сети [Электронный ресурс]. Режим доступа: http://ria-stk.ru/stq/adetail.php?ID=10236, свободный (дата обращения: 10.03.2012).

4. Архитектуры систем управления сетями. Протокол управления сетью SNMP [Электронный ресурс]. Режим доступа: http://kunegin.narod.ru/ref3/snmp/file0.htm, свободный (дата обращения: 25.02.2012).

МОДЕЛИРОВАНИЕ ОБЪЕКТОВ В СИСТЕМЕ МОНИТОРИНГА ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

С.Ю. Исхаков*, *аспирант*; *А.Ю. Исхаков*, *Н.С. Козыренко*, *А.О. Шумская*, *студенты 4-го курса

г. Томск, *ТУСУР*, *каф. КИБЭВС*, *iay@security.tomsk.ru*

Развитие локально-вычислительных сетей (ЛВС) большинства организаций зачастую проходит по экстенсивному пути. При таком подходе возникают не только проблемы с обслуживанием отдельных станций, но и проблемы управления всей сетью в целом. Именно наличие системы контроля и управления позволяет поддерживать сеть в работоспособном состоянии, прогнозировать проблемы и своевременно вносить изменения в структуру сети.

В рамках проекта ГПО № КИБЭВС-1002 разрабатывается система мониторинга, предназначенная для контроля функционирования локально-вычислительных сетей. Продукт реализуется на базе веб-интерфейса. Это позволяет достичь распределенности системы: администратор может получить доступ к данным о состояниях сетевых устройств с любой рабочей станции. Так как в большинстве локальных сетей состав аппаратного и программного обеспечения носит гетерогенный характер, то для сбора данных необходим протокол, поддерживаемый всеми типами оборудования. В разрабатываемой системе используется Simple Network Management Protocol (SNMP) [1].

ЛВС физически состоит из совокупности объектов (устройств). Каждое устройство может быть описано с помощью некоторой модели, согласно которой его можно представить в виде описания параметров и их значений в текущий момент времени.

В качестве параметров могут выступать как технические, так и программные характеристики устройства (модель процессора, объем памяти, количество сетевых интерфейсов и их текущая загрузка). Количество параметров современных устройств, работающих в сети, исчисляется десятками и даже сотнями. В большинстве случаев для построения адекватной в текущем исследовании модели объекта достаточно описать только некоторые из них.

В целях автоматизации процесса сбора данных была разработана процедура типизации объектов, которая состоит в выделении типов устройств с определенными для них наборами параметров.

Оператору системы предоставляется возможность выбора необходимых и достаточных для каждого объекта наборов свойств: пользователь может сам выбирать, какие именно интерфейсы, жесткие диски, элементы оперативной памяти должны опрашиваться.

Тем самым обеспечивается построение множества частных моделей объектов. Также предусмотрена возможность фиксации текущего набора свойств объекта и возможность изменения этого набора.

Блок-схема алгоритма данной процедуры представлена на рис. 1.

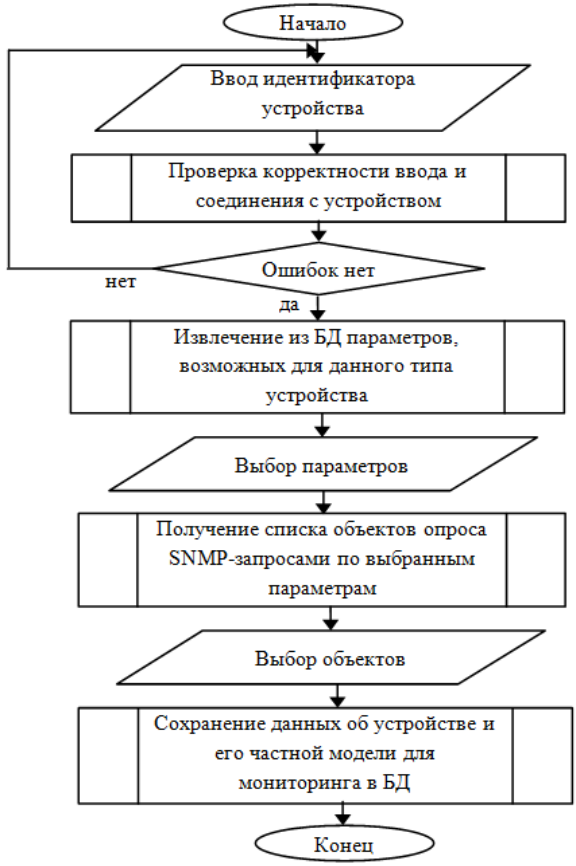


Рис. 1. Алгоритм определения модели устройства в системе мониторинга

Таким образом, приложение осуществляет сбор данных о текущем состоянии сетевых устройств, руководствуясь частными моделями объектов, которые хранятся в базе данных.

В структуре предлагаемой системы можно выделить 5 взаимосвязанных модулей: центр управления, модуль авторизации, блок сбора данных, блок статистической обработки данных, модуль оповещения.

Наиболее важным свойством любой системы мониторинга является возможность оповещения операторов о сбоях и отклонениях в работе. В большинстве случаев такие оповещения формируются исходя из заданных критериев и текущих показателей свойств объектов.

При большом количестве устройств, а также при большом количестве параметров зачастую трудно сформировать критерии анализа состояний объектов. Трудности также могут быть обусловлены периодичностью изменения свойств (например, повышение трафика в рабочие часы). Все это может стать причиной ложных оповещений о сбоях в системе.

В утилите RRDTool [2], используемой для хранения значений, полученных с устройств, и обработки статистических данных, реализован метод прогнозирования Хольта–Винтерса [3]. Поведение устройства сравнивается со сгенерированным для него краткосрочным прогнозом, и если отклонения превышают допустимую норму, формируется предположение о наступлении аномалии в работе сети.

Следующие этапы разработки включают использование данного метода для расширения функционала системы в виде краткосрочного прогнозирования сбоев системы и оповещения операторов.

Проект ГПО КИБЭВС-1002 – «Построение автоматизированной системы администрирования локально-вычислительных сетей».

ЛИТЕРАТУРА

1. Описание протокола SNMP (Simple Network Management Protocol) [Электронный ресурс] // Delphi Sources. Электрон. текст. дан. [Б. м.], 2002–2004. URL: http://www.delphisources.ru/pages/faq/ base/snmp_protocol_description.html (дата обращения: 20.02.2012).

2. Bogaerdt A. van den. RRDtool tutorial [Electronic resource] // About RRDtool. Electron. text data. [S.l.], 2011. URL: http://www.mrtg.org/rrdtool/tut/rrdtutorial.en.html (access date: 15.02.2012).

3. Brutlag J.D. Aberrant Behavior Detection in Time Series for Network Monitoring [Electronic resource] // Usenix: The Advanced Computing Systems Association. Electron. text data. [S.l.], 2012. URL: http://www.usenix.org/events/lisa00/full_papers/brutlag/brutlag_html (access date: 10.02.2012).

МОДЕЛЬ ВОДОЗАБОРА ПОДЗЕМНЫХ ВОД ДЛЯ ЭНЕРГОЭФФЕКТИВНОГО УПРАВЛЕНИЯ НАСОСНЫМИ СТАНЦИЯМИ

Е.О. Иванов*, *аспирант каф. АОИ

Научный руководитель Н.В. Замятин, проф. каф. АОИ, д.т.н.

г. Томск, *ТУСУР*, *egor.o.ivanov@ya.ru*

При использовании подземных вод 80% общей стоимости эксплуатационных расходов на водопроводных предприятиях составляют расходы электроэнергии на перекачку вод центробежными насосами. Несмотря на столь высокую стоимость расходов, проблеме энергоэф-

фективной работы насосных установок не уделяется должного внимания, в результате чего 25–50% энергии расходуется нерационально [1].

Артезианские скважины, объединенные между собой сборными водоводами, представляют единую гидравлическую систему, в которой прослеживается связь между изменением производительности скважин, изменением гидравлических параметров отдельных сооружений (понижение уровня воды), потерями напоров в водоводах, изменением уровня воды в резервуаре (изменение водопотребления). Кроме того, каждый насосный агрегат имеет свою фактическую расходно-напорную характеристику [2]. Поэтому система «скважины–насосы–трубопроводы–резервуар» должна рассматриваться как единая сложная система.

Совместная работа насосов и сети характеризуется точкой материального и энергетического равновесия системы. Совместная работа насосов, скважин, трубопроводов и резервуара связана следующими зависимостями [3]:

$$H = f(Q_p),\ H_r = G(Q_p, q),\ h = j(Q),$$

где Q – расчётный расход в трубопроводе; Q_p – подача воды насосом; q – расход воды в системе; H – напор, развиваемый насосом, H_r – уровень воды в резервуаре; h – гидравлическое сопротивление водоводов и сети.

Аналитический расчёт режимной точки работы насоса довольно трудоёмкий процесс, так как приходится оперировать четырьмя переменными величинами Q_p, H, q и h, которые находятся между собой в функциональной зависимости. При расчёте системы используют метод последовательного приближения или производят расчёт на ЭВМ. Однако эти вычисления не дают наглядности, и анализ работы насоса весьма затруднителен [3]. Поэтому для повышения наглядности полученных результатов предполагается построить модель системы «скважины–насосы–трубопроводы–резервуар» в среде моделирования, имитации и анализа динамических систем SIMULINK.

На рис. 1 представлена модель совместной работы одиночной скважины, резервуара, трубопровода, насоса. Эта модель учитывает понижение уровня воды в скважине, потери напора в трубопроводе и геометрическую высоту подъёма воды, то есть требуемый напор.

Также для насоса производится расчёт развиваемого напора при заданной подаче и частоте вращения электродвигателя, потребляемой мощности и его КПД.

Представленная динамическая модель была расширена для случая множества скважин с учётом их взаимного влияния друг на друга и совместной работы на один резервуар (на примере водоканала г. Стрежевого).

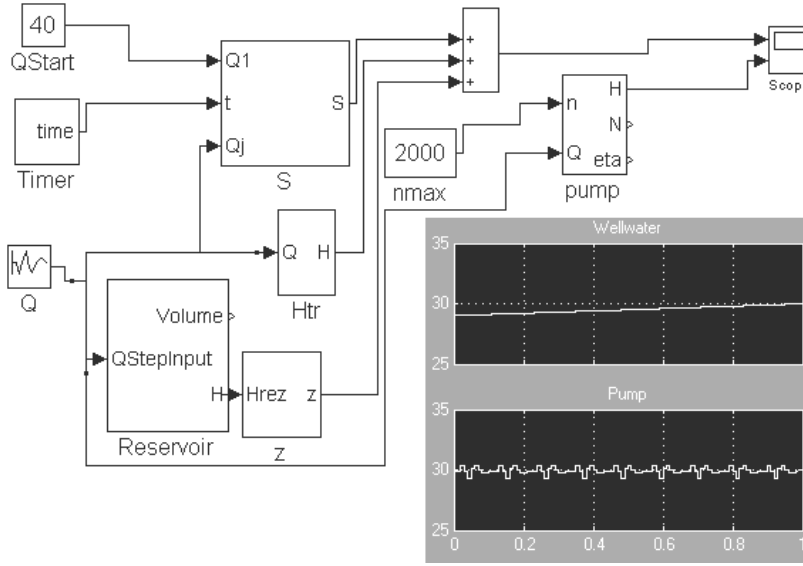


Рис. 1. Модель совместной работы скважины, насоса, сети

На рис. 2 представлены графики расходно-напорных характеристик насоса и системы «скважина–трубопроводы–резервуар» и понижения уровня воды в скважине при динамическом изменении её дебита. Точка пересечения графиков является наиболее энергоэффективным режимом работы (минимальные потери напора).

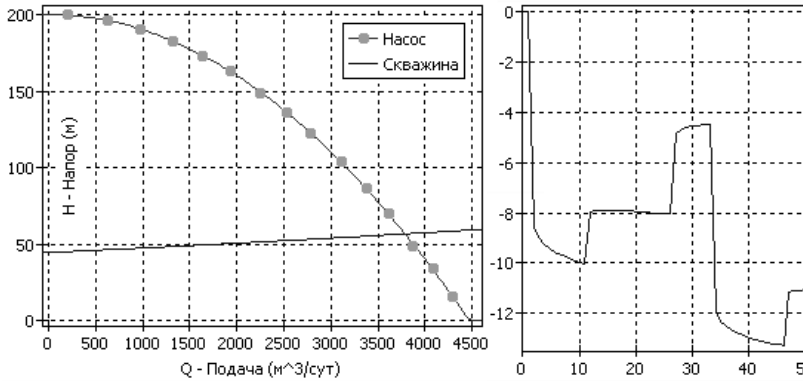


Рис. 2. Совместная работа скважины и насоса (слева) и понижение уровня в скважине (справа)

Представленная модель позволяет выразить следующий критерий оптимальности управления водозабором подземных вод. С одной стороны, это поддержание уровня воды в сборном резервуаре на определенной отметке (с учетом прогноза водопотребления), а с другой – это минимизация энергетических расходов на добычу и перекачку воды путем оптимального регулирования частот вращения рабочих колес насосов (или включение/отключение определенных насосов) при сохранении материального и энергетического баланса системы. Для оптимального управления в реальном времени предполагается использовать нейросетевое ситуационное управление.

ЛИТЕРАТУРА

1. Лезнов Б.С. Энергосбережение и регулируемый привод в насосных и воздуходувных установках. М.: Энергоатомиздат, 2006. 360 с.

2. Пособие по проектированию сооружений для забора подземных вод (К СНИП 2.04.02-84) / ВНИИ ВОДГЕО Госстроя СССР. М.: Стройиздат, 1989. 272 с.

3. Карелин В.Я., Минаев А.В. Насосы и насосные станции: учеб. для вузов. 2-е изд. М.: Стройиздат, 1986. 320 с.

ПРЕИМУЩЕСТВА ОСНАЩЕНИЯ АВТОРЕМОНТНЫХ ПРЕДПРИЯТИЙ СПЕЦИАЛИЗИРОВАННЫМ РАЗБОРОЧНО-СБОРОЧНЫМ ОБОРУДОВАНИЕМ

А.А. Копытин, М.С. Козлов, студенты

Научный руководитель Т.Ю. Лебединская, доцент, к.т.н.

г. Краснодар, ГОУ ВПО «Кубанский государственный технологический университет»

В наше время автомобильные перевозки выходят на первое место по значимости, доступности и использованию в народном хозяйстве. Количество автомобилей на дорогах постоянно растёт, а вместе с этим растет и значимость оперативности их ремонта, ведь даже один день простоя транспортного средства без особой необходимости приносит его владельцу убытки. Так как особо важна скорость обслуживания подвижного состава, предприятия автомобильного транспорта должны быть оснащены современным оборудованием, обеспечивающим оперативный и качественный ремонт. В наши дни существует множество фирм, выпускающих авторемонтное оборудование для автотранспортных предприятий любого размера, начиная с узкоспециализированных частных станций технического обслуживания и заканчивая большими авторемонтными предприятиями, обслуживающими огромное количество автомобилей.

Среди предлагаемого на рынке оборудования имеется довольно большое количество стендов для сборки и разборки двигателей, коробок передач и редукторов, а также универсальных стендов и стендов-кантователей. Стенд для ремонта двигателей предназначен для подвешивания мотора с целью работ по диагностике, ремонту и транспортировке по помещению. Специальный механизм вращения позволяет изменять углы положения подвешенного мотора в диапазоне от 0° до 360° для наиболее удобного доступа. Существуют узкоспециализированные стенды для ремонта определенных моделей двигателей, такие как стенд российского производства М-409 для разборки и сборки двигателя Д-160, но наряду с ними производится большое количество стендов для сборки-разборки и стендов кантователей, которые позволяют закреплять практически все типы двигателей, а также коробок передачи редукторов, а именно модели Р-776Е и Р-770Е российского производства, итальянские модели R12 и R11, немецкие стенды WW-HV-1500, или китайские модели кантователей Т63002, Т63003, Т63004, Т63005. Последние примечательны подозрительно малой ценой и высокой заявленной грузоподъёмностью. Качественно сделанный стенд будет обеспечивать высокую точность измерений и требуемую скорость работы механика в агрегатном цехе, а следовательно, оперативный ремонт и минимальное время нахождения транспортного средства в ремонте, что сократит убытки владельца автомобиля, связанные с понижением коэффициента технической готовности подвижного состава из-за поломки двигателя автомобиля.

В условиях современной жизни особо важна и скорость обслуживания автомобиля, а чтобы повысить скорость работы автомеханика, специализированное оборудование, которым он пользуется, должно отличаться и такими параметрами, как оперативность установки и закрепления агрегата, удобство, эргономичность. Благодаря конструктивной продуманности мелких деталей сборочно-разборочного оборудования для двигателей, таких как поддон для смазочно-охлаждающих жидкостей, маленькая полка для инструмента или особый вид специализированных креплений, можно сэкономить драгоценное время, которое автомобиль находится в ремонте, а значит, и увеличить коэффициент технической готовности автопарка клиента, что обеспечит высокую конкурентоспособность авторемонтному предприятию, где используется это оборудование. Если же взять такие серьезные улучшения разборочно-сборочных стендов, как червячный редуктор для поворота агрегата на 360°, который обеспечивает фиксацию в любом положении благодаря самотормозящемуся червяку в червячной паре, или электродвигатель, который устанавливается на стенде вместе с редуктором и облегчает работу автомеханика посредством уменьше-

ния усилия при вращении агрегата, то авторемонтное предприятие, использующее данное высокотехнологичное оборудование, будет однозначно выигрывать в скорости обслуживания автомобилей по сравнению с менее технологично оборудованными конкурентами.

Проанализируем предложение сборочно-разборочного оборудования для агрегатов на современном рынке. Прежде всего, стоит выделить стенд для разборки и сборки двигателей внутреннего сгорания немецкой фирмы Werner-Weitner. Несмотря на весьма завышенную цену (почти в три раза по сравнению с достойными российскими аналогами), стенды этой фирмы отличаются особой надёжностью и качеством исполнения узлов конструкции, а также продуманностью буквально до мелочей. Также существуют весьма добротно сделанные стенды отечественного производства, такие как Р776Е с ручным приводом и Р770Е с электромеханическим приводом поворота двигателя, что является особым преимуществом данного стенда над другими этой ценовой категории. Стенды итальянской фирмы Ravaglioli R11 и R15 примечательны установленными на них подвижными опорами для транспортировки стенда, а также высоким качеством при большей грузоподъёмности, чем у конкурентов.

Наряду с элитным оборудованием для больших авторемонтных предприятий стоит выделить оборудование чуть ниже классом, но позволяющее, в принципе, проводить все те же работы, что проводятся и на дорогостоящем оборудовании, но, правда, с гораздо большей трудоёмкостью. Следует выделить такого производителя стендов, как AE&T. Это китайский производитель, предлагает модели стендов T63002, T63003, T63004, T63005. Эти стенды не отличаются особым качеством, но их основное достоинство – крайне низкая цена. Грузоподъёмность их ограничена до 300–500 кг, а некоторых моделей – до 900кг. Вес таких стендов на порядок ниже, чем у конкурентов, а так как стенды установлены на подвижных опорах, их легко перемещать по производственному помещению. Стенды этой же ценовой категории выпускает и отечественный производитель. Это, например, стенд модели Т26801. Его главным преимуществом является цена, а также мобильность, вследствие установки на подвижных опорах и малой массы, которая не превышает 34 кг. К недостаткам такого разборочно-сборочного оборудования для двигателей стоит отнести отсутствие редуктора для поворота закрепленного агрегата. Это повлияет на удобство и скорость работы автомеханика, что негативно скажется на производительности всего авторемонтного предприятия в целом.

Механизация технологических процессов ремонта автомобильного подвижного состава имеет важное технико-экономическое и социальное значение, которое выражается в уменьшении численности ре-

монтных рабочих за счет снижения трудоемкости работ по ремонту автомобилей, улучшении условий труда рабочих авторемонтных предприятий, повышении качества выполнения работ. Снижение трудоемкости работ по техническому обслуживанию и ремонту достигается за счет сокращения времени выполнения соответствующих операций в результате внедрения средств механизации. Таким образом, очевидны преимущества оснащения авторемонтных предприятий современным специализированным разборочно-сборочным оборудованием.

ЛИТЕРАТУРА

1. Сарбаев В.И., Селиванов С.С., Коноплев В.Н., Демин Ю.Н. Техническое обслуживание и ремонт автомобилей: механизация и экологическая безопасность производственных процессов. Сер. Учебники, учебные пособия / Ростов н/Д: Феникс, 2004. 448 с.

2. http://www.avk76.ru/catalog/detail.php?ID=2054&sphrase_id=3824

3. http://www.technosouz.ru/Pages/sborochno_razborochnoe.html

4. http://diasat.ru/shop/UID_159.html

5. http://www.ta-yug.ru/garajnoe_oborudovanie/stendyi_dlya_dvigatelya/

6. http://www.ttsauto.ru/katalog-oborudovaniya/gruzovoj-avtoservis/specializirovannoe-oborudovanie/82/

ПРОБЛЕМЫ ШИНОМОНТАЖНЫХ ПРЕДПРИЯТИЙ ЛЕГКОВОГО АВТОТРАНСПОРТА КРАСНОДАРСКОГО КРАЯ

М.С. Козлов, А.А. Копытин, студенты

Научный руководитель Т.Ю. Лебединская, доцент, к.т.н.

г. Краснодар, ГОУ ВПО «Кубанский государственный технологический университет»

Шиномонтажный бизнес немного специфичный, в основном, из-за сезонного потребления – это осенний и весенний сезон, смена резины с летней на зимнюю и обратно. Так же из-за специфики климата – затяжная осень, резкие перепады температуры, продолжительные оттепели, неожиданные похолодания в начале весны – все эти факторы влияют на количество «переобуваний», некоторые клиенты с осени по весну производят замену резины по четыре и более раз. В летнее время, в связи с курортным сезоном, увеличивается численность автомобилей.

Множество станций технического обслуживания (СТО), в том числе и очень мелкие, имеют среди своего оборудования шиномонтажные, балансировочные станки и сопутствующие шиномонтажу дополнительные принадлежности. Все это используется на полную мощность в осенний и весенний периоды, когда большой поток клиентов

перед резкими заморозками «переобуваются» на зимнюю или с потеплением на летнюю резину.

Существует несколько категорий предприятий, которые занимаются шиномонтажом, – это крупные СТО со всем необходимым оборудованием; мелкие СТО; индивидуальные предприниматели и гаражи, которые держат у себя шиномонтажное оборудование, и открываются к сезону, чтобы подзаработать.

Индивидуальные предприниматели и некоторые мелкие СТО покупают бывшее в эксплуатации оборудование, так как оно гораздо дешевле, и работают, чтобы охватить как можно больше разнообразных услуг и получить увеличение дохода предприятия в период сезона. Но услуги, оказываемые на такого рода станках, из-за люфтов и выработок практически на всех трущихся и движущихся участках станка оставляют желать лучшего. Особенно если это большой радиус колеса или низкопрофильная резина. Конечно, для оснащения СТО лучше выбирать новое оборудование.

На рынке шиномонтажного оборудования представлены следующие станки: Кс-302А (Россия) до 24 дюймов, 48000 руб.; 1850 до18 дюймов (Россия), 38540 руб.; Nordberg NB 4639 (Китай), до 24 дюймов 56570 руб.; Corghi Jollu (Италия) до 21 дюйма, 90580 руб; TECO 22 (Италия) до 21 дюйма, 85000 руб.; M&B TC322 (Италия) до 23 дюймов, 68500 руб; Hofmann Monty 2300 (Германия) до 26 дюймов, 13000 руб., а также многие другие модели.

На большинстве шиномонтажных предприятий на станках не имеется такой опции, как «третья рука». «Третья рука» представляет собой дополнительную стойку с несколькими вспомогательными лапами, устанавливается на шиномонтажный станок, помогает при работе с жесткими и низкопрофильными шинами, а также с дисками больших радиусов. Она используется в тех случаях, когда возникают трудности при выполнении работ по замене шины одним сотрудником. Конечно, стоимость «третьей руки» составляет примерно 70% от стоимости самого станка, и многие предприятия экономят или используют еще одного сотрудника с дополнительной монтировкой.

На рынке представлены следующие фирмы, у которых существуют станки, на которые можно отдельно приобрести опцию «третья рука»: Corghi PU1500 (Италия), 63380 руб.; NORDBERG 46H (Китай), 31715 руб. Также существуют станки уже с встроенной опцией, это, например, Hofmann Monty 3550 (Германия), 256000 руб.

Сравнив ценовую политику, можно сделать вывод, что мелкие, развивающиеся шиномонтажные СТО могут сначала, например, приобрести станок Nordberg NB 4639, а в процессе работы – опцию для

него «третья рука» NORDBERG 46H. Это будет менее затратно чем сразу приобрести стенд шиномонтажный, оснащенный «третьей рукой».

В летний период также возрастает нагрузка на шиномонтажные предприятия, так как многие клиенты приезжают со всей страны отдыхать на курортах нашего края. Нагрузка на СТО заключается уже не в «переобувке», а в шиноремонтной, дископрокатной сфере и в подкачке колес. Учитывая дорожное покрытие и нахождение разных мелких предметов на дороге, из-за которых случаются проколы, порезы шин, необходимо шиноремонтное и дископрокатное оборудование, которым нужно оснащать СТО, стоящие на федеральных трассах.

На рынке предоставлено следующее дископрокатное оборудование: Титан ST17 (Россия) от 4 до 6,5 дюйма и диаметром 13–17 дюймов, 78200 руб.; K-Max Doruk (Турция) диаметр от 10 до 22 дюймов 180000 руб.; АТЕК MAKINA KONIG 1400 (Турция) от 10 до 16 дюймов, 39000 руб. и др.

К шиноремонтному оборудованию относятся вулканизаторы, они нужны для свариваемости резины и камер, при боковых порезах и ремонте шишек. На рынке существует следующее оборудование: Nordberg V1 (Китай) вулканизации шин легковых и грузовых автомобилей, автобусов и тракторов, 12860 руб.; ГАРО В 101 (Россия) ремонт покрышек легковых и грузовых автомобилей посадочным диаметром 13–20 дюймов, шириной профиля 5,9–9 дюймов: сквозные повреждения до 10 мм, несквозные – до 100 мм, 24700 руб.; Сибек Этна (Россия) вулканизатор универсальный для ремонта камер и покрышек легковых а/м, легких грузовых а/м и микроавтобусов до 17», включая боковые повреждения, 37300 руб.; а также множество других вариантов.

Вышеперечисленное оборудование необходимо для оснащения шиноремонтных предприятий вблизи федеральных трас для удовлетворения потребностей населения в шиномонтажной сфере. Можно сделать выводы, что шиномонтажным предприятиям, если они хотят быть весьма конкурентоспособными в наши дни, не стоит опасаться расходов, связанных с обновлением и модернизацией их оборудования «по последнему слову техники». От качества и скорости обслуживания напрямую зависит спрос на их услуги, а значит, и доход предприятия, что позволит быстро окупить модернизацию оборудования и оставаться конкурентоспособными на рынке своих услуг долгое время.

ЛИТЕРАТУРА

1. АвтоПромСнаб оборудование для СТО [Электронный ресурс]: Каталог. URL: http://www.apsnab.ru/catalog (дата обращения: 04.03.2012).

СИСТЕМА ТЕСТИРОВАНИЯ ЗНАНИЙ СТУДЕНТОВ

К.А. Козловский, В.Б. Егоров,
А.Н. Сусиков, студенты 4-го курса каф. КИБЭВС
Научный руководитель Е.М. Давыдова, доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, ФВС

Разрабатываемая система предназначена для проведения тестирования знаний студентов и анализа результатов тестирования.

Цель работы: повышение качества обучения студентов.

Задача: Разработать полноценную систему тестирования знаний студентов, основанную на ФГОС 3-го поколения, с возможностью присвоения предметам компетенций и учёта их при оценивании. Для преподавателей будет создан специальный интерфейс, позволяющий создавать и редактировать свои тесты, для студентов – эти тесты проходить. Система будет работать на поддомене кафедрального сайта, планируется использовать общую систему авторизации с главным сайтом, для этого необходимо синхронизировать таблицы пользователей БД кафедры и БД системы тестирования.

Анализ рейтинговой системы. В связи с наличием недостатков в оценке рейтинга студента как среднего арифметического его оценок, целесообразно применить систему оценивания, предложенную А.А. Шантаевым в своей дипломной работе (автоматизированная система расчёта рейтинга студентов). Дисциплины разбиваются на квалификационные группы и каждой группе присваивается коэффициент сложности. Затем по уравнению, предложенному В.С. Аванесовым в его работе «Теория и методика педагогических измерений», будет определяться рейтинг студента:

$$Y_i = a + b_1 \times x_{i1}, + b_2 \times x_{i2} + \ldots + b_k,$$

где Y_i – совокупный балл; x_{i1}, x_{i2} – оценки по дисциплинам; a – свободный член уравнения (равен 0); b_1, b_2, … b_k – коэффициенты значимости дисциплины.

По завершении работы над нашим проектом мы получим онлайн-систему для тестирования знаний студентов, включающую в себя полный набор функций для тестирования: создание тестов, прохождение тестов, анализ результатов и построение рейтинга на их основе.

Проект ГПО КИБЭВС-1006 – «Система тестирования знаний студентов».

СИТУАЦИОННЫЙ ЦЕНТР УПРАВЛЕНИЯ ЭНЕРГОЭФФЕКТИВНОСТЬЮ

В.В. Латровкин*, *аспирант каф. АОИ
Научный руководитель Н.В. Замятин, *проф. каф. АОИ*, *д.т.н.*
г. Томск, *ТУСУР*, *latrovkin@yandex.ru*

Тенденции развития отечественной экономики и опыт зарубежных стран показывают, что в современных условиях, при росте стоимости энергоресурсов, отрицательного воздействия энергетических технологий на окружающую среду, проблема энергоэффективности приобретает критически важное значение.

Решением данной проблемы является формирование ситуационного центра управления энергоэффективностью (СИТЦУЭ).

СИТЦУЭ – это информационно-аналитический комплекс управления энергосбережением и энергетической эффективностью [1].

СИТЦУЭ позволяет:

- получить экономию потребления энергоресурсов от 30 до 40%;
- предоставлять качественные услуги по тепло- и электроснабжению;
- снизить социальную напряженность в условиях реформирования ЖКХ за счет предоставления населению возможности платить за фактически потребленные ресурсы и регулировать количество получаемого тепла;
- более эффективно использовать имеющиеся ресурсы за счет реального энергосбережения.

Целью создания ситуационного центра управления энергоэффективностью является автоматический мониторинг и интеллектуальный анализ в реальном времени объёмов и режимов распределения и потребления топливно-энергетических ресурсов (ТЭР) региона [1].

СИТЦУЭ предназначен для предприятий, организаций, органов власти и других участников рынка ТЭР, заинтересованных в модернизации существующих технологий энергосбережения, их систематизации и оптимизации с целью создания условий, обеспечивающих повышение качества энергоснабжения населения [1].

СИТЦУЭ имеет трехуровневую структуру. Основные функции верхнего уровня:

- автоматизированный сбор информации по управлениям и отраслям;
- хранение интегрированной информации о потреблении и поставках ТЭР;
- анализ информации;
- генерация отчетов.

Второй уровень состоит из независимых автономных автоматизированных систем управления отраслей, которые агрегируются с СИТЦУЭ, а также автоматизированные системы управлений (АСУ) департаментов и управлений, построенных в иерархической последовательности, несущих на себе задачи обобщения информации о непосредственных потребителях ТЭР.

Третий уровень предоставляет данные о потреблении ТЭР, которые должны поступать с автоматизированных средств сбора информации или, при невозможности, из соответствующих служб и управляющих компаний.

СИТЦУЭ предоставляет следующие возможности:

1) комплексный учет и мониторинг всех потребляемых энергоресурсов;

2) диспетчеризация данных по учету индивидуального энергопотребления и контролю работы инженерных систем дома;

3) диагностика неисправностей элементов системы и несанкционированного доступа.

СИТЦУЭ позволяет успешно решить задачи экономии всех видов энергоресурсов:

- электрической энергии в натуральном и стоимостном выражении;
- тепловой энергии в натуральном и стоимостном выражении;
- воды в натуральном и стоимостном выражении;
- природного газа в натуральном и стоимостном выражении.

Кроме этого, СИТЦУЭ позволяет решить следующие оперативные задачи:

- выявление сверхнормативных потерь энергоресурсов и предотвращение аварийных ситуаций;
- отслеживание соблюдения параметров качества и режима поставки энергоресурсов;
- контроль состояния объектов диспетчеризации;
- самодиагностика компонентов системы и линий связи;
- автоматическое дистанционное снятие показаний приборов учета (ПУ) и архивирование информации в базе данных (БД);
- автоматический расчет количества потребленных энергоресурсов с учетом субабонентов и транзитов;
- автоматическая коррекция данных;
- автоматическое формирование актов передачи данных;
- формирование отчетов и обменных файлов.

Сопоставление данных, полученных на каждом уровне СИТЦУЭ, позволяет верифицировать поступающую информацию, производить анализ эффективности потребления энергии и вырабатывать эффек-

тивные решения для повышения энергоэффективности зданий – сооружений и производств.

Сочетание измерительных и интеллектуальных аналитических функций СИТЦУЭ дает возможность не только автоматизировать задачи выявления потенциала энергосбережения, но и контролировать процесс реализации этого потенциала. Взаимодействуя с другими информационными системами, СИТЦУЭ способен стать основой и связующим звеном при построении муниципальных и региональных информационно-аналитических систем (МИАС и РИАС).

ЛИТЕРАТУРА

1.Замятин Н.В., Латровкин В.В. Ситуационный центр энергоэффективности регионального уровня // Доклады ТУСУРа. 2011. №2 (24), ч. 3. С. 171–175.

КОНФЕРЕНЦ-СВЯЗЬ. КОНГРЕСС-СИСТЕМЫ, СИНХРОННЫЙ ПЕРЕВОД И СИСТЕМЫ ВИЗУАЛИЗАЦИИ

А.Е. Леонов, студент 5-го курса каф. КИБЭВС;
А.Д. Иванов, инженер ООО «Бюро «Сервис»
г. Томск, ТУСУР, ФВС, alex.leo970@gmail.com

В современных условиях территориального распределения и высокой динамичности бизнеса стандартные средства связи, такие как телефон, факс, электронная почта, не всегда способны удовлетворить постоянно возрастающие требования к обмену информацией между подразделениями компании. Личное же присутствие специалиста в определенном месте довольно часто бывает сопряжено с очень высокими материальными и, что наиболее важно, временными затратами на переезды и перелеты. Результаты исследований, проведенных Национальным советом по статистике США, показывают, что участие в четырехчасовом совещании требует примерно 16 ч подготовки, из которых большую часть занимает дорога. А успех во многом зависит от своевременного поступления информации и быстрого принятия решений [1].

Конференц-система представляет собой комплект аппаратуры, обеспечивающий голосовую связь участников коллективного обсуждения, расположенных, как правило, в одном помещении.

Конференц-системы принято классифицировать по функциональным возможностям и по способу передачи информации.

По функциональным возможностям выделяют:

– дискуссионные системы, обеспечивающие поочерёдное или совместное выступление нескольких участников обсуждения;

– конгресс-системы, рассчитанные, как правило, на большой состав участников и предоставляющие ряд дополнительных возможностей, в том числе – идентификацию участников совещания, автоматическую работу по заданному графику, голосование, синхронный перевод и др.

По способу передачи информации выделяют проводные и беспроводные конференц-системы, в том числе использующие радиосигналы и ИК-сигналы. Наиболее распространены проводные системы, обеспечивающие простую и надёжную передачу сигналов в двух направлениях.

В свою очередь, беспроводные системы обладают следующими преимуществами:

– отсутствие кабельных связей;

– быстрая и легкая инсталляция;

– свободное расположение микрофонных пультов в любом месте зала.

Реализация беспроводных конференц-систем связана со значительными техническими проблемами. Основной сложностью при построении такого рода систем является обеспечение двусторонней беспроводной связи с большим количеством абонентов. Тем не менее отдельные системы такого типа представлены на рынке [2].

В современной бизнес-среде особая роль отводится видеоконференц-связи – одному из наиболее эффективных и относительно недорогих способов качественного улучшения процесса принятия решений, своевременного информирования ключевых сотрудников компании и сокращения расходов на деловые поездки.

Видеоконференция – это технология, которая позволяет людям видеть и слышать друг друга, обмениваться данными и совместно обрабатывать их в интерактивном режиме, используя возможности привычного всем компьютера, максимально приближая общение на расстоянии к реальному живому общению.

Сегодня практически не осталось области жизнедеятельности, в которой нельзя было бы использовать видеоконференц-связь. Она находит применение везде, где необходимы оперативность в анализе ситуации и принятии решений, консультация специалиста или совместная работа в режиме удаленного доступа над проектами и решениями и т.д. [1].

Синхронный перевод – вид устного перевода, при котором речь переводится одновременно с ее изложением. Данный вид перевода наиболее сложен и является высшим пилотажем переводческой деятельности.

Встречаются три разновидности, синхронного перевода. Первой, наиболее распространенной разновидностью синхронного перевода, является синхронный перевод на слух: переводчик воспринимает речь оратора через наушники и переводит ее по мере поступления.

Второй разновидностью является синхронный перевод с листа с предварительной подготовкой или без нее: переводчик получает письменный текст речи оратора за некоторое время до выступления или непосредственно перед выступлением и выполняет перевод с опорой на письменный текст. При этом может возникнуть необходимость коррекции, если оратор отступает от первоначального текста.

Третьей разновидностью синхронного перевода, является синхронное чтение заранее переведенного текста: в ходе выступления оратора переводчик зачитывает заготовленный письменный текст перевода, вносит необходимые корректировки по необходимости.

Вне зависимости от типа синхронного перевода, он стал возможен благодаря созданию необходимой технической базы, качество которой во многом определяет удобство работы переводчиков и участников. Системы синхронного перевода могут устанавливаться как отдельно, так и в комплексе с конференц-системами.

Синхронный перевод дает значительную экономию времени, особенно на международных встречах, где используется несколько рабочих языков.

Применение синхронного перевода очень разнообразно. Он широко практикуется в области политических межгосударственных связей и в области обмена научно-технической информацией, в области культурного обмена и при контактах по военной линии. Появились и расширяются новые области применения синхронного перевода, например синхронный перевод лекций, кинофильмов, театральных представлений [3].

ЛИТЕРАТУРА

1. Видеоконференц-системы // Матер. сайта «Викинг». URL: http://www.viking.ru/info/video_conference.php (дата обращения: 11.02.2012).

2. Конференц-системы // Матер. сайта «Викинг». URL: http://www.viking.ru/info/conference_system.php (дата обращения: 15.02.2012).

3. Синхронный перевод // Матер. сайта «Викинг». URL: http://www.viking.ru/info/simultaneous_translation.php (дата обращения: 17.02.2012).

ПРОГРАММА МОДЕЛИРОВАНИЯ ПРИБОРОВ МИКРОЭЛЕКТРОНИКИ

А.Н. Медведева*, *студентка 6-го курса
Научный руководитель Л.А. Торгонский, *доцент каф. КИБЭВС*
г. Томск, *ТУСУР*, *ФВС*

Предлагаемый в статье программный модуль предназначен для проверки усвоения дисциплины и оказания помощи в расчётах конструкции п/п резисторов и БПТ. Применяемый подход позволяет сократить время на выполнение рутинных операций расчётов и оформление текстов, снижает непроизводственные затраты времени в изучении дисциплины.

Работу в этом направлении выполняли предшественники в курсовых и дипломных проектах, однако функционирования программы на настоящее время по разным причинам нет [1]. Очередная попытка принята в представленной работе.

Программа моделирования состоит из части для преподавателя и части для студента. На рис. 1 представлена укрупнённая структура средства.

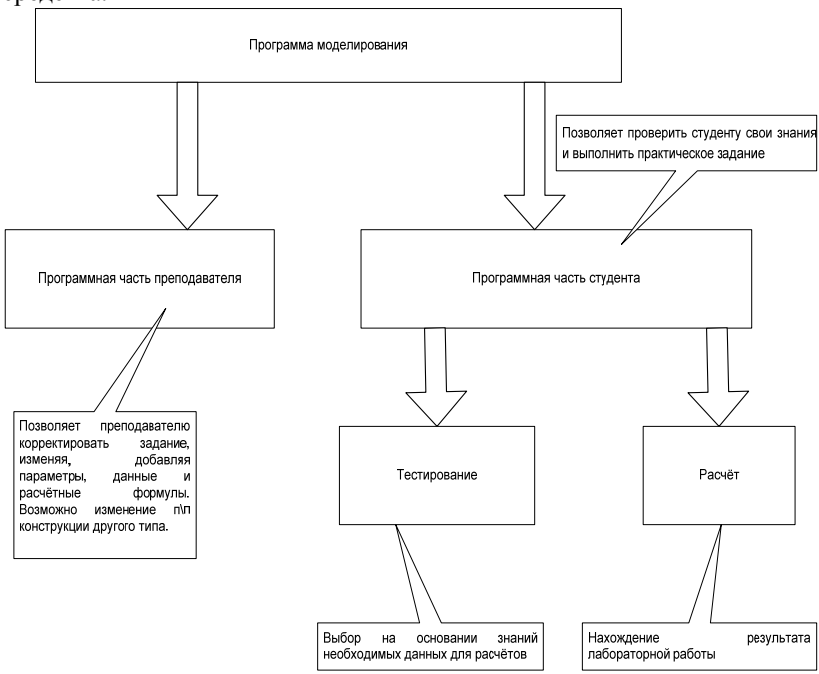


Рис. 1. Структурная схема состава программы

Программная часть для преподавателя позволяет изменять, добавлять расчётные формулы, параметры и их значения. В ходе эксплуатации программного комплекса практические задания могут корректироваться или полностью меняться.

Программная часть для использования студентом состоит из теста на предмет усвоения дисциплины и расчёта параметров по нахождению зависимостей конструкций.

При тестировании студента выводятся рисунки структуры топологии приборов, сводка исходных данных, которую студент может редактировать.

Тестирование предполагает возможность пройти тест на проверку своих знаний для расчёта зависимостей размеров конструкции приборов, а в качестве поощрения за правильные ответы получать числовые значения характеристик исследованных зависимостей.

Расчёт размеров конструкций приборов состоит из расчётных формул, которые указаны и определены в ходе тестирования, также возможно изменение необходимых значений.

В режиме «Тестирование» результат поэтапных расчётов конструкции накапливается и может быть повторён с изменением цифровых данных без повторного прохождения тестирования.

По завершении расчётов программный комплекс выводит на монитор указанные зависимости в графическом виде, и формируется отчёт с полученными расчётными значениями, которые впоследствии могут редактироваться. Затем отчёт можно вывести на печать.

Программа моделирования реализуется на языке программирования C++ (Builder). Вызвано это тем, что у языка C ++ наработаны более обширные библиотеки функций, которые позволяют реализовать программу. Профессиональные библиотеки не только во много раз уменьшают сроки разработки программ, но и снижают возникновение случайных программных ошибок [2].

C ++ одинаково подходит как для новичка (позволяет с небольшими затратами сил и времени создавать прикладные программы), так и для опытного профессионала (создание сложных приложений, работающих с любыми базами).

ЛИТЕРАТУРА

1. Торгонский Л.А., Савельев Д.В., Серов С.А. // Интеллектуальные системы в управлении, конструировании и образовании: Сб. статей. Вып. 5 / Под ред. А.А. Шелупанова. Томск: Изд-во Ин-та оптики атмосферы, 2006. 132 с.

2. Архангельский А.Я. Программирование в C ++ Builder 6. М.: БИНОМ, 2008. 1152 с.

3. Торгонский Л.А. Проектирование интегральных микросхем и микропроцессоров: Лабор. пособие. ТУСУР, Томск: 2011. 23 с.

РОЛЬ ПОДЪЕМНО-ОСМОТРОВОГО ОБОРУДОВАНИЯ ПРИ ОБСЛУЖИВАНИИ ГРУЗОВЫХ АВТОМОБИЛЕЙ

В.В. Мытько*, *студент
Научный руководитель Т.Ю. Лебединская, *доцент*, *к.т.н*
г. Краснодар, *КубГТУ*, *www.kubstu.ru*

Оборудование для автосервиса оказывает влияние на качество и себестоимость работ. К выбору таких конструкций необходимо подходить очень серьезно, так как ни один, даже самый лучший специалист не сможет произвести ремонт автомобиля без соответствующего технического оснащения. Автосервис отличается от частного гаража тем, что оборудование там должно быть представлено в разнообразном ассортименте, так как уровень проводимых в нем работ намного более сложен, чем самостоятельное устранение некоторых неполадок.

Для создания удобства при техническом обслуживании, ремонте и облегчения труда используют подъемно-осмотровое оборудование, обеспечивающее возможность работы снизу автомобиля.

По расположению автомобиля относительно уровня пола поста все подъемно-осмотровое оборудование делят на две группы:

– оборудование, при котором автомобиль устанавливают на уровне пола – различные осмотровые канавы;

– оборудование, позволяющее поднимать весь автомобиль или его часть (переднюю или заднюю ось), – подъемники, тали, краны и домкраты.

Промышленность ориентируется на выпуск второй группы.

Ввиду габаритов и массы грузовых автомобилей для их обслуживания особую актуальность имеют подъемники. В наше время существует большое количество специализированных станций, выполняющих ограниченный вид работ, это привело к выпуску подъемников, предназначенных именно для кузовного ремонта и покраски, участка сходразвала колес, участка шиномонтажа. Все они, как правило, предлагаются вместе с другим оборудованием и наиболее эффективно работают в комплексе.

На сегодняшний момент наибольшее применение находят электрогидравлические подъемники, имеющие ряд весомых преимуществ перед электромеханическими подъемниками:

– отсутствие быстроизнашивающихся механических частей (винтов, гаек) подъемника;

– отсутствие необходимости регулярного контроля и регулировки зазоров между рабочей и страховочной гайками;

– более высокий ресурс и надежность;

– упрощенное ТО;

– плавность хода;

– низкий шум;

– меньшее потребление электроэнергии;

– возможность легко опустить автомобиль при сбое электроснабжения.

Но за эти преимущества приходится платить: электрогидравлический подъемник сложнее в производстве, и цена зачастую в полтора раза выше, чем у аналогичного электромеханического подъемника.

В таблице представлены некоторые модели подъемников, которые можно приобрести в нашей стране. Информация о продавце, технических характеристиках изделий находится в [1–4] .

Краткий обзор подъемников, представленных на российском рынке

Модель	Тип конструкции	Страна-производитель	Грузоподъемность, т	Цена, тыс. руб.
HD-18	Четырехстоечный, электрогидравлический	США	8	577
HD-27X	Четырехстоечный, электрогидравлический	США	12	739
HD-35	Четырехстоечный, электрогидравлический	США	16	964
HD-40X	Четырехстоечный, электрогидравлический	США	18	1 269
ПС-10	Четырехстоичный, электромеханический, бесплатформенный	Россия	10	303
12Г272М	Гидравлический, параллелограммный	Россия	12	670
24Г272М	Гидравлический, параллелограммный	Россия	24	867
ПС-15	Шестистоечный, электромеханический	Россия	15	420
ПЛ-15	Электромеханический, четырехстоечный	Россия	15	389
ПЛ-20	Электромеханический, четырехстоечный	Россия	20	453
ПЛ-25	Электромеханический, шестистоечный	Россия	25	584
ПГ-30	Четырехстоечный, электрогидравлический	Россия	30	690
RAV4800	Электрогидравлический, четырехстоечный	Италия	8	410
RAV 709	Электрогидравлический, ножничный	Италия	9	1235
RAV718	Электрогидравлический, ножничный	Италия	18	1567
RAV 733	Электрогидравлический, ножничный	Италия	33	2170
RAV 755	Электрогидравлический, ножничный	Италия	55	3814

Сегодня на российском рынке представлено большое количество различных автомобильных подъемников. Для каждого грузового автосервиса можно выбрать подходящий по качеству и стоимости подъемник.

ЛИТЕРАТУРА

1. Подъемники четырехстоечные [Электронный ресурс]. URL: http://www.ttsauto.ru/katalog-oborudovaniya/gruzovoj-avtoservis/podemnoe-oborudovanie/70/ (дата обращения: 05.03.2012).

2. Подъемники для грузовых автомобилей и автобусов [Электронный ресурс]. URL: http://www.mrmz.ru/electro/avtoservis/servis/gruz.html (дата обращения: 06.03.2012).

3. Каталог – грузовые подъемники [Электронный ресурс]. URL: http://www.bendpak.ru/page3.php. (дата обращения: 07.03.2012).

4. Автомобильные подъемники [Электронный ресурс]. URL: http://www.technosouz.ru/Pages/hoisting_gear_rus.html (дата обращения: 09.03.2012).

ЭЛЕКТРОДУГОВАЯ НАПЛАВКА ШЕЕК ВАЛОВ ПОРОШКОВОЙ ПРОВОЛОКОЙ

В.В. Николаев*, *А.А. Копытин*, *студенты

Научный руководитель Т.Ю. Лебединская, *доцент*, *к.т.н.*

г. Краснодар, *ГОУ ВПО «Кубанский государственный технологический университет»*

При длительной эксплуатации машин изнашивание деталей сопровождается снижением эксплуатационных показателей, что, в частности, вызывает ухудшение качества изготавливаемых изделий и выполняемых работ. Изнашивание рабочих поверхностей деталей нередко требует их полной замены. Это повышает себестоимость производства из-за больших амортизационных отчислений. В ряде случаев изготовление деталей целиком из износостойкой легированной стали нерационально в связи с трудностью обработки и высокой стоимостью стали. Поэтому для решения задач повышения эксплуатационных показателей и увеличения срока службы деталей машин используют различные способы поверхностного упрочнения, в частности наплавку, нашедшую широкое применение в производстве разнообразных изделий – от крупногабаритных, таких как валки прокатных станов (металлургия), до мелких деталей типа седел и клапанов двигателей внутреннего сгорания.

Наплавка без защитной среды осуществляется порошковой проволокой при отсутствии подачи флюса или защитного газа в зону дуги. Наплавка открытой дугой порошковой проволокой обладает следующими преимуществами:

1) простота используемого оборудования и технологии, связанная с отсутствием необходимости применения защитного газа и флюса;

2) возможность наплавки в полевых условиях, поскольку ветер практически не оказывает влияния на процесс наплавки;

3) сравнительная простота введения легирующих элементов в наплавленный металл, состав которого можно регулировать в широких пределах.

Проблема наплавки этим способом, связанная с обильным выделением дыма, решена разработкой специального дымового коллектора. Кроме этого, к недостаткам порошковых проволок можно отнести относительно высокую стоимость и свойство металла образовывать неравномерную структуру и поры.

Порошковая проволока представляет собой стальную ленту, свернутую в трубку, наполненную различными легирующими элементами в виде механической смеси. Проволоки различают по конструкции, назначению и составу механической смеси.

Состав механической смеси определяет ее свойства и назначение. В состав входят газообразующие, шлакообразующие, легирующие, раскисляющие, ионизирующие и другие компоненты.

Трубку изготавливают вальцовкой из малоуглеродистой ленты. Наиболее распространены проволоки сплошного и простого трубчатого сечения.

При горении дуги механическая смесь отстает в расплавлении от оболочки, что ухудшает защиту и свойства наплавленного металла. Чтобы повысить электропроводность механической смеси, в нее добавляют до 30% железного порошка или разделяют сердечник проволоки металлическими перегородками, электрически связанными с ее оболочкой.

По назначению проволоки предназначаются для сварки углеродистых и низколегированных сталей; легированных и высоколегированных сталей; цветных металлов и сплавов; наплавки поверхностных слоев с особыми свойствами.

По составу механической смеси проволоки бывают с внешней защитой (под флюсом или в среде углекислого газа) и самозащитные. Токопроводящей частью порошковой проволоки служит металлическая лента (оболочка). Некоторые характеристики порошковых проволок приведены в табл. 1.

Дуга горит между лентой и деталью. Механическая смесь проволоки плавится быстрее оболочки, что способствует лучшему переходу легирующих элементов механической смеси в наплавочный металл.

Известна установка для автоматической наплавки УАНТ-01 [2] (производство Россия, г. Пенза), которая предназначена для автоматической электродуговой наплавки и сварки внутренних и наружных поверхностей деталей цилиндрической формы. Режимы наплавки порошковой проволокой приведены в табл. 2 [1. С. 120].

Таблица 1

Характеристики порошковых проволок для наплавки деталей [1. С. 119]

№	Проволока	Химический состав наплавленного металла, %							HR C
		C	Cr	Mn	W	Si	V	Ti	
1	ПП-3Х3Ф-О	0,3	5,5	0,5	4,5	0,6	0,6	–	40
2	ПП-У15Х12М-О	1,7	2,5	0,5	–	0,8	0,4	0,1	42
3	ПП-У25Х17Т-О	2,6	18	0,6	–	0,6	–	0,7	44
4	ПП-3Х2В8Т	0,65	3	1,2	10	0,35	0,5	1,2	44

Таблица 2

Рекомендуемые режимы наплавки порошковой проволокой [1. С. 120]

Проволока	Диаметр детали	Режимы наплавки			
		Сила тока сварки, А	Напряжение дуги, В	Скорость наплавки, м/ч	Шаг наплавки, мм/об
ПП– У25Х17ТО диаметром 3 мм	50…60	200…300	22…24	35…40	4,0…4,5
	60…75	240…250	24…26	30…35	4,5…5,6
	70…85	260…280	26…28	25…30	5,5…6,0
ПП-1Х14Т-О диаметром 2 мм	44…55	160…180	22…24	25…35	2,5…3,0
	50…65	160…180	22…24	20…25	3,5…4,0
	60…75	200…220	24…26	15…20	4,5…5,0

Проволока ПП-3Х3Ф-О применяется в случае, если восстанавливаемая деталь работает при высоких удельных нагрузках при повышенных температурах. ПП-У15Х12М-О и ПП-У25Х17Т-О применяются при абразивном изнашивании и больших ударных нагрузках. ПП-3Х2В8Т применяется при больших нагрузках.

Основные технические характеристики установки УАНТ-01 отражены в табл. 3.

Таблица 3

Технические характеристики установки УАНТ-01

Наименование характеристики	Значение
Грузоподъемность, кг	120
Габариты восстанавливаемой детали, мм: – диаметр – длина – длина наплавляемой поверхности – диаметр наплавляемой поверхности	 30–1700 10–700 10–200 30–620
Частота вращения детали, об/мин	0–10
Скорость горизонтального перемещения горелки, мм/мин	0–16
Направление горизонтального перемещения	Реверсивное
Регулирование скоростей вращения и перемещения горелки	Плавное независимое
Скорость сварки, мм/с	1–25
Шаг наплавки швов, мм	1–7
Напряжение питания, В	220±10%
Потребляемая мощность, кВт, не более	1,5

ЛИТЕРАТУРА

1. Поправка Д.Л., Иосифов В.В. Технология восстановления автомобильных деталей. Краснодар, 2009.

2. Сварка, резка, металлообработка: autoWolding.ru, 2010.

3. Машиностроение. Терминологический словарь / Под ред. М.К. Узкова, Э.Ф. Богданова, М., 1995.

МАТЕМАТИЧЕСКОЕ И АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЭНЕРГОЭФФЕКТИВНОЙ РАБОТЫ ВОДОГРЕЙНОЙ КОТЕЛЬНОЙ

А.Ж. Нукин*, *студент 1-го курса магистратуры

Научный руководитель С.Г. Михальченко, *доцент каф.ПрЭ*, *к.т.н.*

г. Томск, *ТУСУР*, *nukas1989@mail.ru*

В статье [1] были рассмотрены работа котельной, средства автоматизации, используемые в ней.

В данной статье сделана попытка описать законы регулирования. Входными параметрами являются температура подаваемой воды, расход воздуха, расход газа. Выходные параметры: расход воды, температура воды на выходе, давление в трубах, температура дымовых газов, концентрация углекислого газа в дымовых газах.

Основным параметром работы котельной является температура воды на выходе. Этот параметр регулируется сжиганием смеси газ–воздух. Для обеспечения качественного горения газа необходимо в достаточном количестве подвести воздух в зону горения и добиться хорошего перемешивания газа с воздухом. Оптимальным соотношением считается 1:10. То есть на одну часть газа приходится десять частей воздуха. При этом происходит максимальное высвобождение теплоты и нет излишков воздуха. При сжигании топлива происходит радиационный и конвективный нагрев. Конвективный нагрев рассчитывается по формуле (1):

$$Q = \alpha F (T_{ст} - T_{ж}), \quad (1)$$

где α – коэффициент теплоотдачи; $T_{ст}$ – температура стенок трубы; $T_{ж}$ – температура жидкости.

Радиационный нагрев вычисляется по формуле (2):

$$Q = \delta T^4, \quad (2)$$

где δ – константа излучения; T – температура горючей смеси.

Влияние температуры воды на входе и расхода воды на температуру воды на выходе из котла ясно показывает формула

$$Q = cm(T_к - T_н), \quad (3)$$

где c – удельная теплоемкость воды; m – масса воды; $T_к$ – конечная температура воды; $T_н$ – начальная температура воды.

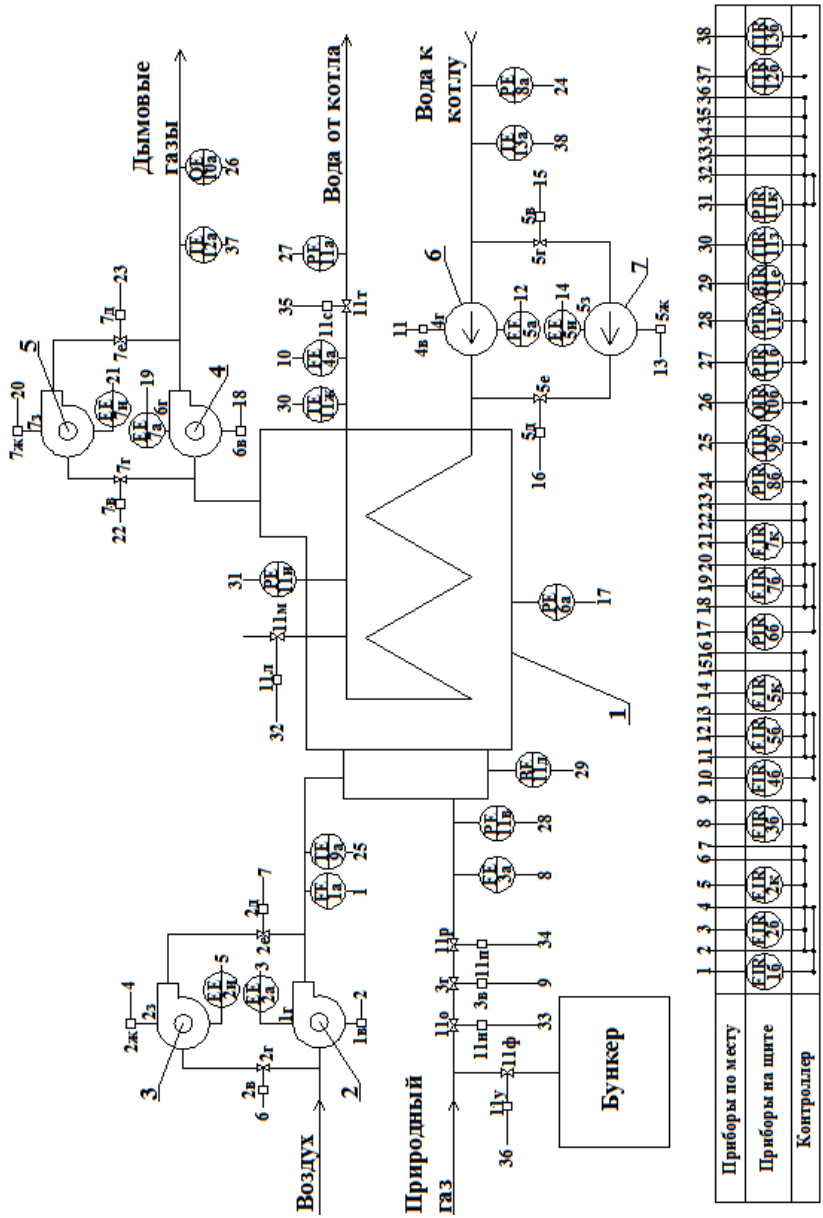


Рис. 1. Функциональная схема автоматизации водогрейной котельной

Давление в трубах создается насосом, который также регулирует расход воды.

Температура дымовых газов зависит от того, насколько хорошо был проведен конвективный нагрев.

Содержание вредных примесей в дымовых газах зависит от того, насколько качественно будет происходить процесс горения [2].

Для применения в автоматизированной системе управления энергоэффективных законов регулирования температуры воды на выходе и давления в трубах требуется модернизация функциональной схемы автоматизированной системы управления водогрейной котельной. Модернизированная функциональная схема водогрейной котельной представлена на рис. 1. Были добавлены резервный вентилятор *3*, резервный дымосос *5* и резервный насос *7*.

Описанные выше зависимости станут основой для создания алгоритмов функционирования, которые будут вшиты в контроллер.

ЛИТЕРАТУРА

1. Нукин А.Ж. Энергоэффективность работы водогрейной котельной // Итоги научно-исследовательских работ и курсового проектирования студентов 1–6-х курсов кафедры промышленной электроники: матер. ежегод. науч.-практ. конф. / Под ред. В.Д. Семенова. Вып. 5. Томск: Том. гос. ун-т систем упр. и радиоэлектроники, 2011. 81 с.

2. Соколов Б.А. Котельные установки и их эксплуатация: учеб. для начального профессионального образования. 2-е изд., испр. М.: Изд. центр «Академия», 2007. 432 с.

СТАТИСТИЧЕСКИЕ ОЦЕНКИ БЛИЗОСТИ ТЕКСТОВЫХ ДОКУМЕНТОВ

Е.О. Оплачко*, *студент 5-го курса каф. КИБЭВС

г. Томск, *ТУСУР*, *ФВС*, *ekatopla@sibmail.com*

Проблема сравнения текстовой информации и выявление степени сходства является одной из наиболее важных и трудных задач анализа данных и поиска информации. Учитывать схожесть текстовых документов необходимо при разработке поисковых систем и повышения их качества за счет удаления избыточной дублирующей информации, кластеризации, при объединении информации в тематические группы или фильтрации необходимой информации. Также определение схожести текстовых документов используется при установлении авторства или выявлении факта плагиата [1].

В данной работе ставится задача сопоставления учебных планов и государственных образовательных стандартов, что позволит опреде-

лить соответствие учебного плана требованиям стандартов или учебных планов между собой. Таким образом, необходимо получить оценку схожести данных документов. С этой целью проведено исследование основных способов оценки близости текстовых документов.

Статистический анализ – это частотный анализ в тех или иных его вариациях. Общая суть такого анализа заключается в подсчете количества повторений слов в тексте и использовании результатов подсчета для конкретных целей [2].

Наиболее распространено векторное представление текстового документа. Для каждого терма в документе фиксируется его наличие в виде 1, или отсутствие 0, тогда текст представляется в виде двоичного вектора. Или же каждому терму сопоставляется его вес в документе, в большинстве случаев положительное число, тогда текст представляет собой вектор с положительными компонентами.

Оценки сравнения объектов, состоящих из двоичных элементов, основываются на значениях:

– мощность множества свойств, присутствующих в обоих объектах, т.е. $p = |\{b_k;\ b_k \in i,\ \ b_k \in j\}|$;

– мощность множества свойств, присутствующих в объекте i и отсутствующих в j, т.е. $q = |\{b_k;\ b_k \in i,\ \ b_k \notin j\}|$;

– мощность множества свойств, отсутствующих в объекте i и присутствующих в j, т.е. $r = |\{b_k;\ b_k \notin i,\ \ b_k \in j\}|$;

– мощность множества свойств, отсутствующих в обоих объектах, т.е. $t = |\{b_k;\ b_k \notin i,\ \ b_k \notin j\}|$.

Существуют три распространенные оценки [3]:

• Коэффициент Джакарда, оценивающий близость. Его значение увеличивается пропорционально тому, на сколько элементы близки друг другу:

$$s_{ij} = \frac{p}{p+q+r}.$$

Также коэффициент Джакарда называют оценкой асимметричной информации. Требованием к входным объектам является наличие хотя бы одного свойства. Значением оценки является вещественное число в интервале [1; 0].

• Простейшим коэффициентом соответствия (Simple Matching Coefficient) называют

$$s_{ij} = \frac{p+t}{n}.$$

Данный коэффициент является мерой близости двух объектов. В отличие от коэффициента Джакарда, простейший коэффициент соот-

ветствия дает оценку симметричной информации. Результатом является вещественное число в интервале [1;0].

• Третья оценка – расстояние Хемминга – оценивает количество различных элементов между объектами и является оценкой удаленности объектов:

$$d_{ij} = q + r.$$

Результатом является натуральное число или ноль.

Оценки сравнения объектов, состоящих из двоичных элементов, распространены из-за простоты их вычисления. Однако в случаях, когда такие оценки являются недостаточными, используются объекты, состоящие из весовых элементов.

Одним из самых простых подходов определения веса является использование нормализованной частоты данного терма в документе:

$$w_{ij} = \frac{n_{ij}}{N_j},$$

где n_{ij} – количество повторений данного терма в документе; N_j – общее количество всех термов в документе.

Более сложные варианты расчета весов учитывают частоту использования данного терма в других документах коллекции. Но эти варианты возможны только при наличии статистики использования термов в коллекции. Такой метрикой является TF-IDF.

TF-IDF – мера, используемая для оценки важности слова в контексте документа, являющегося частью коллекции документов.

TF (частота слова) – отношение числа вхождения некоторого слова к общему количеству слов документа, аналогично рассмотренное выше.

$$TF = \frac{n_i}{\sum_k n_k},$$

где n_i есть число вхождений слова в документ, а в знаменателе – общее число слов в данном документе.

IDF (обратная частота документа) – инверсия частоты, с которой некоторое слово встречается в документах коллекции. Учёт IDF уменьшает вес широкоупотребительных слов.

$$\mathrm{IDF} = \log \frac{|D|}{|(d_i \supset t_i)|},$$

где $|D|$ – количество документов в корпусе; $(d_i \supset t_i)$ – количество документов, в которых встречается t_i (когда $n_i \neq 0$).

Таким образом, мера TF-IDF является произведением двух сомножителей: TF и IDF.

Одной из наиболее распространенных метрик близости является уголовое разнесение [3]:

$$s_{ij} = \frac{\sum_{k=1}^{n} x_{ik} \times x_{jk}}{\sqrt{\sum_{k=1}^{n} x_{ik}^2 \times \sum_{r=1}^{n} x_{ir}^2}}.$$

Эта метрика аналогична косинусу угла между векторами, т.е. текст представляется в виде вектора с весовыми компонентами.

Рассмотренные метрики позволяют достаточно эффективно вычислять близость полнотекстовых документов, но учебный план и программа обладают четко определенной структурой, что делает данные подходы недостаточно эффективными. Для применения данных метрик для поставленной задачи необходимо проводить тщательную предварительную обработку текста.

ЛИТЕРАТУРА

1. Моченов С.В., Бледнов А.М., Луговских Ю.А. Применение статистических методов для семантического анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2005.

2. Чугреев В.Л. Модель структурного представления текстовой информации и метод ее тематического анализа на основе частотно-контекстной классификации (дис.) [Электронный ресурс]. Режим доступа: http://www.gotai.net

3. Комарова А.С. Оценка релевантности электронных документов к онтологии в системе информационного менеджмента // Труды СПИИРАН. Вып. 3. Т. 1. СПб.: Наука, 2006.

УСТРОЙСТВО ТЕСТИРОВАНИЯ ПАМЯТИ

О.В. Пехов*, *студент 5-го курса каф. КИБЭВС

Научный руководитель П.Н. Коваленко, инженер каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, ФВС, olegych@sibmail.com

Оперативная память (ОЗУ) является одним из важнейших элементов компьютера. На сегодняшний момент существует большое количество известных типов памяти, которые строятся на базе относительно недорогой динамической памяти – DRAM (Dynamic Random Access Memory – динамическая память с произвольным доступом) [1].

Для определения работоспособности ОЗУ персонального компьютера используется специальное программное обеспечение, которое исполняется в начальный момент после его включения. Это обеспечение находится в составе базовой системы ввода-вывода материнской

платы компьютера. В случае дефектной работы памяти дальнейшая работа компьютера заканчивается. Вследствие этого достаточно сложно определить причину и место ошибки в модуле памяти. В таких случаях применяются специальные устройства, которые позволяют производить тест памяти в различных режимах. Эти устройства позволяют выявить рабочие параметры модуля памяти, найти проблемные места, обнаружить неработающие микросхемы. Для этого проверяется соответствие считанных данных с записанными.

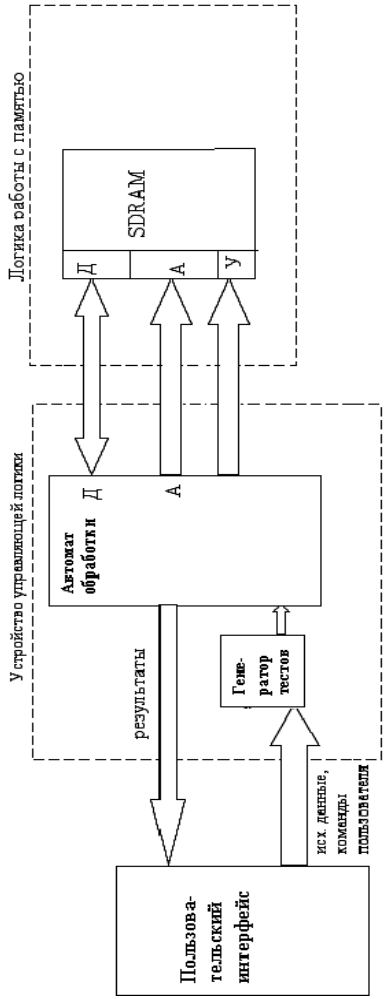


Рис. 1. Структура устройства тестирования памяти

В составе разрабатываемого устройства можно выделить три основные части: пользовательский интерфейс; блок логики работы с памятью; блок управляющей логики. Дальнейшая детализация этих частей позволит построить полную структурную схему проектируемого устройства.

Пользовательский интерфейс должен обеспечивать удобную индикацию результатов и хода теста, возможность с помощью кнопок задавать тестовую последовательность, а также приостанавливать и запускать тесты. Для этого должен быть обеспечен необходимый минимум управляющих элементов. Обработкой команд, поступающих от пользователя, и отображением результатов проверки будет заниматься микропроцессор, выполненный в качестве soft-core процессора.

Термин «soft-core процессор» означает процессор, поведение которого представлено при помощи языка описания электронных схем (Verilog, VHDL) и реализуется синтезом на программируемой логической интегральной схеме (ПЛИС). Примером такого процессора является picoBlaze от фирмы Xilinx. Использование soft-core процессоров позволяет сократить время на разработку, уменьшить цену изделия, повысить эргономические показатели конечного устройства, что позволит ему быть конкурентоспособным на рынке [2].

Применение процессора, а не конечного автомата в качестве управляющего интерфейсной частью элемента, дает возможность для гибкого изменения интерфейсной части. Использование конечного автомата ограничивается числом его рабочих состояний, а добавление новых состояний требует полного переписывания алгоритма работы автомата и при этом снижается его быстродействие. Для микропроцессора количество состояний ограничивается только объемом памяти программ и изменение их количества не требует изменения алгоритма.

Второй частью системы является блок логики работы с памятью. Он отвечает за выполнение операций с ОЗУ. Так как устройство должно тестировать память, соответственно все обращения к ней должны осуществляться точно так же, как и в рабочем режиме. Это означает, что контроллер памяти в проектируемом устройстве и в компьютерной системе должен работать одинаково. Поэтому необходимо определить все возможные состояния памяти, а соответственно и контроллера. При разработке контроллера, согласно описанию работы памяти и ее системы команд, строится диаграмма состояний, в которой описаны необходимые для работы памяти состояния, а также с помощью стрелочек указаны все возможные переходы между состояниями. Эти переходы осуществляются при подаче команд на адресную шину контроллера. Результатом работы стала диаграмма состояний, изображенная на рис. 2.

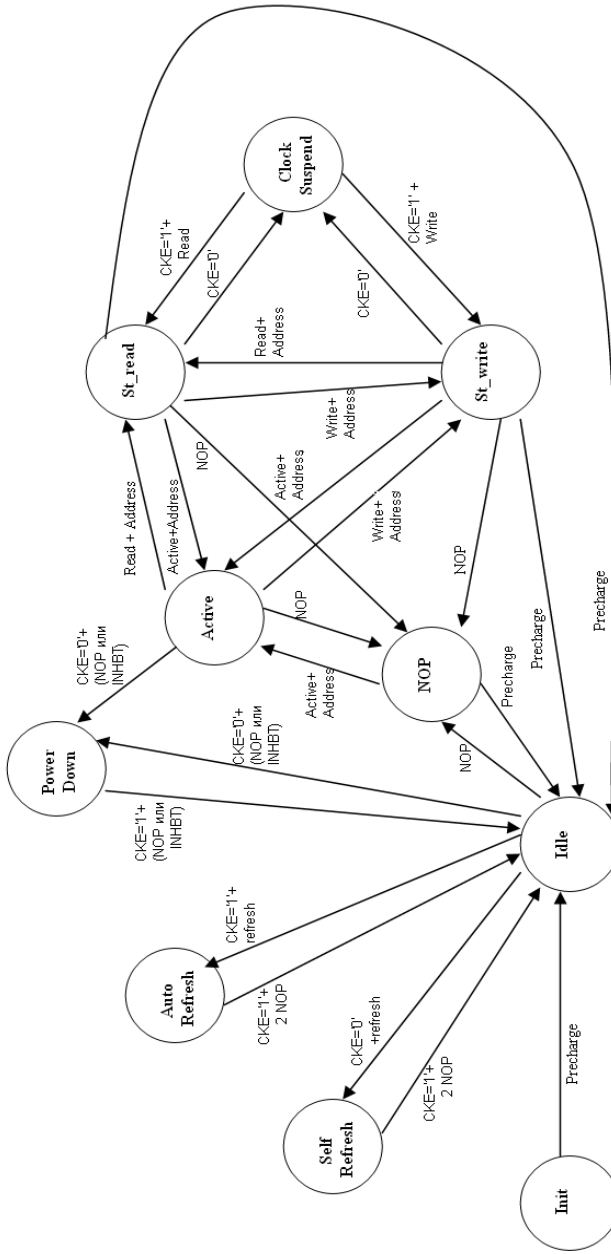


Рис. 2. Диаграмма состояний контроллера

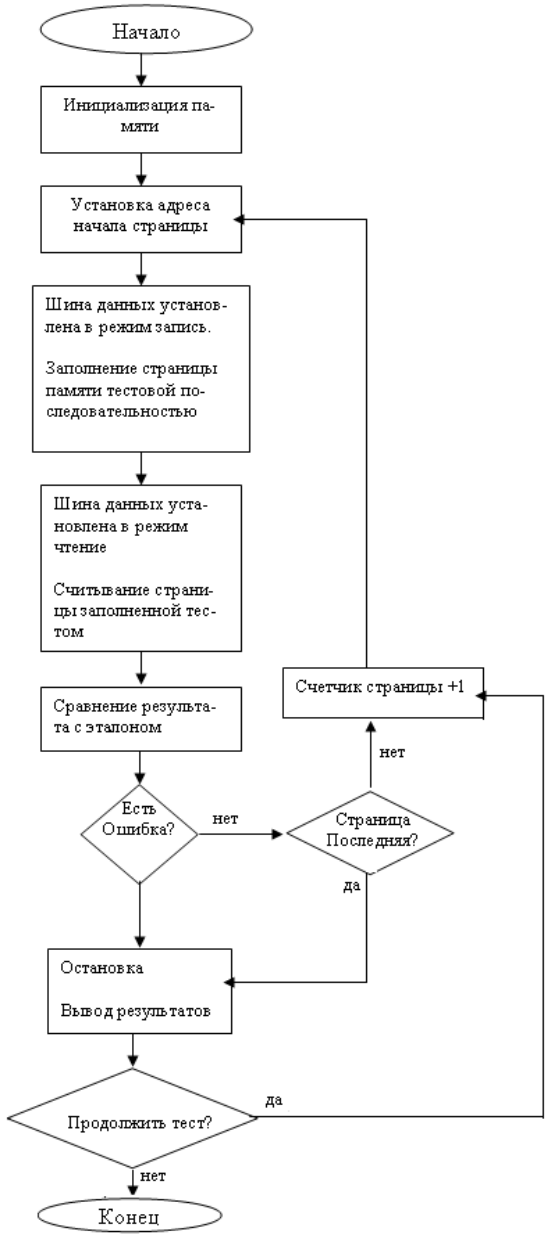


Рис. 3. Алгоритм работы устройства тестирования

Алгоритм работы устройства изображен в виде блок-схемы и представлен на рис. 3. После запуска теста начинается работа с памятью. Вначале, необходимо провести инициализацию памяти. В процессе инициализации производится установка регистра управления, для определения дальнейшего режима работы с памятью.

На следующем шаге, на адресную шину поступает адрес страницы и производится заполнение страницы тестовой последовательностью. После того как получен сигнал об окончании страницы, шина данных переводится в режим чтения и производится считывание записанных в память данных. Устройство управляющей логики сравнивает результат с эталонными данными, и если обнаружено несоответствие, то происходит увеличение счетчика ошибок. В результате этого работа устройства приостанавливается и выводится адрес страницы и показано несоответствие данных, т.е. сама ошибка. Зафиксировав ошибку, пользователь может продолжить работу теста или прекратить его выполнение на свое усмотрение.

ЛИТЕРАТУРА

1. http://www.3rmemory.ru/support/faq/tech/st/. Энциклопедия памяти: оперативная память.

2. Коваленко П.Н., Шелупанов А.А. Обзор программных процессоров // Научная сессия ТУСУР–2011. Томск, 2011. Ч. 3. С. 52–55.

АНАЛИЗ И ВЫБОР КОНСТРУКЦИЙ БАЛАНСИРОВОЧНЫХ СТЕНДОВ ДЛЯ ШИНОМОНТАЖНЫХ РАБОТ

Б.П. Полонец, Г.А. Шабалин, студенты

Научный руководитель Т.Ю. Лебединская, доцент, к.т.н.
г. Краснодар, ГОУ ВПО «Кубанский государственный технологический университет»

В настоящее время на российском рынке технологического оборудования для шиномонтажных работ представлено множество различных моделей балансировочных стендов, что в свою очередь усложняет выбор. Балансировочные стенды просты в использовании: основной деталью станка является вал, определяющий динамику колебаний. Автоматический старт и остановка делают работу с агрегатом быстрой и простой для оператора.

Современные модели балансировочных станков оснащены цветными ЖК-мониторами, позволяющими специалисту видеть значения дисбаланса и сервисные коды. Полуавтоматические балансировочные стенды дают возможность одновременно замерить при помощи автоматической линейки радиус автомобильного колеса и расстояние до него.

Автоматические балансировочные станки позволяют измерить расстояние до колеса, его радиус и ширину. Все замеры на стенде производятся без нажатия кнопок оператором, т.е. диагностические процессы, которые выполняет данный станок, полностью автоматизированы.

Для его облегчения необходимо максимально сузить круг поиска. Сначала нужно определить, какие бренды наиболее представлены в районе, где осуществляется деятельность. Это позволит без проблем приобрести оборудование и получить необходимую поддержку со стороны дистрибьютора в сервисном обслуживании стендов. Заключающим этапом будет выбор ценового диапазона. Наиболее распространенные фирмы указаны в таблице.

Производители балансировочных стендов

Россия	Китай	Италия	Германия
СТОРМ	TAG	CORGHI	Hofmann
Sivik	Nordberg Automotive	ItalEQUID	John Bean
	Zuver	Sice	Beissbarth
	AET	Ravaglioli	
		Teco	

Самое распространенное оборудование на российском рынке будет итальянское, на втором месте российское, на третьем месте немецкое и менее распространено китайское. Список наиболее представленных фирм на российском рынке будет выглядеть следующим образом: Ravaglioli, Sivik, Hofmann, Zuver.

Hofmann – немецкая компания, созданная в 1931 г. Основная специализация предприятия – создание шиномонтажных станков и балансировочных устройств. Сегодня компания предлагает более 18 серий профессиональных стендов для балансировки колес легковых и грузовых автомобилей. Среди основных преимуществ, которыми отличается балансировочный станок Hofmann, – автоматический зажим колес, использование бесконтактной лазерной техники измерения, широкий выбор диагностических функций, получение справочной информации в режиме реального времени. Балансировочные стенды и другая продукция Hofmann сертифицированы в соответствии с немецким стандартом качества DIN EN ISO 9001.

Ravaglioli – итальянская компания, созданная в 1958 г. Основная специализация фирмы – создание диагностического, шиномонтажного, балансировочного, подъемного и ремонтного оборудования для автосервисов. Сегодня компания предлагает более 30 видов станков, стендов и других агрегатов для автосервисов. Среди основных преимуществ, отличающих станки и другое оборудование Ravaglioli, – воз-

можность использования балансировочных устройств для легковых и грузовых автомобилей, наличие русифицированного ПО, измерение полной геометрии ходовой части. Балансировочные станки Ravaglioli сертифицированы в соответствии с европейским стандартом качества UNI EN ISO 9001.

AET – китайский производитель балансировочных и шиномонтажных стендов и другого ремонтного оборудования для автосервисов. Сегодня компания предлагает более 10 профессиональных балансировочных устройств для автомобилей. Среди основных преимуществ, которыми отличается станок AET – надежность, долгий срок службы и высокая производительность. Продукция компании соответствует международным стандартам качества ISO 9001.

Sivik – НПО «Компания СИВИК» уже более 17 лет занимается разработкой и производством автосервисного оборудования. За это время удалось занять лидирующие позиции на российском рынке. Сегодня уже более 40% российских автосервисов и шиномонтажных мастерских используют в своей работе оборудование Sivik. Ведется активное расширение географии продаж. Продукция компании получила заслуженное признание за пределами России и успешно поставляется более чем в 10 стран мира.

НПО «Компания СИВИК» контролирует весь научно-производственный цикл: от идеи до конечного продукта. С 2007 г. система управления качеством на предприятии сертифицирована по международному стандарту ISO 9001.

Цена балансировочного станка зависит от следующих факторов:

− Технических характеристик, таких как ширина, длина и диаметр обода, максимальный вес колеса диагностируемого автомобиля, точность чтения данных, количество измерительных головок и скорость их вращения. Также учитывается время, за которое стенд осуществляет полный диагностический и балансировочный цикл, и другие показатели.

− Степень автоматизации, от возможности автоматического хранения, обработки и передачи данных о расстоянии и диаметре колесной базы, от наличия функции автоматического торможения колеса после диагностики на стенде и пр. Также учитывается возможность самонастройки и самосинхронизации, которая позволяет использовать станок без выполнения регулярных калибровок оборудования.

− Характеристика цифрового оборудования и программного обеспечения (ПО), исходя из наличия русифицированного ПО, поддержки станком 3D-графики, беспроводных технологий и пр. Также мощность компьютерных микропроцессоров, обрабатывающих балан-

сировочные данные, наличие принтера для печати отчетов, цветного монитора для отображения диагностических данных и др.

При сравнении моделей и выборе оптимальной конструкции первым этапом является изучение модельного ряда каждой из представленных фирм. Второй этап – это непосредственный выбор модели для дальнейшего сравнения. Заключающий этап – сравнение цен конкурирующего оборудования для балансировки колес.

Hofmann. Можно выделить две модели – самую простую и топовую. В качестве простой был выбран Hofmann Geodyna 800, его цена приблизительно равна 70 тыс. руб. и в качестве топового Hofmann Geodyna Optima II, он стоит около 600 тыс. руб.

Ravaglioli. Можно выделить две модели – Ravaglioli G2.124H и Ravaglioli G6.160SH. Их стоимость соответственно 120 и 500 тыс. руб.

AET. Ценовой диапазон данного производителя будет начинаться от 30 и заканчиваться 50 тыс. руб. Это стоимость AET DST910B и AET BL822 соответственно.

Sivik. Наиболее предпочтительно обратить внимание на следующие стенды. Sivik SPUTNIK СБМК-60, его цена приблизительно равна 60 тыс. руб., и Sivik GALAXY СБМП 60/3D, он стоит около 120 тыс. руб.

ЛИТЕРАТУРА

1. Першин В.А. и др. Типаж и техническая эксплуатация оборудования предприятий автосервиса: учебное пособие. Ростов н/Д: Феникс, 2008. 413 с.

2. Сарбаев В.И. и др. Техническое обслуживание и ремонт автомобилей: механизация и экологическая безопасность производственных процессов. Сер. Учебники, учебные пособия. Ростов н/Д: Феникс, 2004. 448 с.

3. http://www.ural-k-s.ru/p/balansirovochnie_stendi.html 12.02.2012.

4. http://www.sivik.ru 16.02.2012.

5. http://www.ravaglioli.com 15.02.2012.

ПРИЛОЖЕНИЕ ДЛЯ МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ ВЗАИМОДЕЙСТВИЯ С WEB-РЕСУРСАМИ

А.А. Поляков*, *А.А. Межевалов*, *А.А. Ковалев*, *студенты 4-го курса

г. Томск, *ТУСУР*, *каф. КИБЭВС*, *ФВС*, *koshachy@gmail.com*

В настоящее время достаточно актуальным является программное обеспечение, разрабатываемое для мобильных платформ, то есть для телефонов, обладающих собственной операционной системой. И это неудивительно – человеку удобно иметь под рукой все необходимые ему функции и инструменты для учебы, работы и всех остальных дел.

За последние пять лет на рынке появились, а также успели исчезнуть многие мобильные операционные системы (ОС): Symbian, RIM Blackberry, Bada, Maemo, Google Android, Apple iOS, Microsoft Windows Phone, Windows Mobile и др. Со временем некоторые операционные системы набрали популярность, другие – изжили себя и перестали поддерживаться разработчиками. По данным агентства Gartner [1] на ноябрь 2011 г., большую нишу на рынке мобильных ОС занимает Google Android, также большие доли имеют Apple iOS, RIM Blackberry и Symbian OS (рис. 1).

Рис. 1. Распределение рынка мобильных ОС

Однако эксперты дают следующую оценку распределения рынка мобильных ОС к 2015 г.: Microsoft Windows Phone и Google Android будут иметь большую долю (порядка 30–40%), Apple iOS и RIM Blackberry – 10–15% рынка. В связи с этим были взяты для работы три следующие платформы: Apple iOS, Google Android и Microsoft Windows Phone.

Для удобства разработки были выбраны нативные для этих систем языки программирования: для Apple iOS – objective-C, для Google Android – Java, для Microsoft Windows Phone – связка C# + Silverlight.

Проект представляет собой приложение, которое дает возможность пользователю читать новости студенческого портала za4et.tusur.ru (rss-лента), а также просматривать учебное расписание для групп ТУСУРа с возможностью поиска группы. Принцип работы приложения можно увидеть на рис. 2.

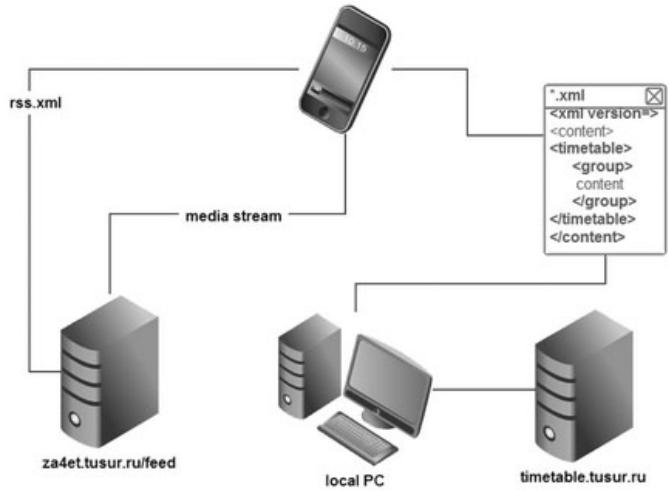


Рис. 2. Упрощенный принцип работы приложения

Как видно из рисунка, приложение получает rss-ленту с сайта za4et.tusur.ru/feed, и с сайта timetable.tusur.ru проходит парсинг расписания в xml-файл на локальной машине с последующим добавлением в приложение.

Результатом работы стали три бета-версии приложения на три разные платформы, пример работы можно увидеть на рис. 3.

Рис. 3. Пример работы приложений на Google Android, Apple iOS, Microsoft Windows Phone

В заключение необходимо отметить, что мобильные технологии имеют огромное будущее и большой потенциал развития. Рынок мо-

бильных приложений постоянно пополняется, и это дает стимул писать оригинальные, необходимые для большинства групп людей актуальные программные решения.

ЛИТЕРАТУРА

1. Gartner, Inc http://www.gartner.com
2. Bert Altenberg, Alex Clarke, Philippe Mougin, Become an Xcoder, русское издание.
3. Российский IT-блог Хабрахабр – http://www.habrahabr.ru
4. Дэвид Хантер, Джефф Рафтер и др. XML. Базовый курс = Beginning XML. М.: Вильямс, 2009. 1344 с
5. Петзольд Ч. Программируем WindowsPhone 7. Redmond, Washington.
6. Хашими С., Коматинени С., Маклин Д. Android. Разработка приложений. СПб.: Питер, 2011.

ДЕДУКТИВНОЕ УСТРОЙСТВО «ПОЗНАЮ МИР»

И.Е. Романова*, *студентка 6-го курса
Научный руководитель Л.А. Торгонский, *доцент каф. КИБЭВС*
г. Томск, *ТУСУР*, *каф. КИБЭВС*, *romanovaaqua@gmail.ru*

На сегодняшний момент необычайно развиты спрос и предложение детских интерактивных игрушек, это обусловлено тем, что игрушки подобного рода помогают ребенку самостоятельно изучать окружающий мир. Во время игры дети расширяют не только кругозор, но и развивают такие качества, как логическое и ассоциативное мышление, память, внимательность, воображение, усидчивость и т.д. [1].

К сожалению, не каждая игрушка может «похвастаться» своей функциональностью и длительной потребности в ней ребенком. Именно поэтому предлагается дедуктивное устройство, которое позволит развивать кругозор детей дошкольного возраста [2].

Устройство представляет собой планшет (рис. 1). На планшете находятся: 10 клавиш с цифрами от 0 до 9 (*1*), 10 светодиодов (*2*), для примера установлена карточка (*3*), кнопка «ПУСК» (*3*). В набор с планшетом входят 9 наборов карточек разных тематик, всего 63 карточки.

Во время игры ребенок устанавливает карточку на макет и при нажатии на кнопку «ПУСК» устройство проигрывает звук, характеризующий изображение на карточке. В это же время загорается комбинация светодиодов, повторив комбинацию светодиодов с помощью клавиш, устройство повторно проигрывает мелодию, характеризующую изображение на карточке.

Схема устройства изображена на рис. 2.

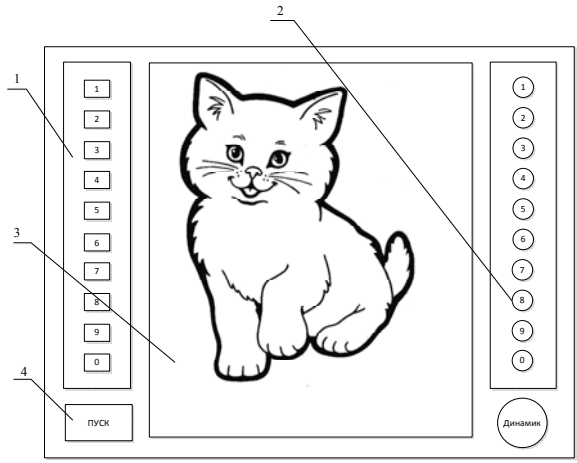


Рис. 1. Примерное изображение устройства с установленной карточкой

Работа устройства исполняется на программируемом микроконтроллере семейства MCS-51 (Atmel – AT89C51).

Микроконтроллер семейства МК-51 (AT89C51) – низкопотребляющий 8-битный КМДП микроконтроллер [3].

Микроконтроллер AT89C51 оснащен 32 программируемыми линиями входа/выхода. Для работы представленного устройства потребуется 28 линий входа/выхода.

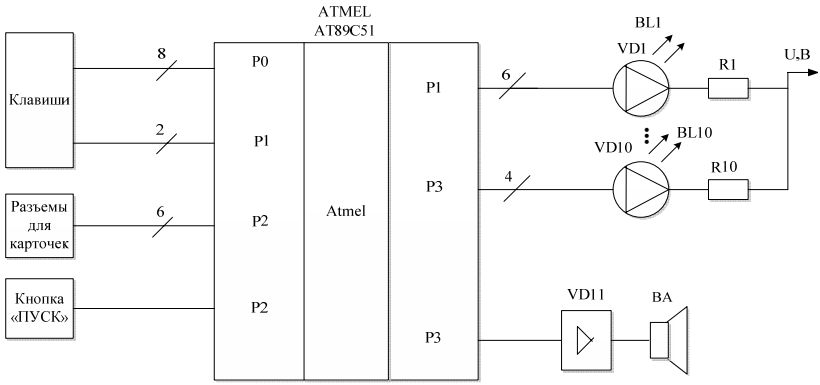


Рис. 2. Функциональная схема устройства

На данном этапе выполнены электрические схемы, разработана конструкция устройства, программное обеспечение, сценарий применения устройства.

ЛИТЕРАТУРА

1. Фестиваль педагогических идей «Открытый урок» // Развитие элементарного логического мышления у детей дошкольного возраста. Электрон. дан. Режим доступа: http://festival. 1september. ru/articles/563483/

2. Дидактор /Дидактика, мультемедийные уроки и педагогическая техника. Электрон. дан. Режим доступа: http://didaktor.ru/texnologiya-konstruirovaniya-interaktivnogo-plakata/

3. Мортон Дж. Микроконтроллеры AVR. Вводный курс.: Пер. с англ. М.: Изд. дом «Додэка – XXI», 2006. 272 с.

АНАЛИЗ КОНСТРУКТИВНЫХ ВОЗМОЖНОСТЕЙ ПЛАТФОРМЕННЫХ СТАПЕЛЕЙ, ПРЕДСТАВЛЕННЫХ НА РОССИЙСКОМ РЫНКЕ

Г.А. Шабалин*, *Б.П. Полонец*, *студенты

Научный руководитель Т.Ю. Лебединская, доцент, к.т.н.

г. Краснодар, ГОУ ВПО «Кубанский государственный технологический университет»

В настоящий период мировая автомобильная промышленность находится на достаточно высоком уровне. Неуклонно растет спрос на личные транспортные средства, что требует от дизайнеров и инженеров новых эстетических и технических решений. Производители автомобилей повышают активную и пассивную безопасность автомобилей. Данные меры привели к увеличению линейных размеров автомобилей и усложнению геометрической формы. В России значительную долю ремонтных работ составляет трудоемкий и долговременный кузовной ремонт разной сложности. Одним из его ключевых составляющих является восстановление геометрической формы, так как отклонения размеров может вызвать увод автомобиля с траектории, некорректную работу узлов и агрегатов. При ремонте кузовов используется большая номенклатура оборудования: от ручного инструмента до автоматизированных стендов для правки кузовов [1]. Широкое распространение получили стапели для кузовного ремонта. Практически все крупные станции технического обслуживания, а также дилерские центры оборудованы стапелями для правки кузовов автомобилей. Принцип работы стапеля заключается в применении многотонного усилия в растягивающем и сжимающем направлениях. Автомобиль при этом фиксируется на раме, и конечный результат работы во многом зависит от надежности крепления [2]. В зависимости от технических особенностей можно выделить несколько видов стапелей: платформенные, напольные, рамные и использующиеся совместно с подъемниками.

Для выполнения наиболее сложных работ используются платформенные стапели. Также они являются наиболее функциональными и способны выполнять работы любой сложности. В основе такого стапеля лежит платформа, к которой при помощи зажимов крепится автомобиль. Геометрию кузова восстанавливают при помощи нескольких силовых стоек, создающих необходимое усилие. На сегодняшний момент на рынке оборудования кузовного ремонта имеются большой выбор платформенных стапелей как зарубежного, так и отечественного производства. Наиболее известные марки, предлагающие стапели: BLACKHAWK, Trommelberg, Celette, Wedge Clamp, Сивер, Профессионал, Мастер, Эксперт, Car-O-Liner.

Многообразие качественного оборудования на внутреннем рынке России требует его изучения и сравнительного анализа с целью выявления преимуществ и недостатков, разработки рекомендаций по выбору и применению. Данный анализ может быть полезен при разработке бизнес-планов и совершенствовании отечественного стапельного оборудования.

Стапели серии Сивер производятся российскими компаниями по американской лицензии. Это рихтовочные стенды, предназначенные для восстановления аварийных кузовов транспортных средств массой до 3000 кг. Привод пневмогидравлический. Стенд имеет классическую американскую конструкцию с большой платформой и силовыми устройствами башенного типа. Просторная широкая платформа 5,2×2,1 м. позволяет закреплять широкую гамму автомобилей от малолитражек до тяжелых вседорожников. У стапелей серии «Сивер» силовое устройство расположено непосредственно на платформе. Платформа имеет округлую форму и рельсовые опоры с внешней и внутренней стороны по которым передвигается силовое устройство, оснащенное роликами. Эта конструкция создает рабочую зону в 360° вокруг автомобиля и позволяет легко перекатывать силовое устройство вдоль периметра платформы, тем самым экономя время и силы, увеличивая производительность и, конечно же, прибыль. Конструкция стапеля имеет ряд преимуществ: платформа имеет округлую форму и рельсовые опоры с внешней и внутренней стороны, по которым передвигается силовое устройство, оснащенное роликами, конструкция исключает трудоемкое позиционирование силовых устройств. Возможна установка стапеля «Сивер D» на подъемник. Стапель «Сивер» серии D позволяет быстро установить и снять любой автомобиль, даже с заблокированными колесами (необходима дополнительная лебедка и тележки под колеса). Устройство имеет ряд модификаций. К недостаткам следует отнести значительную массу (1600 кг), значительные габариты и обязательное подключение к компрессору. Конструкция стапеля типична для зару-

бежных производителей. Данная конструкция одобрена многими известными производителями автомобилей (BMW, Mersedes, Toyota). Используется на многих крупных сервисных центрах. Требует стажировки персонала для выполнения ремонтных работ. Стапель серии «Сивер Е» также соответствует современным требованиям безопасности, что подтверждается сертификатом соответствия РОСС RU.MT20.B 08132. Неоспоримым достоинством стапеля Siver E является наличие пожизненной гарантии на устройства этого класса [3].

Одним из крупнейших российских производителей стапельного оборудования является компания «Сивик». На отечественном рынке представлены стапели серий «Профессионал» и «Мастер». Предназначены для организации комфортных условий работы во время правки кузовов легковых автотранспортных средств любых марок, имеющих отбортовку порогов и весом до 3000 кг. Устройство для правки автомобильных кузовов «Сивик Профессионал» представляет собой раму, оснащенную крепежными элементами, позволяющими надежно зафиксировать кузов автомобиля. Конструкцией предусмотрено наличие подкатного домкрата, трапов, а также одного или нескольких силовых устройств, которые соединены с рамой стенда. Присутствует блок для правки днища автомобиля и комплект спецоснастки. Силовое оборудование может быть установлено с любой стороны и на любой высоте. На рынке предложены три основные категории стапелей «Сивик Профессионал». Масса стапеля не превышает 1200 кг. Вариант с одним силовым устройством является наиболее экономичным. Стапель подходит для восстановления повреждений легкой степени тяжести. Стапель с двумя силовыми устройствами является лидером продаж. Как правило, одно силовое устройство используется непосредственно для вытяжки, а второе поддерживает кузов, исключая риск дополнительной деформации. Оборудование, оснащенное тремя силовыми устройствами, способно восстановить кузов автомобиля даже после сложных аварий, например после бокового удара. Достоинством стапеля серии «Мастер» является модульный принцип, разборная рама и портативность. Масса стапеля 1000 кг [5].

Рассмотрим импортное оборудование, представленное фирмой Korek и AUTOROBOT. Наиболее универсальной является стапельная рама фирмы Korek в комплекте с опорами для фиксации и векторными выпрямителями. Она монтируется в пол, используется для восстановления геометрии цельнокузовных и рамных автомобилей. Пригодно для ремонта всех типов легковых автомобилей и микроавтобусов. Это оборудование компактно, не требует выделения особого места в цеху, на нем можно выполнять любые кузовные работы, в том числе и рихтовочные. Этот тип стапеля особенно удобен для применения в не-

больших цехах. Стапель Korek, в отличие от традиционных стапелей, не имеет ограничений по размерам рамы, грузоподъемности, жесткости и др. Благодаря своей модульной структуре и легкости установки автомобиля, на нем можно выправлять любые удары – от легких вмятин до сильных винтообразных искривлений. Это позволяет быстрее окупить ее и сделать участок прибыльным. Особенности конструкции позволяют одновременно прилагать к автомобилю векторы силы различного направления, что значительно ускоряет ремонт. Однако для качественного проведения работ особенно важна высокая квалификация персонала. Это требует дополнительных затрат на подготовку и стажировку [5].

Autorobot представляет широкий модельный ряд стапелей, предназначенных для мелкого, среднего и сложного ремонта аварийных кузовов автомобилей как для небольших ремонтных автомастерских, так и для крупных автоцентров. Модульная система Autorobot позволяет поэтапно наращивать комплектацию стапеля от самого простого до стапеля более высокого уровня, возможность работы с любыми типами автомобилей, включая MB, BMW, AUDI, а также микроавтобусами и рамными а/м. Измерительные системы – механическая и электронная «ИС» – с точностью измерения ±1 мм имеют собственные базы данных по нижним и верхним контрольным точкам кузовов а/м; возможность модернизации механической «ИС» в электронную. Высокая технологичность производства, оригинальные технические и конструкторские решения, а также возможность поэтапного наращивания комплектации позволяют занимать стабильные позиции на рынке [6].

ЛИТЕРАТУРА

1. Першин В.А. и др. Типаж и техническая эксплуатация оборудования предприятий автосервиса: учеб. пособие. Ростов н/Д: Феникс, 2008. 413 с.

2. Сарбаев В.И., Селиванов С.С., Коноплев В.Н., Демин Ю.Н. Техническое обслуживание и ремонт автомобилей: механизация и экологическая безопасность производственных процессов. Сер. Учебники, учебные пособия. Ростов н/Д: Феникс,2004. 448 с.

3. Стапели – оборудование для кузовного ремонта. Авто-Капитал [Электронный ресурс]. URL: http// www.avk76.ru/catalog (дата обращения: 15.02.2012).

4. Стенды-стапели для кузовного ремонта [Электронный ресурс]. URL: http// www.inmart.ru/stend-stapel-izmerenie-geometrii-kuzova.htm. (дата обращения: 17.02.2012).

5. Автосервисное оборудование для СТО [Электронный ресурс]. URL: http// www.technosouz.ru/Pages/coach_rus.html (дата обращения: 15.02.2012).

6. Оборудование для кузовного ремонта и окраски автомобилей [Электронный ресурс]. URL: http// www. vioton.ru/oborudovanie_dlya_kuzovn. (дата обращения: 16.02.2012).

УСТРОЙСТВО УПРАВЛЕНИЯ ПРОМЫШЛЕННЫМ РОБОТОМ

И.И. Шиляев*, *студент 5-го курса каф. КИБЭВС
Научный руководитель П.Н. Коваленко, *инженер каф. КИБЭВС*, *к.т.н.*
г. Томск, *ТУСУР*, *ФВС*, *virtualist@sibmail.com*

Объектом работы является изучение предмета робототехники. В процессе работы разрабатывалась схема управления двигателями ПЯ-250Ф, проводился анализ принципов управления двигателями постоянного тока с независимым возбуждением, проводился анализ современной элементной базы.

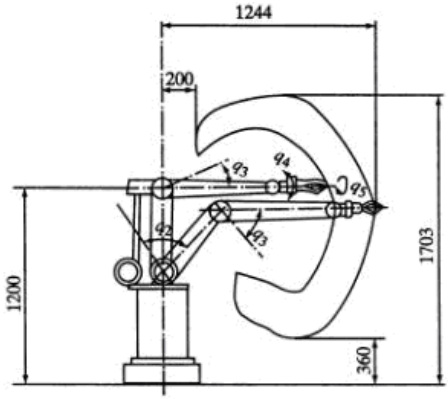


Рис. 1. Размеры звеньев робота ТУР-10: $q_1 = \pm 170°$; $q_2 = \pm 45°$; $q_3 = +25 \div -45°$; $q_4 = \pm 90°$; $q_5 = \pm 180°$

Звенья руки последовательно соединены друг с другом. В качестве приводов звеньев манипулятора используют мотор-редуктор, содержащий двигатель постоянного тока типа ПЯ 250Ф, P = 250 Вт, n = 3000 об/мин, управляемого от ШИП, и волновой редуктор. Передача движения к звеньям осуществляется через кривошипно-шатунные механизмы и цепные передачи [1].

Для управления механическим моментом вала двигателя применяется импульсное управление. Суть его заключается в том, что частоту вращения двигателя регулируют не величиной постоянно подводимого напряжения, а длительностью питания двигателя номинальным напряжением. Схема импульсного управления приведена на рис. 2, *а*. Там же (рис. 2, *б*) показаны графики скорости при различных t.

В период, когда электронный ключ открыт, питающее напряжение полностью подается на двигатель, ток якоря увеличивается, двигатель развивает положительный момент, и частота вращения возрастает; когда электронный ключ закрыт, ток под действием запаса электро-

магнитной энергии продолжает протекать в том же направлении, но через обратный диод. При этом он уменьшается, момент двигателя уменьшается, угловая скорость вращения падает.

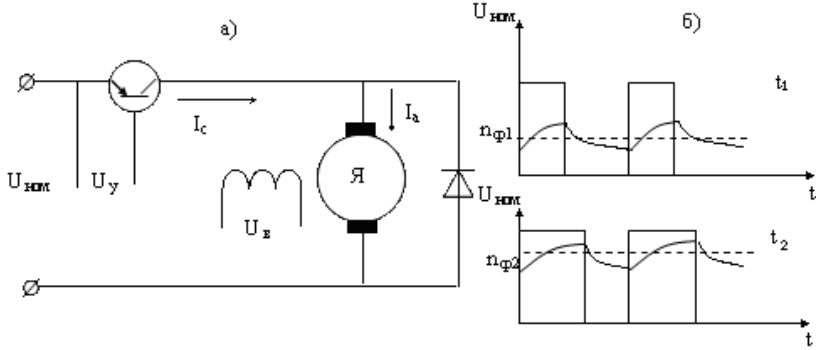


Рис. 2. Схема импульсного управления (*а*), графики скорости вращения (*б*) при разных t ($t_2 > t_1$)

На структурной схеме управления (рис. 3) в общем виде представлен блок управления роботом ТУР-10. Программирование робота ТУР-10 осуществляется с помощью ЭВМ (PC). Через COM-порт подается управляющий сигнал на один из контроллеров (Controller C1), который помимо управления одним из пяти электромоторов принимает показания датчиков и передает управляющие сигналы остальным контроллерам, которые управляют каждый своим мотором (CM2–CM5).

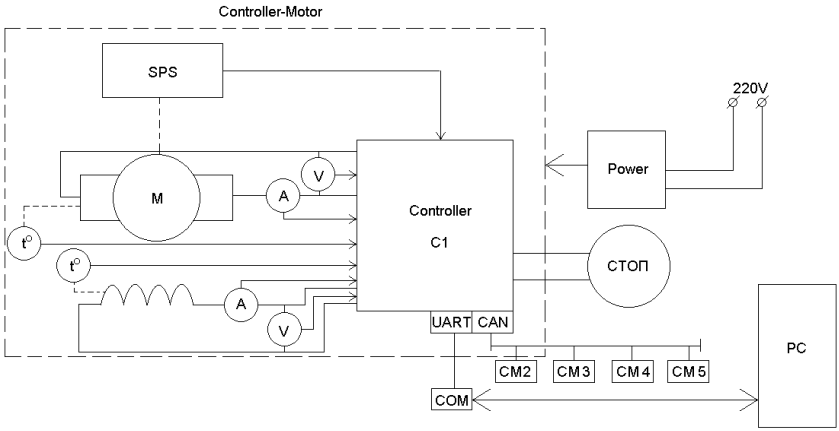


Рис. 3. Структурная схема управления

Помимо датчика скорости и положения (Sensor Position Speed – SPS), в каждой системе СМ (Controller-Motor) установлены по два вольтметра, амперметра и датчика температуры, которые помогут достичь наибольшей точности и подобрать режим работы робота и в случае непредвиденной неполадки в моторе получить оперативные данные [2].

Проект ГПО КИБЭВС-0845 – «Устройство управления промышленным роботом».

ЛИТЕРАТУРА

1. futurman.ru URL: http://futurman.ru/news/2011-03-05-409 (дата обращения: 26.01.2012).

2. Шиляев И.И. Устройство управления промышленным роботом: Отчет по групповому проектному обучению гр. КИБЭВС-0845/ 1 марта 2012 г., Россия, Томск. Томск: Том. гос. ун-т упр. и радиоэлектроники, 2012. С. 17–18.

СОВРЕМЕННЫЕ МЕТОДЫ ПРОЕКТИРОВАНИЯ ЦИФРОВЫХ СХЕМ

Е.В. Шмитько*, *студентка 5-го курса каф. КИБЭВС

Научный руководитель П.Н. Коваленко, *инженер каф. КИБЭВС*, *к.т.н.*

г. Томск, *ТУСУР*, *ФВС*, *577_sev@sibmail.com*

Развитие современной элементной базы тесно связано с развитием методик проектирования сложных цифровых устройств. Разработка современных устройств невозможна без применения систем автоматизированного проектирования (САПР), которые выполняют значительную часть рутинной работы. Однако реализация открывающихся возможностей требует использования новых, современных методов проектирования.

На сегодняшний момент наиболее эффективными считаются методы, использующие текстовые описания проектов вместо традиционных графических редакторов схем. В этом случае проект представляет собой текст, сохраняемый в нескольких файлах. Эти файлы в совокупности определяют общие представления разработчика об устройстве и используются на всех этапах проектирования. К числу этих этапов можно отнести следующие: моделирование устройства, синтез принципиальной схемы. Таким образом, разработчик не конкретизирует структуру схемы, а лишь описывает ее поведение, то есть как она должна работать. Составление же самой электрической схемы возлагается на программу-компилятор.

Тексты описания в большинстве языков проектирования дискретных устройств по составу синтаксических конструкций очень схожи с

традиционными языками программирования. Поэтому часто такое текстовое описание называют программой на языке проектирования или, коротко, HDL-программой.

Языковое описание позволяет описывать устройство на уровне алгоритмов его работы, возлагая при этом синтез самой структуры на систему автоматизированного проектирования (САПР). В этом заключается мощное превосходство языков описания аппаратуры перед графическими редакторами схем, где проектировщик вынужден полностью рисовать структуру устройства с максимальной степенью детализации.

Современная технология проектирования СБИС (сверхбольших интегральных схем) базируется на использовании HDL-языков, прежде всего языка VHDL, получившего наибольшее распространение на территории России. Язык VHDL был разработан в 1983 г. по заказу Министерства обороны США с целью формального описания логических схем для всех этапов разработки электронных систем. Он является стандартным языком с 1987 г. [1]. Аббревиатура VHDL (Very High Speed Integrated Circuit Hardware Description Language) переводится как язык описания высокоскоростных интегрированных схем.

Преимущества, которые делают VHDL привлекательным для рассмотрения большинством проектировщиков:

− имеет широкое распространение в среде разработчиков;

− системы могут быть определены структурными и/или поведенческими способами на различных уровнях;

− синтез языка может производиться множеством инструментальных средств;

− проект, описанный языком VHDL, не ограничивается электроникой.

Сегодня созрела и аппаратная база для применения VHDL. Современные доступные программируемые логические интегральные схемы (ПЛИС) имеют емкость в сотни тысяч эквивалентных логических вентилей, что может быть достаточно даже для реализации микропроцессора. Проектирование схем такой сложности с помощью традиционных схемотехнических редакторов требует больших сроков и чаще всего выполняется коллективами разработчиков. В то же время применение современных средств проектирования, в первую очередь ориентированных на работу с языками описания аппаратуры, позволяет даже отдельным специалистам решать задачи в сжатые сроки [2].

Разрабатываемый на языке VHDL проект устройства вводится, редактируется. Имеются несколько инструментальных средств, доступных для синтеза из VHDL спецификаций системы.

Таким образом, для того чтобы разработать электронную схему, достаточно владеть языком описания аппаратуры (VHDL) и средой проектирования.

ЛИТЕРАТУРА

1. Бибило П.Н. Основы языка VHDL. М.: ЛКИ, 2007. 328 с.
2. Грушвицкий Р.И. Проектирование систем на микросхемах программируемой логики / Р.И. Грушвицкий, А.Х. Мурсаев, Е.П. Угрюмов. СПб.: БХВ-Петербург, 2002. 608 с.

УСТРОЙСТВО СБОРА ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ

М.С. Тарасов*, *кафедра ЭП
Научный руководитель Л.Н. Орликов, проф., д.т.н.
г. Томск, ТУСУР, tarassov.mikhail@gmail.com

В настоящее время проблема измерения сигналов является весьма актуальной и трудоемкой ввиду того, что не всегда имеется возможность использовать специализированные дорогостоящие приборы для измерения однотипных сигналов.

Для решения данной проблемы предлагается использовать аналогово-цифровой преобразователь АЦП последовательного приближения для реализации оцифровки исходного сигнала и его дальнейшей обработки на ЭВМ [1].

Устройство представляет собой комплекс, состоящий из аппаратной и программной части.

Аппаратная часть прибора содержит АЦП (AT Mega8), источник опорного напряжения (REF195GP) фирмы Analog Devises и устройства для согласования логических уровней для дальнейшей передачи оцифрованного сигнала по шине USB (FT232RL) [2].

Основное назначение источника опорного напряжения – создавать образцовое напряжение, которое могло бы быть использовано электронными устройствами преобразования информации в качестве меры, эталона.

АЦП (AT Mega8) – это высокоскоростной 10-разрядный АЦП, который позволяет производить съем данных с частотой до 100 киловыборок в секунду.

Основополагающей характеристикой любого измерительного прибора является его точность, которая определяется по формуле:

$$U_{\min} = \frac{U_{ref}}{2^q}, \qquad (1)$$

где U_{ref} – напряжение питания микроконтроллера, q – разрядность АЦП, $U_{\min}$ – минимально различимое напряжение.

Напряжение питания является очень важной характеристикой, требуемой для правильной работы прибора. Для обеспечения качественных характеристик питания устройства было проведено исследование шумов.

В качестве анализатора шумовых характеристик был использован цифровой осциллограф DS-1150.

В результате исследований и мероприятий по фильтрации напряжения питания [3] были получены следующие результаты.

Скачки напряжения, которые изначально составляли приблизительно 200 мВ, были снижены до приемлемых 9 мВ.

Аппаратную часть устройства можно представить в виде комплекса программного обеспечения для микроконтроллера и программного обеспечения для ЭВМ.

Программа для микроконтроллера реализована на базе языка программирования Си.

Использование достижений в области цифровой техники позволяет создавать измерительные схемы высокой степени точности и быстродействия, а их совмещение с соответствующим программным обеспечением и компьютерными возможностями делает процесс построения переходных характеристик и получения данных об объекте быстрым легким и понятным пользователю.

Измерительно-регистрационное устройство позволяет получать сигнал с датчика, установленного на объекте исследования, преобразовывать его в цифровую форму, передавать по высокоскоростной шине USB в персональный компьютер или ноутбук.

Данные значения в дальнейшем можно использовать в других программных продуктах, например, импортируя их в электронные таблицы Excel.

Разработанное устройство апробировано в комплексе с термопарой для измерения температуры в диапазоне температур до 200 °С. Устройство может применяться в качестве стенда для лабораторного практикума, а также при анализе технологических процессов.

ЛИТЕРАТУРА

1. Евстифеев А.В. Микроконтроллеры AVR семейств Tiny и Mega фирмы ATMEL. 4-е изд., стер. М.: Додэка-XXI, 2007. 103 с

2. Шило В.Л. Популярные цифровые микросхемы: Справочник. 2-е изд., испр. М.: Радио и связь, 1989. 352 с.

3. Хоровиц П., Хилл У. Искусство схемотехники. М.: Мир, 1994. 340 с.

4. Гелль П. Как превратить персональный компьютер в измерительный комплекс: Пер. с фр. 2-е изд. испр. М.: ДМК, 1999.

ЯЗЫК VHDL. СИНТЕЗ ЭЛЕКТРОННЫХ СРЕДСТВ

Е.Е. Усов, студент 5-го курса; П.Н. Коваленко, инженер
г. Томск, ТУСУР, каф. КИБЭВС, ФВС

При проектировании сложных современных устройств используются различные технологии. Описание проектов цифровых систем, реализуемых на кристаллах СБИС (сверхбольших интегральных схем), производится на формальных языках, по конструкции приближенных к привычным языкам программирования. Одним из примеров является язык VHDL (Very high integrate dcircuits Hardware Description Language). Этот язык предназначен для описания поведения цифровых систем и их моделирования на начальных этапах проектирования. С помощью специального программного обеспечения описание на языке VHDL преобразовывается в схему на уровне простейших элементов цифровой электроники. Язык является альтернативой графического представления проекта и обеспечивает компактную запись для проектируемой схемы. Преимуществом использования языка являются:

– сокращение трудоемкости и сроков разработки проекта;

– простота реализации проекта в различных интегральных технологиях;

– наличие множества инструментальных средств для описания проекта;

– получение возможности оценивать варианты реализации проектируемого устройства при различных вариантах проектных ограничений, на различных технологиях;

– высокая надежность проекта.

Главной особенностью языка VHDL является наличие разных стилей описания поведения устройства:

– структурное описание, в котором архитектура представляется в виде иерархии связанных компонентов (вентильный уровень);

– потоковое описание – описание системы, в котором архитектура представляется в виде множества параллельных регистровых операций, каждая из которых управляется вентильными сигналами;

– поведенческое описание – описание систем при помощи некоторых процедур на уровне зависимости выходов от входов. Оно позволяет не конкретизировать структуру схемы, а лишь описывать её поведение.

Все три стиля могут совместно использоваться при проектировании цифровых электронных схем.

Язык VHDL предназначен для решения комплекса задач в ходе проектирования и применения цифровых систем, таких как:

1. Описание структуры системы, разбиение системы на подсистемы, установление связей и взаимодействий подсистем.

2. Описание функционирования системы, в том числе узлов, блоков, реализуемых функций.

3. Моделирование системы и ее работы на основе четкой спецификации структуры системы, а также функционирования ее компонентов.

4. Синтез схемотехнической реализации системы, автоматической генерации детальной структуры на основе строгого описания системы на языке VHDL.

Стоимость ошибки при проектировании СБИС очень высока, особенно на ранних этапах. Поэтому все этапы проектирования – алгоритмический, структурный, логический, технологический – сопровождаются моделированием внешних устройств с помощью так называемого испытательного стенда (testbench). Этот стенд представляет собой VHDL-модель, составными частями которой являются модель тестируемого внешнего устройства (ВУ) и модели генератора тестовых сигналов и логического анализатора, проверяющих правильность функционирования ВУ. Причем на всех этапах может использоваться один и тот же испытательный стенд [1].

ЛИТЕРАТУРА

3. Сергиенко А.В. VHDL для проектирования вычислительных устройств). М.: 2003. 208 с.

КОМПЛЕКСНАЯ СИСТЕМА СИГНАЛИЗАЦИИ И ВИДЕОНАБЛЮДЕНИЯ

***В.А. Воротников*, студент**

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

г. Томск, ТУСУР, каф. КИБЭВС

Обеспечение и поддержание безопасности сотрудников и сохранности имущества предприятия требует от организации установки и введения в эксплуатацию систем, обеспечивающих выполнение данных задач. Поэтому уже долгое время организации оборудуют собственные здания и помещения не только системами охранно-пожарной сигнализации, но и системами охранного видеонаблюдения и контроля доступа. Монтажная организация несет в течение гарантийного срока обязательства в отношении развернутой системы. Далее вопросы по ремонту, обслуживанию, модернизации могут выполняться собственником или по договору со сторонними организациями. В этих условиях документация на систему является необходимой [1, 2].

Действующая на предприятии система сигнализации представлена на рис. 1 и имеет в своем составе:

– кабинетную часть – набор извещателей и приемно-контрольных приборов местного расположения, отвечающих за формирование тревожных сообщений и сигналов управления дополнительным оборудованием;

– промежуточное оборудование – система прокладки кабельных трасс и кроссового оборудования, функциональное назначение которых – с минимальными потерями и искажениями коммутировать служебные сигналы;

– пункт централизованного наблюдения (ПЦН) – комплекс приемно-контрольных приборов и дополнительного оборудования для отображения тревожных сообщений и управления служебными сигналами.

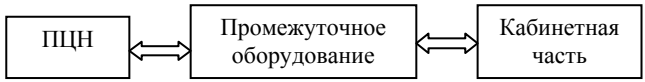


Рис. 1. Структурная схема

Комплексная система сохраняет общую структуру построения. Структурная схема системы сигнализации с использованием нового оборудования и материалов, выполняющая принцип многозадачности и комплексного использования, приведена на рис. 2.

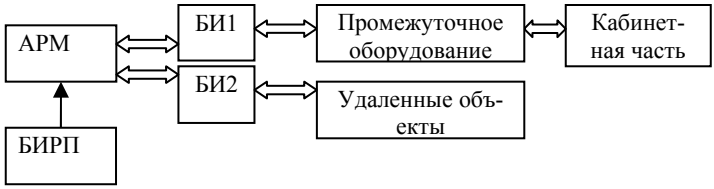


Рис. 2. Структурная схема комплексной системы

Согласно этой схеме роль ПЦН выполняет автоматизированное рабочее место (АРМ) – персональный компьютер с необходимым набором функциональных узлов и соответствующего программного обеспечения, необходимых для обработки, хранения и отображения набора служебной информации, обеспечивающих резервирование и/или дублирование функций.

Блок источника резервного питания (БИРП) – выполняет функцию защиты от бросков питания и поддержания работоспособности систе-мы при его отключении.

Блок интерфейсов (БИ1) – обеспечивает сбор и обработку сигналов извещений и технологической информации от кабинетных (этажных) приборов.

Блок интерфейсов (БИ2) – обеспечивает прием потока данных с удаленных объектов посредством проанализированных средств доставки, а именно GSM, Internet, ТФоП.

Монтаж маршрутных и транзитных кабельных линий современными материалами дает возможность резервирования и дальнейшего расширения.

Так, использование других типов приборов позволит увеличить адресность и степень детализации выдаваемых тревожных сообщений. Монтаж структурированной кабельной системы позволит увеличить выживаемость системы и даст возможность интеграции в комплекс дополнительных систем. Использование в ПЦН автоматизированной рабочей станции с новым приемно-контрольным оборудованием повысит тактико-технические показатели всей системы в целом.

Ввод предложенной системы позволит:

– увеличить степень наглядного (визуального) отображения поступающей информации для следящего персонала;

– повысить зону обхвата видеоприсутствия на территории до 100%; подключать к ней поток данных от объектов-выносов;

– охватить сетью охранной сигнализации любой сложности все помещения территориального комплекса зданий; подключать к ней поток данных от особой режимности объектов-выносов для дублирования поступающих сообщений и объектов без постоянного персонала;

– в случае необходимости интегрировать в систему прокладки других комплексов – компьютерной сети предприятия, системы доступа и управления персоналом, телефонной связи, проводного телевидения и громкоговорящей связи.

ЛИТЕРАТУРА

1. РД 78.145–93. Руководящий документ. Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ.

2. ВСН 60–89. Ведомственные строительные нормы. Устройства связи, сигнализации и диспетчеризации инженерного оборудования жилых и общественных зданий. Нормы проектирования.

СИСТЕМА ПЕРЕДАЧИ ДАННЫХ ПО ЭЛЕКТРОСЕТИ ДЛЯ ЭЛЕКТРОПРИВОДОВ

К.М. Жернаков*, *студент 5-го курса каф. КИБЭВС

г. Томск, *ТУСУР*, *ФВС*, *kzhernakov@sibmail.com*

При транспортировке жидких или газообразных веществ по трубопроводу на дальние расстояния возникает проблема удаленного контроля и управления электроприводами, осуществляющими запорную,

запорно-регулирующую или регулирующую функции. Это проблема может быть решена посредством прокладки сигнальных линий, так как собственный блок управления электроприводом имеет внешний интерфейс. Но ввиду большой протяженности данное решение оказывается трудоемким и требует существенных затрат денежных средств. Другим вариантом является передача данных по электросети. Это позволит избежать затрат на прокладку отдельных линий связи и использовать имеющиеся силовые линии, наличие которых в любом случае необходимо для питания электроприводов.

Телекоммуникационная технология, базирующаяся на использовании силовых электросетей для информационного обмена, называется Power Line Communication (PLC). Основой технологии PLC является использование частотного разделения сигнала, при котором высокоскоростной поток данных разбирается на несколько относительно низкоскоростных потоков, каждый из которых передается на отдельной поднесущей частоте с последующим их объединением в один сигнал [1].

Передача диспетчерской информации по проводам линий электропередач широко применяется как один из видов связи. Но на сегодняшний момент нет сведений о применении такой системы для управления электроприводами трубопроводной арматуры. При использовании технологии PLC в этой сфере можно столкнуться с рядом проблем, одной из которых являются помехи, создаваемые самими электроприводами. Решением этой задачи является использование более сложных способов модуляции сигналов, а также различных методов сохранения целостности данных.

Одним из более сложных способов модуляции сигнала является OFDM-модуляция (Orthogonal frequency-division multiplexing – мультиплексирование с ортогональным частотным разделением каналов), которая использует большое количество близко расположенных ортогональных поднесущих. Это позволяет сохранить общую скорость и точность передачи данных [2].

При использовании данной технологии электропривод оснащается фильтром для выделения нужных поднесущих частот, платой премапередачи данных и ретранслятором для усиления сигнала.

Данный вид передачи информации является экономически эффективным для любого вида промышленности, в том числе и для трубопроводов, оснащенных электроприводами с системой управления.

ЛИТЕРАТУРА

1. Никифоров А.В. Технология PLC-телекоммуникации по сетям электропитания // Сети и системы связи. 2002. № 5.

2. Лебедев В.С. Модуляция OFDM в радиосвязи // Радиолюбитель. 2008. № 9. С. 36–40.

АВТОМАТИЗАЦИЯ РАСПРЕДЕЛЕННОГО ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА НА ПРИМЕРЕ АВТОМАТИЗАЦИИ РАБОТЫ ТАКСОПАРКА

И.Н. Шишкин, студент 5-го курса
Научный руководитель М.И. Мельников, аспирант
г. Томск, ТУСУР, каф. КИБЭВС, sin@keva.tusur.ru

В настоящие время автоматизация технологических процессов находит всё большее распространение в сфере общественного транспорта. Существует большое количество систем мониторинга автобусных парков, грузоперевозок.

В нашем городе существует большое количество фирм такси. Однако, уровень автоматизации работы диспетчера, водителей и управляющего персонала остаётся на низком уровне. Большинство фирм такси до сих пор используют устное распределение заказов по радио. Всё это значительно замедляет процесс оказания услуг по перевозкам, снижается эффективность работы персонала, увеличиваются расходы фирмы такси.

В качестве объекта автоматизации выступает процесс распределения заказов для множества автомобилей такси. Распределение заказов должно производиться исходя из географической близости и состояния персонала.

Структурная схема программно-аппаратного комплекса для автоматизации работы таксопарка приведена на рис. 1.

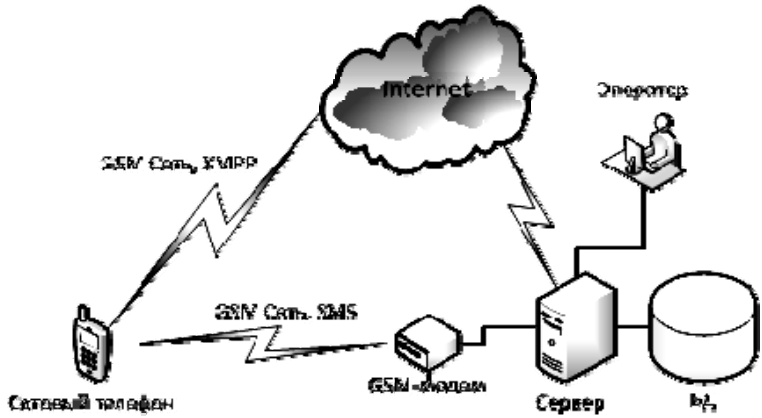


Рис. 1. Структурная схема комплекса

В качестве основного канала передачи данных был выбран GPRS, из-за простоты использования, большей скорости передачи и меньших

накладных расходов. SMS используется в качестве резервного канала. Два канала передачи были выбраны для увеличения надёжности системы.

Главным элементом системы является сервер, с установленным на нём программным обеспечением. Функции ПО:

1) графическое представление информации, в удобном для оператора виде;
2) работа с БД;
3) приём и отправка сообщений с помощью внешнего GSM-модема;
4) приём и отправка сообщений по протоколу XMPP.

Функции БД:

1) хранение информации о персонале;
2) хранение текущего положения персонала;
3) хранение текущих заказов;
4) хранение отчётности;
5) хранение географической информации;
6) хранение информации о сотовых вышках.

На мобильном устройстве должно быть установлено специальное ПО для взаимодействия с серверной частью системы. Функции ПО:

1) графическое представление информации, в удобном для оператора виде;
2) взаимодействие по определённому протоколу с серверной частью, независимо от канала связи;
3) приём и отправка SMS сообщений;
4) приём и отправка сообщений по протоколу XMPP;
5) определение местоположения.

Функциональная схема комплекса представлена на рисунке 2.

Вначале заказ от клиента поступает оператору. С помощью графического интерфейса серверного ПО производиться оформление заказа.

При оформлении заказов производиться поиск в базе данных адресов или организаций. После чего выбирается несколько ближайших к месту заказа свободных таксистов, и производится рассылка сообщений по одному из каналов связи. В случае если в БД нет такого адреса или организации, запрос отправляется в общий эфир.

Заступая на смену, водители запускают мобильное приложение. При запуске мобильного приложения персоналу необходимо авторизоваться в системе (ввести логин и пароль). После чего можно устанавливать свой текущий статус «Занят», «Свободен», «На Обеде».

Рис. 2. Функциональная схема комплекса

Когда сообщение о заказе приходит на мобильное устройство, программа отображает его в удобном для восприятия виде. После чего таксист может отклонить или принять заказ. Автоматически состояние меняется на «Занят».

Кроме того мобильное приложение получает информацию о текущем положении из GPS\Глонасс модуля или из сотовой сети[1]. После получения данных о местоположении, приложение отправляет их на сервер. На сервере данные о метаположении заносятся в БД и визуализируются с помощью объектов на карте.

Внедрение такой системы позволит увеличить уровень качества услуг в фирмах такси, уменьшит время распределения заказов. Уменьшит время простоя такси, а также его пробег без пассажиров.

Эта система избавляет диспетчеров от рутинной работы и предоставляет управляющему персоналу различные инструменты для отслеживания работы персонала.

ЛИТЕРАТУРА

1. Шишкин И.Н., Леонов А.Е., Жернаков К.М. Система слежения за персоналом для АСУ на базе gsm сетей // Сб. тр. VIII Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых «Технологии Microsoft в теории и практике программирования». Томск: изд-во НИ ТПУ, 2011. С. 153–155.

СЕКЦИЯ 18

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель – **Шелупанов А.А.**, проректор по НР ТУСУРа, зав. каф. КИБЭВС, профессор, д.т.н.,*
*зам. председателя – **Мещеряков Р.В.**, зам. начальника НУ, зам. зав. каф. КИБЭВС по НР, доцент, к.т.н.*

ПЕРИОДИЧЕСКИЕ АТ-ГРУППЫ НАД АБЕЛЕВЫМИ И НЕАБЕЛЕВЫМИ ГРУППАМИ В ВОПРОСАХ ЗАЩИТЫ ИНФОРМАЦИИ

М.В. Алчебаева, ст. преподаватель ЧГАА;
А.В. Рожков проф. ЮУрГУ
г. Челябинск, ЮУрГУ, ros@wtpro.ru, great.ros.marine@gmail.com

Речь идет о важном подклассе групп автоморфизмов однородных деревьев (АТ-группах), а именно об АТ-группах над последовательностью элементарных абелевых групп и групп перестановок конечных множеств. АТ-группы как объекты, обобщающие примеры бернсайдовых групп, обладают многими экстремальными свойствами. Например, существуют АТ-группы, порожденные двумя элементами, в которых все элементы имеют конечный порядок, причем для любого натурального числа n в них есть элемент порядка n, т.е. их спектр совпадает со всем натуральным рядом. Существуют АТ-группы с очень медленным ростом периодов и с промежуточным ростом числа элементов группы данной длины и т.д.

Конструкция АТ-групп оказалась очень продуктивной. Не только потому, что обобщила многие конструктивные примеры бернсайдовых групп (кроме групп, сходных с конструкцией Е.С. Голода), но и позволила передоказать многие теоремы о периодических группах, которые ранее были доказаны только при помощи конструкции Е.С. Голода.

Также в рамках развития теории АТ-групп удалось решить около полутора десятка известных проблем алгебры, в том числе несколько проблем из «Коуровской тетради».

АТ-группы в силу своей конструкции как групп автоморфизмов однородных деревьев, например бинарных, оказались полезными в теоретической кибернетике. Не случайно пионерская работа в этой области принадлежит профессору кафедры интеллектуальных систем

мехмата МГУ С.В. Алешину. В его честь группы названы АТ-группами (группами алешинского типа).

Периодические АТ-группы над группами перестановок очень трудно поддаются изучению. Но они интересны тем, что позволяют моделировать информационные процессы, в частности процессы взаимодействия противоборствующих сторон. Причина в том, что преобразования информации, самого общего вида, не ведущие к потерям данных, – это, часто, просто перестановки элементов некоторого множества, например состояний объектов взаимодействия или действий, производимыми этими объектами. Многие протоколы хорошо моделируются конечными автоматами, что подтверждает естественность использования АТ-групп в решении подобных задач, поскольку АТ-группы, построенные над конечными множествами фиксированной мощности, могут быть заданы как группы преобразований, определяемых конечными автоматами.

АТ-группы над последовательностью элементарных абелевых групп, например над группой Z_2, полезны в вопросах построения кодов, исправляющих ошибки. По линейному коду, исправляющему ошибки, строится регулярная АТ-группа, т.е. АТ-группа, действующая на слоях дерева сдвигами на элементы групп, которые и образуют данные слои, и исследуются ее алгебраические свойства.

В свою очередь, выявляется связь между количеством ошибок, исправляемых кодом, и алгебраическими характеристиками АТ-группы, например ростом ее периодов. По любому линейному коду над конечным полем мы можем построить регулярную АТ-группу с одним продольным порождающим. Каким образом свойства кода сказываются на алгебраических свойствах этой АТ-группы и можно ли по свойствам АТ-группы выяснить свойства кода? Это совершенно новая постановка вопроса, возможно, не бесполезная и для теории АТ-групп и для теории линейных кодов. Во всяком случае диаметр пространства кодов с метрикой Хэмминга и рост периодов АТ-групп тесно связаны.

В работе построено несколько классов примеров АТ-групп над последовательностями абелевых групп и групп подстановок. Доказана периодичность построенных групп. АТ-группами сгенерированы коды, исправляющие ошибки. АТ-группами над группами перестановок порождаются конечные автоматы, моделирующие протокол взаимодействия двух субъектов. Параметры протокола интерпретируются в терминах конечных автоматов и АТ-групп.

ЛИТЕРАТУРА

1. Рожков А.В. Об условиях конечности, ослабляющих локальную конечность // Доклады РАН. 1998. Т. 362, № 4. С. 445–448.

2. Рожков А.В. Centralizer-graph finiteness conditions in the class of AT-groups // Acta Applicandae Mathematicae. 2005. Vol. 85, № 1–3. P. 265–275.

3. Рожков А.В. Периодические АТХ-группы над группой подстановок // Объединенный научный журнал. М.: Тезариус, 2003. № 8 (66). С. 80–86.

4. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: учеб. пособие. 3-е. изд. М.: Гелиос-АРВ, 2005. 480 с.

5. Рожков А.В., Ниссельбаум О.В. Теоретико-числовые методы в криптографии: учеб. пособие. Тюмень: ТюмГУ, 2007, 160 с.

МОДЕЛИРОВАНИЕ СЕТИ ДЛЯ ИЗУЧЕНИЯ СПОСОБОВ КОМБИНИРОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И СИСТЕМ HONEYPOT

Ю.В. Алейнов*, *аспирант каф. БИС

г. Самара, *СамГУ*, *yual@samsu.ru*

Обнаружение атак на компьютерные системы – сравнительно новое направление исследований в компьютерной науке. Считается, что начало этому направлению положил Джеймс Андерсон своей статьёй «Мониторинг угроз компьютерной безопасности», вышедшей в 1980 г. [1]. Данное направление отличается высокой динамичностью. Это связано с тем, что проблема противодействия атакам на компьютерные системы остаётся нерешённой вплоть до настоящего времени.

В то же время широкое распространение компьютерных сетей приводит к увеличению рынка программного обеспечения с функциями работы по сети, что приводит к увеличению количества потенциальных жертв сетевой атаки. Регистрируемое ежегодно число сетевых атак на всевозможные компьютерные системы только растёт [2].

На данный момент существует несколько различных подходов к построению систем обнаружения вторжений (СОВ) и большое количество их реализаций [3]. Однако всем типам СОВ свойственны следующие основные недостатки:

− высокий процент ложных срабатываний;

− ненулевая вероятность пропуска атаки;

− сложность обнаружения новых типов атак;

− обычно высокие требования к производительности аппаратной платформы.

Данные недостатки связаны с тем, что СОВ должна обрабатывать все события защищаемой системы. В случае с сетевой СОВ она должна анализировать весь трафик в сети. Одним из возможных решений большинства указанных проблем является применение так называемых систем Honeypot.

Основной идеей систем Honeypot является то, что они, в отличие от других средств защиты, предназначены для того, чтобы подвергнуться сканированию и атаке. Такая система не выполняет производственных функций, а выполняет роль своеобразной ловушки для атакующего. Поскольку практически любая сетевая активность такой системы не является легитимной, а общий объём анализируемых данных сравнительно невелик, все перечисленные недостатки СОВ не характерны для систем Honeypot. В связи с этим выглядит оправданным использование Honeypot для целей обнаружения атак (например, в качестве сенсора СОВ). Однако системам Honeypot свойственны свои недостатки, в числе которых – отсутствие какой-либо общепринятой методики конфигурирования ловушек. Для каждой конкретной сети должна быть построена своя конфигурация Honeypot. При этом при изменении параметров сети конфигурация ловушек также должна изменяться [4].

Таким образом, необходимо построить модель взаимодействия СОВ и Honeypot, которая позволила бы дать ответ на вопрос об оптимальной конфигурации системы ловушек для достижения максимальной эффективности при обнаружении атак.

Для построения такой модели необходимо сначала построить адекватную модель подвергающейся атакам сети. Такая модель должна отвечать следующим критериям:

− модель должна быть применима к любой сети с любыми средствами защиты и с любым набором сервисов;

− моделью должна предусматриваться некоторая мера защищённости сети для определения оптимальности конфигурации применяемых мер защиты.

В основе модели предлагается положить следующие основные принципы:

− сетевая атака направлена на эксплуатацию уязвимостей приложений;

− вероятность компрометации приложения зависит только от него и не является фиксированной величиной;

− компрометация приложения с некоторой вероятностью влечёт компрометацию других связанных с ним приложений сети;

− компрометация приложения уменьшает общий показатель защищённости сети.

Математически модель может выглядеть как неориентированный граф, узлы которого представляют приложения и связаны друг с другом рёбрами различных типов. Связь двух вершин такого графа ребром соответствует возможности напрямую произвести атаку на одно приложение при условии успешной компрометации другого, так как

два приложения в сети могут быть связаны между собой различными способами:

− разделение вычислительных ресурсов;

− наличие связи между хостами на сетевом уровне и использование одного и того же протокола прикладного уровня.

Вследствие этого граф будет содержать рёбра разных типов, для которых стоимость будет рассчитываться по-разному.

Среди направлений дальнейшего исследования можно выделить следующие:

− разработка способа определения параметра защищённости приложения;

− введение параметра защищённости сети в целом;

− определение способа формального описания системы Honeypot в рамках предложенной модели;

− поиск оптимальной конфигурации Honeypot.

ЛИТЕРАТУРА

1. Лукацкий А.В. Обнаружение атак. СПб.: БХВ-Петербург, 2001. 624 с.

2. Статистика CERT (Computer Emergency Response Team, Центр реагирования на компьютерные инциденты) http://www.cert.org/stats/cert_stats.html

3. Allen J., Christie A., Fithen W. et all. State of Practice of intrusion detection technologies // Technical Report CMU/SEI-99-TR-028. Carnegie Mellon Software Engineering Institute, 2000.

4. Lance Spitzner. Dynamic Honeypots. http://www.securityfocus.com/infocus/1731.

ШАБЛОНЫ СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ

М.А. Ананев, Е.В. Цыбань, С.В. Штыгайло, А.Ю. Якимук, студенты 3-го курса;

М.А. Сопов, ст. преподаватель

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

Сертификат открытого ключа электронной подписи используется для проверки соответствия открытого ключа подписи и информации, которая идентифицирует владельца ключа. Сегодня общепринятым стандартом формата сертификата открытого ключа является X509 версии 3. Использование формата сертификата версии 3 обеспечивает определённую политику безопасности в системе за счёт нововведения под названием «Дополнения».

В таблице приведены отличительные особенности формата сертификатов всех версий.

Сравнительная таблица форматов сертификатов

	Версия 1	Версия 2	Версия 3
Номер версии	+	+	+
Серийный номер	+	+	+
Идентификатор алгоритма подписи	+	+	+
Имя издателя	+	+	+
Период действия (не ранее/позднее)	+	+	+
Имя субъекта	+	+	+
Информация об открытом ключе субъекта	+	+	+
Подпись	+	+	+
Уникальный идентификатор издателя	–	+	+
Уникальный идентификатор субъекта	–	+	+
Дополнения	–	–	+

Рассмотрим поле «Дополнения» подробней.

Поле «keyUsage» имеет несколько параметров, которые дают возможности для:

– digitalSignature – формирования и проверки электронно-цифровой подписи (ЭЦП);

– nonRepudiation – неотказуемости;

– keyEncipherment – шифрования других ключей;

– dataEnciphermen – функции шифрования и расшифрования данных и контроль целостности с использованием имитозащиты;

– keyAgreement – формирования других ключей различными алгоритмами;

– KeyCertSign – формирования ЭЦП сертификатов;

– CRLSign – формирования ЭЦП списка аннулированных сертификатов (САС);

– EncipherOnly/ DecipherOnly – только для функции зашифрования/расшифрования.

Другие поля:

– extendedKeyUsage – задает одно или несколько назначений ключа помимо или вместо дополнения keyUsage. Например: serverAuth, clientAuth;

– cRLDistributionPoint – URL для хранения списка отозванных сертификатов;

– privateKeyUsagePeriod – период действия секретного ключа, соответствующего открытому ключу;

– certificatePolicies – уникальный номер OID;

– BasicConstraints – указывает, действует или нет субъект как удостоверяющий центр (УЦ), задает длину пути сертификации;

– PolicyConstraints – используется только в сертификатах УЦ, задает проверку пути к политике, запрашивая идентификаторы политик и (или) запрещая задание соответствий политик;

– NameConstraints – используется только в сертификатах УЦ, задает ограничения на имена, которые могут использоваться в качестве имен для любого следующего сертификата на пути сертификации;

– другие, такие как: альтернативные имена субъекта (DNS, IP, EDI-имя, e-mail, ID, произвольное имя), альтернативное имя издателя, необязательные атрибуты каталога субъекта (e-mail, телефон, адрес и т.д.) [1].

В качестве примера приводится корневой сертификат «Удостоверяющего центра Сибири» версии 3. Обратим внимание на поля «Издатель» и «Субъект», которые являются одинаковыми, что и отображено на рис. 1.

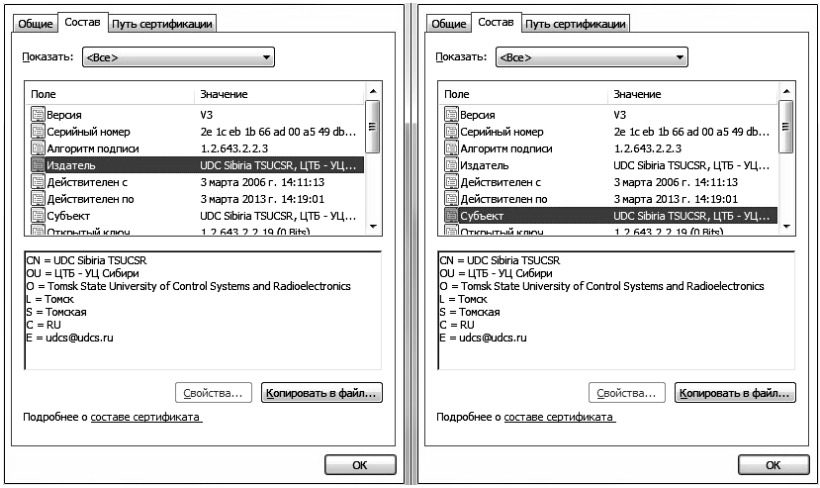


Рис. 1. Параметры сертификата Удостоверяющего центра Сибири

CN (Common Name) – имя сертификата. При создании серверных сертификатов используется доменное имя сайта, для клиентских сертификатов может быть использовано что угодно. Обязательный параметр. Максимальная длина 64 символа.

OU – (Organization Unit). Название отдела. Необязательный параметр.

O – (Organization Name). Название организации. Необязательный параметр.

L – (Locality Name). Название города/посёлка... Необязательный параметр.

S – (State Name). Название региона/области/края/республики/... Необязательный параметр.

C – (Country). Двухсимвольный код страны. Необязательный параметр.

E – (E-mail address). Почтовый адрес. Необязательный параметр. Максимальная длина 40 символов [2].

Проект ГПО КИБЭВС-1103 – «Инженерия баз данных».

ЛИТЕРАТУРА

1. Интернет-университет.
http://www.intuit.ru/department/security/pki/6/pki_6.html

2. Информационный ресурс: OpenNET.
http://www.opennet.ru/base/sec/ssl_cert.txt.html

ПРОЕКТИРОВАНИЕ ПРОГРАММЫ БЕЗОПАСНОГО ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА УСТРОЙСТВАХ ПОД УПРАВЛЕНИЕМ ANDROID

Р.А. Воронкин*, *доцент каф. защиты информации;
В.Ю. Бабкин*, *студент
г. Ставрополь, *ФГБОУ ВПО «Северо-Кавказский государственный технический университет»*, *zik@ncstu.ru*

Устройства под управлением операционной системы (ОС) Android получили большое распространение в последнее время. К таким устройствам можно отнести ноутбуки, планшеты, КПК, электронные книги, смартфоны (коммуникаторы). Сфера их применения давно не ограничивается только набором номера или набиранием коротких сообщений. Современные портативные устройства имеют память для хранения данных, измеряемую в гигабайтах, удаленное администрирование, поддержку VPN, Flash и JavaScript, синхронизацию почты, заметок, обмен файлами и т.д. Подавляющее число пользователей хранит на своих устройствах конфиденциальную информацию, как личную, так и служебную. Но она никак не защищена и при утере устройства, что является основной угрозой конфиденциальной информации на мобильных устройствах, возможен беспрепятственный доступ злоумышленника к защищаемой информации.

Отсюда возникает проблема безопасного хранения такой информации. Для решения данной задачи была разработана программа для

хранения конфиденциальной информации в памяти устройства в виде, затрудняющем извлечение информации.

Основные особенности программы:

– возможность ввода информации различного вида (графическая, текстовая, бинарные данные);

– журнал событий. Предназначен для фиксации действий пользователя и выявления несанкционированных действий с хранилищем;

– контроль целостности БД с внесением результатов проверки в журнал событий;

– резервное копирование и восстановление. Возможно два способа: сохранение копии БД в локальной памяти устройства, либо синхронизация с облачным хранилищем;

– хранение информации в виде, затрудняющем извлечение полезной информации;

– простой и эффективный способ аутентификации, основанный на мастер-пароле. Имеется контроль сложности создаваемого мастер-пароля;

– исполняемый файл программы обфусцирован для противодействия анализу и модификации программы при декомпиляции.

Рассмотрим процесс входа в систему и внесения информации для хранения. Данный процесс изображен на рис. 1.

Прежде всего, осуществляется проверка целостности базы данных. В случае отрицательного результата выдается соответствующее сообщение пользователю и информация о проверке заносится в журнал событий. В случае успешной проверки у пользователя запрашивается мастер-пароль, после чего происходит его проверка. Если введённый пароль неверный, то пользователю дается еще несколько попыток на ввод. В случае правильности пароля на его основе вырабатывается ключ преобразования информации в читаемый вид и происходит преобразование информации, хранимой в базе данных.

После этого пользователь осуществляет ввод новой информации, которая преобразуется в трудно воспроизводимый вид и сохраняется в базе данных. Далее происходит отправка базы данных с преобразованной информацией в облачное хранилище.

Таким образом, использование данной программы позволяет предотвратить утечку конфиденциальной информации, хранимой на мобильных устройствах под управлением ОС Android. И если злоумышленник получит доступ к защищаемой информации, то приведение ее в человеко-читаемый вид займет достаточное время для потери актуальности атакуемой информации.

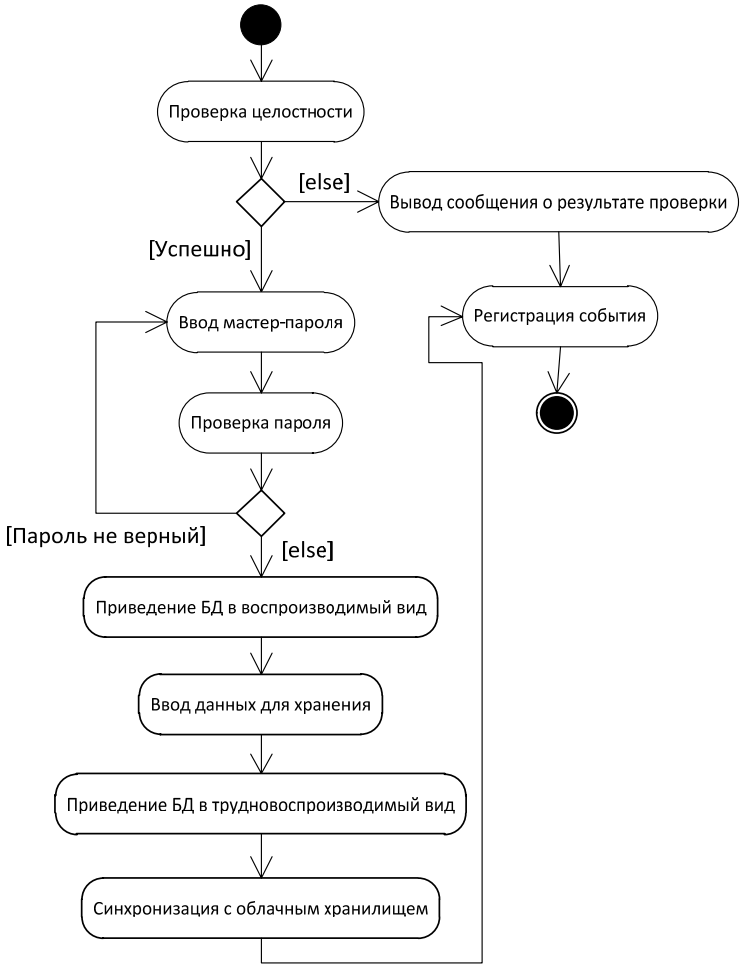


Рис. 1. Диаграмма деятельности операции входа
внесения конфиденциальной информации

ЛИТЕРАТУРА

1. Коматинени С., Маклин Д., Хашими С. Android 3 для профессионалов. Создание приложений для планшетных компьютеров и смартфонов = Pro Android 3. М.: Вильямс, 2011. 1024 с.

2. Голощапов А. Google Android: программирование для мобильных устройств. СПб.: БХВ-Петербург, 2010. 448 с.

3. Android developers [Электронный ресурс]. Режим доступа: http://developer.android.com/guide/index.html, свободный. Загл. с экрана. Яз. англ.

СИСТЕМАТИЗАЦИЯ ПАРАМЕТРОВ СИСТЕМНЫХ СОБЫТИЙ С ЦЕЛЬЮ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Е. Баринов, студент 5-го курса каф. БИС
г. Челябинск, ЮУрГУ, ПС, barinov_ae@bk.ru

В сложных корпоративных системах операционный процесс управления информационной безопасностью нуждается в автоматизации и использовании специализированных инструментов, которые повышают его эффективность и предоставляют широкий спектр функций и услуг для специалистов, отвечающих за обеспечение информационной безопасности предприятия. Инструменты такого типа предоставляет технология SIEM.

Данная технология обеспечивает анализ в режиме реального времени предупреждений безопасности, сгенерированных сетевыми аппаратными средствами, операционными системами и приложениями, с целью автоматизации обнаружения аномалий подсистем ИБ и их устранения.

Решения SIEM представляют собой программное обеспечение, устройства или управляемые службы.

В разрезе топологии SIEM решения представляют собой серверную часть, обрабатывающую базу данных событий, поступающих от клиентской части (сенсоров). Также на уровне серверной части реализуется искусственный интеллект, отвечающий за автоматическое принятие решений. Сенсоры соответственно не только обеспечивают сбор информации, но также и имеют под собой некую подсистему исполнения команд, полученных от серверной части.

Одной из основных проблем SIEM-решений на текущий момент является отсутствие стандартов интеграции средств обеспечения ИБ с конкретным SIEM-решением. В настоящее время стандартизировано 2 протокола: устаревший протокол syslog и находящийся в разработке и потому малопопулярный протокол CEE.

Для обнаружения аномальных событий SIEM-решение последовательно производит следующие этапы обработки событий: отбор, систематизация, обнаружение аномалий. Систематизация – обработка информации с целью приведения ее к определенному виду и её интерпретация, позволяющая в дальнейшем информационной системе определенным образом отреагировать на полученную информацию. Систематизация состоит из подэтапов: выделения аномальных событий и корреляции событий. Критерием аномального события является обнаружение не характерных для него или системы в целом одного или нескольких параметров. В различных операционных системах сама

сущность события представима по-разному. Например, в Unix-подобных системах это просто строка текста, записанная в файл системного журнала. В операционных системах семейства Microsoft Windows событие – это любое значительное происшествие в операционной системе или приложении, о котором следует сообщить пользователю. Каждое хранимое событие представляет собой совокупность атрибутов, которых может быть до 19. Журналом событий является совокупность схем, предназначенных для записи и создания запросов к произошедшим в системе событиям.

С точки зрения дальнейшей обработки событий в операционных системах Microsoft Windows подсистема обладает большей гибкостью за счёт некоторых атрибутов, позволяющих, в том числе в момент возникновения события в системе, устанавливать его связь с другими событиями. То есть происходит корреляция событий в виде «цепочек» и бинарных деревьев, что позволяет анализировать не каждое событие в отдельности, а структуры событий целиком, что существенно повышает производительность.

В работе проведён подробный анализ подсистем управления событиями в Unix- и Windows-системах, предложены алгоритмы оптимизации выборки событий при централизованном мониторинге, в том числе осуществляемых на локальных устройствах. В итоге работы было достигнуто уменьшение объёма централизованно собираемых событий на 25%, вследствие чего выросли производительность системы и скорость реакции на возникающие аномалии. Были вынесены многочисленные рекомендации разработчикам прикладного и системного ПО и разработчикам средств защиты информации. В настоящее время создаются средства, приводящие системные журналы Unix-подобных систем в атрибутивное представление.

ЛИТЕРАТУРА

1. Виханский О.С., Наумов А.И. Обмен информацией начинается с формулирования идеи или отбора информации. Менеджмент: учебник. 3-е изд. М.: Гардарики, 1999. 528 с.

ТРЕБОВАНИЯ ПО ПЕРСОНАЛЬНЫМ ДАННЫМ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Г.А. Бут*, *студент 5-го курса каф. КИБЭВС
г. Томск, *ТУСУР*, *ФВС*, *ilovethisgame@sibmail.com*

Одной из задач, поставленных на преддипломной практике, являлось задание, в котором необходимо было изучить базу нормативно-правовых документов на наличие требований по персональным дан-

ным, с учетом специфики для ИС компании. Главная цель исследования заключалась в том, чтобы посредством ссылки на существующие (действующие) нормативно-правовые акты показать защищенность ИС компании с правовой точки зрения.

На основании указа Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» можно сказать, что информация, обрабатываемая в изучаемой ИС, в частности сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами, в данном случае – врачебная тайна, является информацией конфиденциального характера.

Что же есть врачебная тайна? Согласно Основам законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 г. № 5487-1, врачебной тайной считается информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении.

Так как БД ИС компании производит получение, хранение, обработку (передачу) информации о пациентах в частности, то на основании этого факта можно утверждать, что в данной ИС производится обработка персональных данных.

На основании Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). На основании ст. 8 Закона «О персональных данных» персональными данными считают следующую информацию – фамилия, имя, отчество, адрес, абонентский номер, год, месяц, дата и место рождения, семейное, социальное, имущественное положение, образование, профессия, доходы, сведения о профессии и иные персональные данные.

Так как врачебная тайна входит в перечень конфиденциальной информации, то необходимо реализовать в системе режим конфиденциальности информации.

Согласно Федеральному закону «О персональных данных» под конфиденциальностью информации понимают обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В соответствии с Федеральным законом «О персональных данных» под информационной системой персональных данных понимается информационная система, представляющая собой совокупность

персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных. Рассматриваемая ИС является ИСПДн.

Остается еще один вопрос: может ли быть оператором персональных данных программа ПО, т.е. ИС? Среди изученных нормативно-правовых актов при подготовке данного задания не удалось найти ни в одном из них точного и прямого ответа на этот вопрос. Скорее всего, это может быть связано с тем, что в России пока слабо используется автоматизация в плане обработки персональных данных. Существует Реестр операторов персональных данных, размещенный на «Портале персональных данных» (www.pd.rsoc.ru).

Кто же есть оператор персональных данных? Согласно закону РФ «О персональных данных» оператором ПДн может является государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Касаемо безопасности в ИСПДн: работы по обеспечению безопасности персональных данных при их обработке в ИСПД являются неотъемлемой частью работ по созданию ИСПДн (п. 4 Приложения к Постановлению Правительства РФ от 17.11.2007 г. № 781). Создавать какие-либо ИСПДн без системы защиты ПДн в ИСПДн запрещено.

Таким образом, имеем следующее заключение: изучаемая ИС является ИСПДн, обрабатывает конфиденциальную информацию, включающую в себя врачебную тайну, т.е. пациент при лечении доверяет информацию о состоянии своего здоровья и себе в целом своему лечащему врачу, т.е. осуществляет передачу персональных данных.

Данная статья базируется на документе, разработанном во время прохождения преддипломной практики, соответственно представляет собой лишь часть информации без приведения конкретных выдержек из нормативно-правовых документов. В ходе решения вопроса по поводу того, может ли быть любая АС оператором ПДн (без конкретного указания данной системы), были написаны письма с просьбой экспертам разъяснить решение данного вопроса. Следует отметить следующее: вопросы, связанные с затрагиванием ПДн, являются новым динамичным направлением правовой деятельности РФ, т.е. законы, указы, постановления и прочие документы периодически обновляются, не говоря уже об издании и принятии новых документов. Поэтому считать этот обзор окончательным нельзя.

ЛИТЕРАТУРА

1. Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных».
2. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
3. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
4. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».
5. Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28 марта 2008 г. № 154 «Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных».
6. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК РФ 15 февраля 2008 г.
7. Директива 95/46/ЕС Европейского парламента и Совета Европейского союза от 24 октября 1995 г. «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных».
8. Директива 97/66/ЕС Европейского парламента и Совета Европейского Союза от 15 декабря 1997 г., касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций.

ИССЛЕДОВАНИЕ МОДЕЛЕЙ УГРОЗ ПРИ ПОМОЩИ МАТЕМАТИЧЕСКИХ МЕТОДОВ

Е.Ц. Чимитдоржиева*, *студентка 5-го курса
г. Томск, *ТУСУР*, *каф. КИБЭВС*, *ash06@mail.ru*

В информационный век роль информации приобретает все большую важность, следовательно, и остро встает проблема ее защиты. Осмысление проблемы информационной безопасности не может быть достаточно полным и глубоким без представления о существующих видах угроз, которым может подвергаться информация, а также факторах и обстоятельствах, оказывающих влияние на состояние информационной безопасности [1].

Под угрозой безопасности обычно понимают совокупность условий и факторов, создающих опасность важным интересам личности, общества и государства. Возможность реализации тех или иных угроз зависит от наличия уязвимостей (слабого места) системы, на которую

направлена угроза. Также не стоит упускать из внимания того, кто может реализовать некоторую угрозу, т.е. злоумышленника и канал реализации угрозы.

Перед тем как построить систему защиты информации, необходимо определить перечень возможных угроз и отобрать из них наиболее применимые к конкретному случаю, т.е. построить модель угроз.

Модель угроз необходима в первую очередь для определения необходимых требований к системе защиты. Грамотно составленная модель угроз позволяет построить адекватную систему защиты информации. В то время как поверхностно составленная модель угроз является либо недостаточно эффективной, либо приводит к необоснованным затратам на средства защиты информации.

Моделирование угроз подразумевает функционирование процесса, в котором должны быть входные данные, представляющие подробную информацию о конкретном объекте, выходные данные, представляющие угрозы для конкретного объекта и параметры моделирования угроз. Существующие модели угроз представляют собой лишь некоторый список угроз для конкретной предметной области.

В результате исследования различных моделей угроз, таких как базовая модель угроз безопасности ПДн (ФСТЭК) [2], частная модель угроз безопасности ПДн Минздравсоцразвития [3], ГОСТ Р ИСО/МЭК ТО 13335-3–2007 [4], ГОСТ Р ИСО/МЭК 17799–2005 [5], были выделены критерии в соответствии, с которыми можно определить актуальность отдельной угрозы для каждого из стандартов. Каждый из перечисленных стандартов можно смоделировать, в зависимости от выделенных критериев, несколькими методами.

В результате рассмотрения методов моделирования были выбраны аппарат теории игр, аппарат теории графов, аппарат теории сетей Петри и аппарат теории случайных процессов. И был исключен аппарат теории нечетких множеств, так как при рассмотрении критериев, в соответствии с которыми определяется актуальность угрозы, дается однозначное определение этих критериев.

Применение аппарата теории игр позволяет моделировать конфликтные ситуации между злоумышленником и защитником и подразумевает наличие используемых или предполагаемых средств защиты информации. Таким образом, с помощью аппарата теории игр возможно смоделировать стандарт ГОСТ Р ИСО/МЭК 17799–2005, в котором одним из критериев определения актуальных угроз является уровень защищенности, который определяется наличием тех или иных средств защиты.

Применение аппарата сетей Петри позволяет описать причинно-следственные связи, параллельные процессы и поведение системы, в

отличие от применения аппарата теории графов, которая не дает полной информации о моделируемой системе и описывает систему без развития. С его помощью возможно моделировать как стандарт ГОСТ Р ИСО/МЭК 17799–2005, так и стандарт ГОСТ Р ИСО/МЭК ТО 13335-3–2007, а также базовую модель угроз ПДн ФСТЭК и частную модель угроз ПДн Минздравсоцразвития.

Применение аппарата теории случайных процессов также не дает полной информации о моделируемой системе. В модели не учитываются изменения характеристик системы (обновление системы, добавление нового модуля в системе и т.д.), которые приводят к переходу из одного состояния системы в другое. С его помощью возможно моделировать стандарт ГОСТ Р ИСО/МЭК ТО 13335-3-2007, базовую модель угроз ПДн ФСТЭК и частную модель угроз ПДн Минздравсоцразвития.

Для дальнейшего исследования был выбран аппарат теории сетей Петри для динамического описания поведения системы, а также для статического моделирования был выбран аппарат теории графов.

ЛИТЕРАТУРА

1. [Электронный ресурс]. Электронные данные. Режим доступа: http://www.ci.ru/inform9_97/aiti1.htm

2. [Электронный ресурс]. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК. Режим доступа: www.fstec.ru/_spravs/model.rar

3. [Электронный ресурс. Электронные данные. Режим доступа: www.minzdravsoc.ru/docs/mzsr/informatics/5/Metodika_sostavleniya_CHMU_v_uchrezhdeniyah_Minzdravsotcrazvitiya.doc

4. [Электронный ресурс]. ГОСТ Р ИСО/МЭК ТО 13335-3–2007 Методы и средства обеспечения безопасности. Ч. 3. Методы менеджмента безопасности информационных технологий. Режим доступа: www.findgost.com/gosts33/topic1/5475.zip

5. [Электронный ресурс]. ГОСТ Р ИСО/МЭК 17799–2005 Информационная технология. Практические правила управления информационной безопасностью. Режим доступа: gostexpert.ru/gost/getDoc/2794

КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ ДЛЯ ОПЕРАЦИОННЫХ СИСТЕМ, ОСНОВАННЫХ НА ЯДРЕ LINUX

Н.В. Чижов*, *студент 4-го курса каф. КИБЭВС

г. Томск, *ТУСУР*, *ФВС*, *chizov.nv@yandex.ru*

С ростом запросов пользователей должна пропорционально вырастать и безопасность ОС. Термин «безопасность ОС» имеет общий характер, включающий в себя много частностей. Важно понять, что

ОС – это не только ядро, а как минимум файловая система + системные утилиты + ядро. И поэтому каждый из этого минимума компонентов обязан предоставить должную безопасность для своей области действия.

Хорошим примером являются UNIX – системы, а точнее, их клоны, позволяющие более «прозрачно» увидеть модель ОС. Из доживших до нас клонов UNIX годными для обучения [1] можно назвать *BSD и Linux. Можно упомянуть тот факт, что *BSD является целостной операционной системой, в отличие от Linux. Для полноценной работы Linux необходимы дополнительные служебные утилиты.

Для разрабатываемого курса лабораторных работ был выбран Linux (Debian GNU\Linux) в связи с растущей популярностью [2] и заинтересованностью разработчиков сторонних средств защиты информации в отличие от *BSD систем.

Лабораторные работы стараются охватить основную минимальную связку: файловая система + ядро + системные утилиты [2]:

1) Модель DAC [3].

Целью данной работы является практическое изучение дискреционного механизма разграничения доступа на основе встроенных средств ядра Linux, позволяющих управлять доступом к файлам и папкам.

2) Модель MAC.

Лабораторная работа охватывает практическое изучение мандатной модели разграничения доступа на основе патча к ядру Linux – SMACK.

3) Аутентификация при помощи физического носителя.

В лабораторной работе рассмотрены утилиты и приложения, позволяющие производить аутентификацию в операционной системе при помощи физического объекта – eToken.

4) Аудит.

Данная лабораторная работа знакомит студентов с возможностями аудита в Linux, практических приемов использования и выявления с его помощью нарушения безопасности.

Следует отметить тот факт, что приведенные выше лабораторные работы не полностью отражают всех возможностей ядра Linux.

ЛИТЕРАТУРА

1. Таненбаум Э. Современные операционные системы. 3-е изд. СПб.: Питер, 2011. 1120 с.

2. Немет Э., Снайдер Г., Хейн Т. Руководство администратора Linux. 2-е изд.: Пер. с англ. М.: ООО «И.Д. Вильямс», 2011. 1072 с.

3. Родригес К.З., Фишер Г., Смольски С. Linux азбука ядра. М.: КУДИЦ-ПРЕСС, 2007. 584 с.

ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ

А.С. Дремин*, *студент 5-го курса
Научный руководитель Р.В. Мещеряков, *доцент*, *к.т.н.*
г. Томск, *ТУСУР*, *каф. КИБЭВС*, *ФВС*, *tusur.alex@gmail.com*

Информация является одним из важнейших элементов управления деятельностью любого предприятия. В условиях рынка от наличия информации в значительной степени зависит успех предпринимательской деятельности. Сегодня организации нередко сталкиваются с проблемой утечки информации и необходимостью построения системы защиты коммерческой тайны. Создание такой системы – сложный и многоплановый процесс, который затрагивает все структурные подразделения организации.

По мере функционирования предприятия накапливается определенный объем информации, разглашение которой, в т.ч. самими работниками, способно ухудшить его экономическое положение. В связи с этим собственник информации вправе придать ей статус охраняемой путем отнесения к коммерческой тайне и тем самым закрыть свободный доступ к ней на законном основании. Лишь сохранение этой информации в тайне придает ей коммерческую ценность.

Практикой выработаны рекомендации, которые могут быть полезны предприятию, решающему проблему сохранности своей коммерческой информации. При вводе системы защиты информации, возлагая на работников соответствующие обязанности и ответственность, необходимо учитывать требования закона.

В соответствии с действующим законодательством разработка и реализация практических мер по организации защиты коммерческой тайны возлагается на ее собственника, который должен разработать систему защиты сведений, составляющих коммерческую тайну, и обеспечить ее эффективное функционирование.

Предприятие создает систему защиты имеющейся у него конфиденциальной информации самостоятельно, опираясь на действующее законодательство, с учетом размера данного предприятия, типа используемой технологии, характера коммерческой деятельности и деловой информации, возможных каналов утечки информации, исходя из имеющихся в наличии средств и своих финансовых возможностей.

Разрабатывая систему защиты информации, необходимо прежде всего конкретизировать объект, предмет и цели защиты коммерческой информации на предприятии.

Объектом защиты информации являются сведения различных категорий, собранные в процессе деятельности предприятия, к которым может проявить интерес его конкурент.

Предметом защиты информации являются носители информации, на которых зафиксированы, отображены защищаемые сведения: документы, изделия, материалы, предметы, вещества. В качестве носителя защищаемой информации выступает также человек. Именно на охрану носителей засекреченной информации и направлены главным образом усилия предприятия.

Основная цель функционирования системы защиты информации – установить оптимальный режим работы предприятия с таким расчетом, чтобы ограничить распространение сведений, содержащих коммерческую тайну, сделать эти сведения недоступными для посторонних лиц, предотвратить их утечку и создать необходимые условия работы лицам, имеющим к ним законный доступ.

На законодательном уровне установлен ряд ограничений на право собственника владеть, пользоваться и распоряжаться имеющейся у него информацией. Так, законом №98 ФЗ от 29 июля 2004 «О коммерческой тайне» в ст. 5 установлен перечень сведений, которые не могут составлять коммерческую тайну.

К сведениям, которые не могут составлять коммерческую тайну, относятся:

1) содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, составе работников, системе оплаты труда, об условиях труда, в том числе охране труда, о показателях производственного травматизма и профессиональной заболеваемости и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

В процессе обмена информацией с государственными структурами юридическим лицам или индивидуальным предпринимателям нередко приходится сообщать по требованию их представителей сведения, выходящие за пределы указанного выше перечня и составляющие коммерческую тайну предприятия. Для такой информации органы государственной власти обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями. В случае нарушения конфиденциальности информации должностными лицами органов государственной власти эти лица несут ответственность в соответствии с законодательством Российской Федерации.

При составлении перечня сведений, которые могут составлять коммерческую тайну, может возникнуть сложность, т. к. методика отнесения тех или иных сведений к коммерческой тайне в РФ еще не разработана.

Для составления этого документа целесообразно использовать такие критерии, как:

1) информация не является общеизвестной;

2) информация получена правомерно (согласно ФЗ 98 информация, полученная от ее обладателя на основании договора или на другом основании, считается полученной законным способом);

3) информация имеет ценность для ее обладателя (позволяет получить или увеличить доход, избежать убытков, сохранить положение на рынке и т. д);

4) средства, необходимые для защиты информации, не превышают реально возможного дохода;

5) нет запрета на отнесение данной информации к коммерческой тайне в соответствии с законодательством РФ.

При установлении системы защиты информации базовым локальным нормативным документом должно быть Положение о коммерческой тайне организации, устанавливающее порядок организации рабо-

ты с коммерческой тайной, регламентирующее основные направления деятельности, механизм защиты конфиденциальной информации, закрепляющее права и обязанности работников, которые могут возникнуть в связи с их допуском к коммерческой тайне, а также объем их ответственности.

ЛИТЕРАТУРА

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

СРЕДСТВА И МЕТОДЫ АНАЛИЗА ПРОГРАММ И ПРОДИВОДЕЙСТВИЕ ЕМУ

А.И. Дударев*, *студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, ФВС

В основе каждого программного продукта лежит интеллектуальная собственность его разработчиков. На создание программы уходит много часов работы программистов, тестировщиков и службы маркетинга. С целью определения способов защиты интеллектуальной собственности было проведено исследование методов изучения программ и способов противодействия изучению, а также были изучены и протестированы возможности средств защиты, существующих на рынке сегодня.

В ходе исследования были выявлены самые распространенные способы анализа программ. Ими оказались дизассемблирование и деобфускация.

Дизассемблирование является мощным оружием в руках злоумышленника и позволяет не только понять алгоритм работы программы, но и изучить методы ее защиты. В ходе исследования были рассмотрены продукты Themida, ASProtect и Software Passport. Данные продукты используются для защиты большинства программного обеспечения и имеют большой список возможностей, в том числе антиотладчик, не позволяющий произвести анализ программы дизассемблерами. Для обхода защит данных программ взломщиками используют распаковщики, которые сами же создают для определенных версий программ защиты. Процесс обхода защит сложный, но, судя по количеству взломанных программ и генераторов серийных номеров для регистрации программ, есть специалисты, способные обойти такую защиту.

Под термином «обфускация» подразумевается приведение исполняемого кода к виду, сохраняющему функциональность программы, но

затрудняющему анализ и понимание алгоритмов работы. При этом процесс обратного преобразования становится экономически невыгодным. Были рассмотрены методы обфускации, а также программы Mangle it c++ и CXX-Obfus, позволяющие некоторые из них реализовать. Полученный данными программами код отличается от исходного лишь названиями переменных, классов и функций, которые заменяются на бессмысленные и трудночитаемые. Была осуществлена успешная обратная замена, которая сделала код пригодным для изучения. Данные программы не добавляют «мусорный» код и не усложняют логику работы существующего. Было сделано заключение, что при необходимости применения обфускации с целью усложнения логики работы программы, которую будет изучать потенциальный злоумышленник при дизассемблировании программы, программисту необходимо придумать собственные нетривиальные методы защиты наиболее значимых участков кода. Обфускация исходных кодов компилируемых языков программирования малоэффективна.

Также был рассмотрен программно-аппаратный комплекс защиты программного обеспечения HASP. Преимуществом HASP является возможность встраивать защиту в уже готовые, скомпилированные приложения, без изменения их кода. Недостатком является повышение стоимости продукта.

Была рассмотрена тема анализа программного обеспечения на наличие недекларированных возможностей. Контроль отсутствия недекларированных возможностей является одним из видов испытаний, выполняемых испытательной лабораторией при сертификации изделий в системе сертификации Министерства обороны Российской Федерации. Были рассмотрены характеристики ПО, оцениваемые при выполнении испытаний, а также программные комплексы IRIDA, АК-ВС и АИСТ-С для проведения сертификационных испытаний на отсутствие недекларированных возможностей и анализ безопасности программного кода.

Данные продукты имеют сертификаты ФСТЭК. Единственное сертифицированное средство проведения сертификационных испытаний по 2-му и 1-му уровням контроля отсутствия недекларированных возможностей – АК-ВС. Цена АК-ВС 300.000 руб.

В результате проведенного анализа выявлены основные направления безопасного программирования: обфускация, противодействие дизассемблированию, шифрование и поиск недокументированных возможностей. Результаты анализа лягут в основу при подготовке лабораторного практикума по соответствующей дисциплине.

ЛИТЕРАТУРА

1. ФСТЭК. Руководящий документ «Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации.

2. Классификация по уровню контроля отсутствия недекларированных возможностей». URL: http://www.fstec.ru/_docs/ doc_3_3_010.htm;
3. Аладдин Р.Д. http://www.aladdin-rd.ru/catalog/hasp/

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ ОРГАНИЗАЦИИ НА ПРИМЕРЕ РОСГОССТРАХ БАНКА. ТЕХНИЧЕСКИЕ СРЕДСТВА

А.В. Ефремкин*, *студент 5-го курса
г. Томск, *ТУСУР*, *каф. КИБЭВС*, *monster_007@sibmail.com*

С каждым годом в банковской сфере все больше внимания уделяется вопросам информационной безопасности, что вполне объяснимо – ведь банковский бизнес является одним из наиболее активно использующих современные информационные технологии, что влечёт за собой и проблемы информационной безопасности.

Обеспечение информационной безопасности банковской организации должно затрагивать всех её работников, а также представителей внешних сторон, с которыми организация взаимодействует для осуществления своей деятельности. Стратегия банка в части противодействия угрозам в информационной сфере должна заключаться в сбалансированном применении защитных мер различной природы: от мер на уровне бизнеса банка до специализированных мер информационной безопасности, основанных на оценке рисков информационной безопасности.

В своей практической деятельности по обеспечению информационной безопасности банк, наряду с требованиями законодательства, должен руководствоваться передовым отечественным и зарубежным опытом и соответствующими стандартами обеспечения информационной безопасности. В данной практической работе отражено применение одного из стандартов (СТО БР ИББС) к конкретной банковской организации [1, 2]. Данная методика состоит из 6 процедур:

1) определение перечня типов информационных активов предприятия;

2) составление перечня объектов среды каждому из выделенных типов информационных активов;

3) определение потенциальных угроз для объектов среды;

4) оценка степени вероятности реализации угрозы (СВР);

5) оценка степени тяжести последствий нарушения информационной безопасности (СТП);

6) выделение недопустимых рисков и предложение соответствующих защитных мер.

В ходе работы были выделены информационные активы банковской организации, нуждающиеся в защите (в качестве примера взято 2 актива) (табл. 1).

Таблица 1

Перечень информационных активов и их типов

Информационный актив и его назначение	Перечень входящей в актив информации (или документов, содержащих такую информацию)
Информация, содержащая банковскую тайну	Информация об операциях, счетах и вкладах клиентов банка...
	Кредитная история…
Основные персональные данные клиентов	Личные данные, контактная информация и т.д.

Также был определен перечень источников угроз, которые могут привести к потере свойств информационной безопасности (в качестве примера взято 2 актива) (табл. 2).

Таблица 2

Перечень типов объектов среды

Информационный актив	Уровень иерархии информационной структуры	Типы объектов среды
Информация, содержащая банковскую тайну	Физический	Линии связи
	Сетевой	Маршрутизаторы, коммутаторы
	Носителей	Жесткие диски, бумажные носители
Основные персональные данные клиентов	Физический	Линии связи
	Сетевой	Маршрутизаторы, коммутаторы
	Носителей	Жесткие диски, бумажные носители

Были выявлены и оценены риски информационной безопасности для каждого актива, связанные с техническими средствами (в качестве примера взят один тип среды) (табл. 3).

Таблица 3

Перечень угроз и соответствующие оценки СВР и СТП

Типы объектов среды	Свойство информационного актива	Источники угроз	Способ реализации	СВР	СТП
Линии связи	Конфиденциальность	Внешний	Подключение к линии	М	М
	Доступность, целостность	Внешний	Повреждение кабелей	С	М
		Внутренний	Повреждение кабелей	С	М

Затем были выделены недопустимые риски (а в качестве примера взят один недопустимый риск) (табл. 4).

Таблица 4

Выделение недопустимых рисков

Название группы	Описание недопустимого риска
Жесткие диски	Кража накопителя внутренними нарушителями
	Кража накопителя внешним нарушителем
	Поломка накопителя. Выход из строя жесткого диска в связи с неисправностью оборудования.

После чего выбраны соответствующие защитные меры, снижающие риски (в качестве примера взята одна мера защиты) (табл. 5).

Таблица 5

Выбранные меры защиты

Описание недопустимого риска	Мера защиты
Кража накопителя внутренними нарушителями	Действует политика информационной безопасности. Сотрудники несут личную ответственность за несоблюдение данной политики и т.д.

В ходе работы были изучены стандарты, использующиеся для обеспечения безопасности в банковских организациях Российской Федерации. Были проведены анализ и оценка рисков информационной безопасности банковской организации на примере операционного офиса «Томский» Новосибирского филиала ОАО «Росгосстрах Банк» в соответствии со стандартом Банка России [3], а именно:

1) составление перечня информационных активов, нарушение безопасности которых связано с техническими средствами;

2) составление перечня объектов среды, в которых обрабатываются или хранятся данные активы;

3) составление перечня угроз информационной безопасности для активов и объектов среды;

4) выделение недопустимых рисков на основе оценивания угроз;

5) определение защитных мер для недопустимых рисков.

ЛИТЕРАТУРА

1. СТО БР ИББС-1.0-2010. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Введ. 2010-06-21. М.: Издание официальное. 2010. 42 с.

2. РС БР ИББС-2.2-2009. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения инфор-

мационной безопасности». Введ. 2010-01-01. М.: Издание официальное. 2009. 23 с.

3. Официальный сайт Росгосстрах Банка [Электронный ресурс]. Режим доступа: http://rgsbank.ru/

РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ КОНКУРЕНТНОГО РАННЕГО ПРЕДУПРЕЖДЕНИЯ ДЛЯ ПРЕДПРИЯТИЯ

И.И. Ерофеева*, *студентка 4-го курса

Научный руководитель Н.И. Баяндин, *зав. каф. КОИБАС*

г. Москва, *МЭСИ*, *каф. КОИБАС*, *IErofeeva@mesi.ru*

В последние годы руководители предприятий и служб безопасности стали уделять больше внимания экономической и информационной безопасности предприятия в условиях растущей конкуренции. Конкурентоспособность любого предприятия во многом зависит от двух факторов:

– защиты своего информационного пространства от несанкционированного доступа;

– выявления новых сегментов рынка раньше конкурентов.

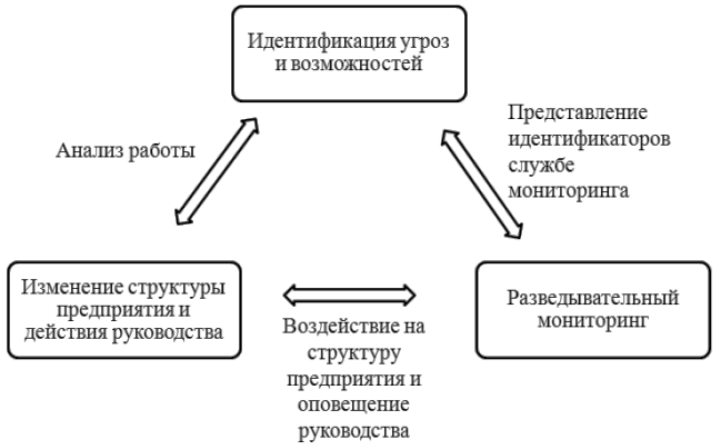


Рис. 1. Механизм КРП

Эффективным инструментом, решающим эти задачи, является конкурентная разведка (КР). Главной задачей КР является достижение стратегического конкурентного преимущества, т.е. осуществление раннего выявления угроз и возможностей компании.

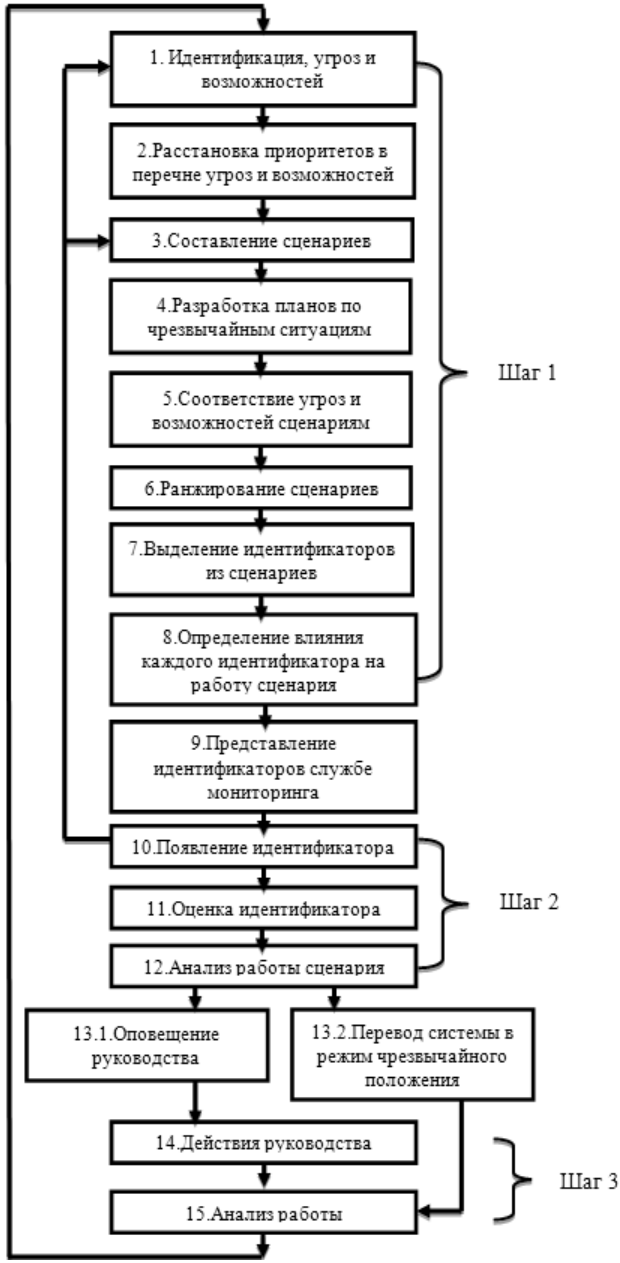


Рис. 2. Алгоритм работы системы КРП

В настоящее время недостаточно разработана методология осуществления стратегического конкурентного анализа, поэтому предлагается рассмотреть методологию «конкурентного раннего предупреждения» (КРП), разработанную американским аналитиком, директором «академии КР» Беном Джиладом [1].

Механизм КРП состоит из трех шагов (рис. 1) [2].

В статье рассмотрены работа системы КРП, а также методы и оценки применимые на её этапах [3, 4]. Использован аппарат теории вероятностей [5]. Проведена формализация процессов каждого шага системы.

В ходе работы использован метод «сопоставления данных», применяемый в военной разведке [5]. Процесс КРП основан на сценарном подходе(рис. 2). Высокая роль неформальных методов обосновывается крайней разнородностью параметров, учитываемых при проведении анализа, а также наличием большого числа качественных оценок (этапы 1, 3, 4, 5) [1].

Планируется продолжение исследований по следующим направлениям:

– построение компьютерной модели работы системы КРП на основе математического аппарата сетей Петри;

– более глубокое исследование факторов, влияющих на оценку истинности идентификаторов;

– построение шаблонов (общих моделей) угроз и возможностей предприятия.

ЛИТЕРАТУРА

1. Джилад Б. Конкурентная разведка. Как распознавать внешние риски и управлять ситуацией. СПб.: Питер, 2010. 320 с.

2. Ерофеева И.И. Система конкурентного раннего предупреждения угроз для образовательного учреждения // Научная сессия ТУСУР–2011: Матер. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых, Томск, 4–6 мая 2011 г.: В 6 ч. Ч. 3. Томск: В-Спектр, 2011. 356 с.

3. Хорин А.Н., Керимов В.Э. Стратегический анализ: учеб. пособие. М.: Эксмо, 2006. 288 с.

4. Плэтт В. Добывание, анализ и обработка стратегических разведывательных данных. М.: ММ Медиа Дистрибьюшн, 2006. 292 с.

5. Работа по анализу информации. Основные методы [Электронный ресурс]. Режим доступа: http://www.vrazvedka.ru/analitic/19-2009-11-30-11-24-36.html

МОДЕЛИ И АЛГОРИТМЫ ПОЛУЧЕНИЯ ВЕРОЯТНОСТНЫХ ОЦЕНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.А. Феденко, слушатель 5-го курса радиотехнического факультета Воронежского института МВД России

Научный руководитель В.В. Меньших, начальник каф. высшей математики ВИ МВД России, проф., д.ф.-м.н.

г. Воронеж, ВИ МВД России, oskic@vor.mvd.ru

В настоящее время осуществляется широкое внедрение в деятельность органов внутренних дел (ОВД телекоммуникационных систем (ТКС), обеспечивающих передачу, хранение и обработку служебной информации. Учитывая характер деятельности ОВД, информация, передаваемая по ТКС, часто служит предметом преступных посягательств. Для противодействия им ТКС оснащаются различными средствами и системами защиты информации. Однако они не могут обеспечить абсолютную защиту информации. Учитывая, что появление угроз невозможно предсказать на 100%, так как они возникают случайным образом, в данном вопросе целесообразнее и эффективнее обратиться к методам моделирования [1], которые используются практически во всех областях человеческой деятельности и позволяют экономить время и ресурсы.

Целью работы является разработка моделей получения вероятностных оценок показателей обеспечения информационной безопасности и алгоритмов их реализации.

1. Построение концептуальной модели системы. Любая ТКС представляет собой множество узлов, соединенных линиями связи. Поэтому удобно для описания структуры ТКС использовать методы теории графов [2]. ТКС может быть представлена графовой моделью, в которой вершины соответствуют узлам, а дуги – линиям связи (если линия связи позволяет осуществлять двустороннее соединение, то она моделируется двумя противоположно направленными дугами).

Однако размерность такой модели для реальных ТКС может оказаться достаточно большой. Анализ осуществления удаленного доступа с помощью ТКС показывает, что не все узлы могут быть использованы для осуществления такого доступа, поэтому будем считать, что граф содержит только те узлы, которые потенциально могут быть использованы для осуществления удаленного доступа.

Для построения модели ТКС, состоящей только из указанных узлов, автором разработан алгоритм, заключающийся в преобразовании построенной графовой модели в две сети Петри [3], выполнение переходов в которых приводит к нахождению искомых узлов.

Полученная модель преобразуется в структурно-параметрическую модель. Обозначим $P=\{p_1, p_2, \ldots, p_m\}$ – множество весов дуг, соответствующих вероятностям угроз информационной безопасности, которые, в свою очередь, определяются совокупностями следующих вероятностей [8]: $A(t) = \{\alpha_1(t), \alpha_2(t),\ldots, \alpha_m(t)\}$– множество весов дуг, соответствующих вероятностям несанкционированного доступа к информации по линиям связи, зависящее от времени t; $B(t) = \{\beta_1(t), \beta_2(t), \ldots, \beta_m(t)\}$ – множество весов дуг, соответствующих вероятностям несанкционированного воздействия на информацию по линиям связи, зависящее от времени t; $\Gamma(t) = \{\gamma_1(t), \gamma_2(t), \ldots, \gamma_m(t)\}$ – множество весов дуг, соответствующих вероятностям несанкционированного блокирования информации по линиям связи, зависящее от времени t.

Таким образом, структурно-параметрической концептуальной моделью ТКС является ориентированный взвешенный граф $G = (V, E, P)$.

Усредним по временному параметру приведенные выше оценки вероятностей (T – достаточно большой промежуток времени функционирования ТКС): $\alpha_i = \int_{t_0}^{t_0+T} \alpha(t)dt/T$, $\beta_i = \int_{t_0}^{t_0+T} \beta(t)dt/T$, $\gamma_i = \int_{t_0}^{t_0+T} \gamma(t)dt/T$.

Тогда оценки вероятностей угроз информационной безопасности на каналах связи равны $p_i = 1 - (1 - \alpha_i)(1 - \beta_i)(1 - \gamma_i)$.

2. Алгоритмизация моделирования оценок. При нахождении значений вероятности доступа требуется находить мультипликативную оценку, т. е. перемножать оценки вероятностей на отдельных дугах, входящих в заданный ориентированный путь. Алгоритмы построения пути, обеспечивающего максимальное и минимальное значение мультипликативной оценки, неизвестны. Вместе с тем известны соответствующие алгоритмы нахождения минимальной и максимальной аддитивных оценок, т. е. оценок, получаемых как суммы оценок на отдельных дугах. Покажем, что эти алгоритмы могут быть преобразованы в алгоритмы нахождения мультипликативной оценки.

Осуществим следующее преобразование:

$$P = e^{\ln P} = e^{-\sum_{i=1}^{k}(-\ln p_i)} = 1/e^{\sum_{i=1}^{k}(-\ln p_i)}. \qquad (1)$$

Данный математический прием позволяет заменить операции умножения операциями сложения, т. е. задачу нахождения мультипликативной оценки заменить задачей нахождения аддитивной оценки. Однако при этом следует заметить, что значения вероятностей $p_i \le 1$, и поэтому $-\ln p_i \ge 0$. Из формулы (1) следует, что:

1) минимизация выражения $\sum_{i=1}^{k}(-\ln p_i)$ приводит к максимизации значения P, т.е. искомой максимальной вероятности возникновения угрозы в телекоммуникационной системе;

2) максимизация выражения $\sum_{i=1}^{k}(-\ln p_i)$ приводит к минимизации значения P, т.е. искомой минимальной вероятности возникновения угрозы в телекоммуникационной системе.

Учитывая это обстоятельство, автором были преобразованы известные алгоритмы нахождения минимального пути в графе в алгоритм нахождения пути, на котором может возникнуть максимальная вероятность угрозы информационной безопасности в ТКС. При помощи данных алгоритмов мы определили узлы и линии связи, которые вероятнее всего будет использовать злоумышленник для доступа к защищаемым информационным ресурсам. Следовательно, их необходимо более надежно защитить с учетом выделенных на мероприятия защиты материальных, технических и программных ресурсов.

Если требуется найти путь, вероятность возникновения угрозы информационной безопасности на котором минимальна, то можно использовать алгоритм, аналогичный алгоритму нахождения критического пути на графе.

Разработанные алгоритмы реализуют схему поиска в ширину и поэтому количество выполняемых операций линейно зависит от суммы числа вершин и дуг графовой модели [4].

Таким образом, разработана модель оценки вероятности оценки информационной безопасности при передаче информации в телекоммуникационной сети, построены новые алгоритмы оценки минимальной и максимальной вероятности осуществления угроз информационной безопасности и нахождения элементов ТКС на которых они могут быть реализованы. Это создает основу для разработки методики модернизации систем защиты информации в интересах максимизации ее информационной безопасности.

ЛИТЕРАТУРА

1. Советов Б.Я. Моделирование систем / Б.Я. Советов, С.А. Яковлев. М.: Высшая школа, 2005. 344 с.

2. Горбатов В.А. Фундаментальные основы дискретной математики. М.: Наука. Физматлит, 2000. 544 с.

3. Питерсон Дж. Теория сетей Петри и моделирование систем: Пер. с англ. М.: Мир, 1984. 264 с.

4. Новиков Ф.А. Дискретная математика для программистов: Учеб. для вузов. СПб.: Питер, 2005. 364 с.

ИССЛЕДОВАНИЕ ПРЕВЕНТИВНЫХ МЕР ДЛЯ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.Г. Ганюшкин, студент 5-го курса
Научный руководитель Р.В. Мещеряков, доцент, к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, GanyushkinIG@gmail.com

Информационная безопасность (ИБ) компаний зависит от снижения рисков, следовательно, эффективное управление рисками способствует обеспечению непрерывности бизнеса. Согласно британскому стандарту BS ISO/IEC 27005:2005 риск ИБ – потенциальная возможность использования определенной угрозой уязвимостей актива или группы активов для причинения вреда организации. Из определения риска ИБ видно, что риск – это потенциальный вред организации. Риск состоит из влияния на бизнес, угрозы и уязвимости (рис. 1).

Рис. 1. Структура риска

Из рис. 1 видно, что если снизить уровень угроз, уязвимостей или влияния на бизнес, то объем риска значительно уменьшится. Рассмотрим способы управления рисками, например, в стандарте BS ISO/IEC 27005:2005 выделяют следующие:

1) уменьшение рисков;
2) принятие рисков;
3) избежание рисков;
4) передача рисков.

Особый интерес представляют методы уменьшения рисков, часто используемые в информационных технологиях (ИТ) и ИБ. Они бывают превентивные, детективные, корректирующие. Рассмотрим их в порядке убывания их эффективности.

Превентивные меры:

1. **Снижение угрозы** считается самым эффективным способом снижения риска. Например, если нашему бизнесу угрожает ураган, то мы можем переехать в местность, где ураганы не встречаются.

2. На втором месте находится метод по **снижению уязвимостей**. Например, устранение (исправление) уязвимостей, т.е. если у нас нет уязвимостей, то и угрозы нам не страшны.

3. На третьем месте находятся **меры по снижению влияния** на актив. К этой мере относятся различные резервирования сервисов, отказ от использования уязвимого актива и т.д.

Детективные меры, а именно **обнаружение**, на четвертом месте. К этим инструментам относятся, например, антивирусы. Эти меры позволяют сообщить, что проблема уже случилась.

Коррективные меры, такие как **восстановление**, расположены на пятом месте по эффективности. Это очень важный метод, который позволяет восстановить систему после критических сбоев. Но этот метод используется уже тогда, когда риск осуществился и нужно восстанавливать работоспособность [1].

Компаниям, занимающимся снижением рисков ИБ, необходимо акцентировать свое внимание на использовании наиболее эффективных мер. Превентивные методы управления рисками являются более эффективными для снижения рисков и повышения непрерывности бизнеса, в то время как детективные и коррективные не дают должного эффекта, в силу ограниченности многими факторами. Среди превентивных методов, с точки зрения возможности использования в компаниях, самым эффективным считается метод устранения уязвимостей, так как уязвимые ресурсы находятся внутри предприятия и сотрудники могут непосредственно управлять ими.

Изучение услуг в сфере защиты информации актуализирует создание технологий для обретения и развития навыков по устранению уязвимостей информационных системы ИТ-специалистами. Для удовлетворения потребностей рынка разрабатывается программный комплекс, позволяющий приобрести и отработать подобные навыки. Повышение эффективности обучения и приближение к реалистичности ситуации достигается посредством функции, позволяющей проведение ролевых игр.

С помощью разрабатываемой системы предполагается:

1) допуск к работе лиц, удовлетворяющих соответствующим квалификационным требованиям в сфере ИТ-безопасности;

2) проведение подготовки и аттестации работников предприятий и учреждений в области ИТ-безопасности;

3) обучение работников служб безопасности действиям при критических или чрезвычайных ситуациях;

4) анализ причин возникновения инцидентов и принятия мер по устранению выявленных причин.

Суть идеи создания программного комплекса заключается в том, что предлагается применять более эффективные методы управления рисками. Применение превентивных мер, а именно снижение количества уязвимостей, хотя бы на 20% приводит к снижению рисков на

80%, это связано с тем, что около 80% злоумышленников могут использовать около 20% уязвимостей (рис. 2) [1].

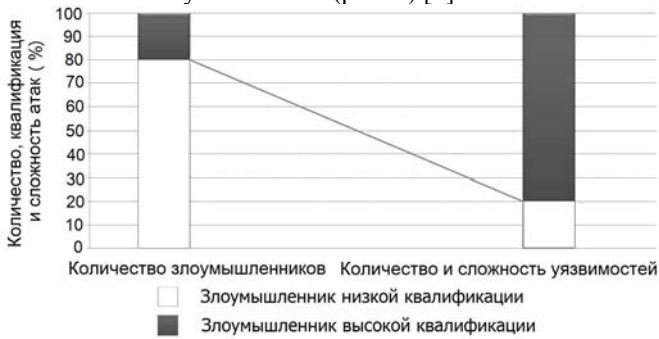


Рис. 2. Диаграммы зависимостей надежности системы

Недооценка серьезности риска реализации угроз ИБ с использованием приложений, доступных со стороны сети Интернет, является основным фактором низкого состояния защищенности большинства из них. По данным статистики, в 83% сайтов были обнаружены критичные уязвимости и в 78% случаев в программном обеспечении приложения содержатся уязвимости средней степени риска, с помощью которых можно осуществить успешную атаку на приложение или сервер. Результаты исследований демонстрируют необходимость повышения количества квалифицированных специалистов, имеющих опыт обнаружения и устранения уязвимостей системы для повышения надежности ведения бизнеса. Разрабатываемая система полезна как на стадии повышения квалификации сотрудников ИТ-отделов и консалтинговых фирм, так и на более ранних стадиях подготовки кадров.

ЛИТЕРАТУРА

1. Превентивные меры снижения рисков [Электронный ресурс]. Электрон. дан. [Москва]. Режим доступа: http://www.penetrationtest.ru/service/ Preventive_measures_detail.html, свободный. Загл. с экрана.

АНАЛИЗ ПОДХОДОВ К ПОСТРОЕНИЮ МОДЕЛЕЙ УГРОЗ ИНФОРМАЦИННОЙ БЕЗОПАСНОСТИ

Р.Ю. Ибрагимов, студент

г. Томск, ТУСУР, каф. КИБЭВС, poweltinah@sibmail.ru

Вопрос защиты информации подразумевает комплексный подход, включая такие элементы, как организационное, правовое управление, программирование, математические средства, программно-аппаратные и технические средства.

Основная задача – затронуть все максимально возможные аспекты в области защиты информации, в частности, определить полный перечень угроз и в будущем использовать данный перечень угроз с конкретной системой. Важны именно полнота и актуальность перечня угроз, так как при отсутствии какого-либо элемента вероятность реализации угрозы резко возрастает и компания может понести ущерб. Правильней и проще из полного перечня угроз выделить те, которые являются актуальными для рассматриваемой системы, чем заниматься поиском угроз каждый раз. Стоит учитывать, что уровень защиты должен соответствовать статусу защищаемой информации и затраты на защиту информации не должны превышать стоимости защищаемой информации. Таким образом, необходимо построение модели угроз, содержащей полный перечень актуальных угроз во избежание трудностей в процессе защиты информации.

Из отечественных моделей угроз были проанализированы базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК), классификация угроз Digital Security, РС БР ИББС-2.4-210, рекомендации в области стандартизации банка России, отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации. В ходе анализа зарубежных моделей угроз (NIST Special Publication 800-30. National Institute of Standards and Technology (NIST) – Risk Management Guide for Information Technology Systems и The STRIDE Threat Model) было установлено, что перечня угроз в них не содержится, а основное их направление – расчет рисков.

Из рассмотренных моделей угроз были выделены источники угроз, объекты угроз, уровень реализации угроз и их деструктивное действие и на их основании был построен полный перечень угроз, а также было показано отсутствие какого-либо элемента в каждой модели. Также было установлено, что каждая из рассматриваемых моделей угроз содержит избыточность в виде присутствия модели нарушителя и ни одна из моделей не описана с помощью математического аппарата. Модель угроз Digital Security имеет поверхностное описание угроз, что затрудняет формализовать данную модель, в отличие от модели угроз информационной безопасности ФСТЭК.

Был получен полный перечень источников угроз, объектов угроз, уровней реализации угроз, деструктивного действия, полученный из рассмотренных моделей угроз информационной безопасности.

Источники угроз:

– внутренний нарушитель (имеющий доступ к АС);
– внешний нарушитель (не имеющий доступа к АС);

– сотрудники, действующие в/вне рамках предоставленных полномочий;
– форс-мажорные обстоятельства, отказ оборудования;
– воздействие на персонал (физическое, психологическое);
– поставщики программно-технических средств;
– программно-аппаратная закладка, вредоносная программа.

Объекты угроз:
– линии, каналы связи;
– информация с ПДн;
– прикладное ПО (включая СУБД);
– сотрудники;
– средства связи;
– носители информации с ПДн (отчуждаемые, встроенные);
– средства ввода-вывода информации.

Уровень реализации угрозы:
– операционная система;
– программное обеспечение, драйверы;
– сетевой уровень (информация с ПДн, обрабатываемая сетевыми службами);
– уровень сетевых приложений;
– система защиты информации;
– программно-аппаратные средства;
– устройства ввода-вывода;
– технические каналы утечки информации.

Деструктивное действие:
– нарушение конфиденциальности, целостности, доступности.

ЛИТЕРАТУРА

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК. Введ. 2008-15-02 [Электронный ресурс]. Режим доступа: http://www.fstec.ru/_spravs/model.rar

2. Модель угроз Digital Security [Электронный ресурс]. Режим доступа: http://dsec.ru/products/grif/fulldesc/classification/

3. РС БР ИББС-2.4-210. Рекомендации в области стандартизации банка России. Отраслевая частная модель угроз безопасности персональных данных при из обработке в информационных системах персональных данных организаций банковской системы Российской Федерации [Электронный ресурс]. Режим доступа: http://cbr.ru/credit/Gubzi_docs/rs-24-10.pdf

4. NIST Special Publication 800-30. National Institute of Standards and Technology (NIST). Risk Management Guide for Information Technology Systems [Электронный ресурс]. Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ И МОНИТОРИНГА ТРАФИКА НА КОММУТАТОРАХ CISCO SYSTEMS

А.Ю. Исхаков*, *студент 4-го курса
Научный руководитель Р.В. Мещеряков, доцент, к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, iay@security.tomsk.ru

Процесс администрирования вычислительных сетей неизбежно связан с необходимостью мониторинга сетевого трафика. Это является источником информации при распределении вычислительных мощностей, определении и локализации отказов, решении вопросов безопасности и масштабировании сети.

Объектом исследования является КВС студенческого городка Томского государственного университета систем управления и радиоэлектроники. Преобладающим большинством устройств, используемых в данной сети, является оборудование мирового лидера в области сетевых технологий – компании Cisco Systems [2].

Сетевой трафик – объём информации, передаваемой по сети за определенный период времени. Доминирующим протоколом межсетевого взаимодействия на сегодняшний момент остается IP версии 4. Протокол IP соответствует сетевому уровню модели OSI [1]. Информация (данные) между отправителем и получателем упаковывается в пакеты, имеющие заголовок, и «полезную нагрузку». Заголовок определяет источник и пункт назначения пакета (IP-адреса отправителя и получателя), размер пакета, тип полезной нагрузки.

Применительно к коммутаторам Cisco Systems для мониторинга и контроля сетевого трафика могут применяться следующие подходы:

1) Непосредственное использование консоли устройства (физический либо удаленный доступ). Данный подход позволяет проводить мониторинг на одном устройстве в данный момент времени. Возможно использование следующего инструментария:

– средства отладки. В состав операционной системы Cisco IOS включена команда *debug*, позволяющая отслеживать все процессы, происходящие на устройстве, в т.ч. трафик сетевых интерфейсов. Основным недостатком данного метода является значительное увеличение нагрузки на процессор коммутатора;

– списки контроля доступа (ACL) [2]. ACL определяют условия, в соответствии с которыми проверяется каждый пакет, обрабатываемый коммутатором. Типичными критериями являются адрес отправителя, адрес получателя и тип протокола.

2) Передача данных о сетевом трафике на выделенные устройства мониторинга. Для применения данного подхода можно использовать

как проприеритарные, так общепринятые специализированные протоколы сбора данных о состоянии сетевых устройств. В частности:

– протокол NetFlow (RFC 3954) [1, 2], разработанный компанией Cisco Systems и поддерживаемый многими производителями сетевого оборудования (Juniper, 3Com и др.). Netflow позволяет передавать данные не только о количественных характеристиках сетевого трафика, но и о его типах и составе (адрес отправителя и получателя, порт, тип протокола др.). Данные передаются с коммутатора (сенсора) на внешнее хранилище (коллектор) и затем подвергаются анализу различными программными средствами;

– протокол удаленного управления SNMP [1]. Протокол SNMP получает необходимые данные из базы управляющей информации (MIB) [1]. MIB представляет собой базу данных древовидной структуры, где все переменные классифицированы по тематике. Каждое поддерево содержит определенную тематическую подгруппу переменных. Наиболее важные компоненты, отвечающие за работу сетевых узлов, объединены в подгруппе MIB-II.

3) Использование комплекса программно-аппаратных средств для захвата и детального анализа всего сетевого трафика. Данный подход может быть реализован как с использованием встроенного функционала коммутаторов Cisco, так и посредством дополнительного оборудования:

– захват трафика непосредственно в точке подключения на уровне устройств доступа (согласно 3-уровневой модели сети, предложенной компанией Cisco). В данном случае необходимо устройство, обеспечивающее копирование всего трафика и передачу его на выделенный сервер с сетевой картой для приема копий Ethernet-пакетов. В качестве таких устройств могут выступать Ethernet hub (repeater) [1] или аппаратный раздвоитель [1];

– настройка зеркалирования (port mirroring) [2] на коммутаторе Cisco.

Проведенный обзор методов и средств анализа сетевого трафика показал, что коммутаторы компании Cisco предоставляют пользователям широкий спектр возможностей для мониторинга процессов в локальных сетях.

ЛИТЕРАТУРА

1. Принципы организации учета IP-трафика [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/136844/, свободный (дата обращения: 17.02.2012).

2. Учет трафика на маршрутизаторах Cisco [Электронный ресурс]. Режим доступа: http://hypercomp.ru/articles/cisco-routers-accounting-with-mrtg-over-snmp//, свободный (дата обращения: 10.03.2012).

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

И.Я. Иванчук , студент 5-го курса; А.А. Конев, доцент
г. Томск, ТУСУР, каф. КИБЭВС

В соответствии с федеральными государственными образовательными стандартами высшего профессионального образования по направлению подготовки (специальности) 090303, подготовка специалиста предусматривает изучение математического и естественнонаучного цикла, в который входит дисциплина «Защита электронного документооборота» [1].

Система электронного документооборота (СЭД) – организационно-техническая система, обеспечивающая процесс создания, управления доступом и распространения электронных документов в компьютерных сетях, а также обеспечивающая контроль над потоками документов в организации [2].

Рассмотрев системы электронного документооборота с сайта «Обзор систем электронного документооборота», можно выделить системы Directum, DocsVision, МОТИВ и ЕВФРАТ. Основные критерии выбора системы для разработки лабораторных работ по специальности «защита электронного документооборота» – сертификация ФСТЭК и наличие демоверсии (демодоступа). Сертификат ФСТЭК выдан системам DocsVision и ЕВФРАТ, поэтому Directum и МОТИВ не подходят по критерию сертификация ФСТЭК. Наличие демоверсии (демодоступа) предоставлено системами DocsVision и ЕВФРАТ, но система ЕВФРАТ не предоставляет того функционала, который нужен для разработки лабораторных работ. Окончательным вариантом выбрана система DocsVision.

В связи с введением новой специальности 090303 «информационная безопасность автоматизированных систем» в Томском университете систем управления и радиоэлектроники и введением новой дисциплины «Защита электронного документооборота», были рассмотрены системы электронного документооборота, чтобы выбрать из них наиболее подходящую и составить комплекс лабораторных работ для этой системы.

Перечень который планируется использовать при разработке комплекса лабораторных работ:

- основные понятия и структура документооборота;
- модуль делопроизводство системы электронного документооборота DocsVision;
- управление бизнес-процессами системы DocsVision, использование конструктора решений и сервиса уведомлений системы электронного документооборота DocsVision;

− работа с документами MS Office системы электронного документооборота DocsVision;

− установка и администрирование системы электронного документооборота DocsVision;

− электронно-цифровая подпись и шифрование для системы электронного документооборота DocsVision.

В перечень ПО, которое планируется использовать в данных лабораторных работах, входят: ОС Windows 7, VirtualBox, MS Office 2010.

В результате работы были рассмотрены системы электронного документооборота, составлены перечень лабораторных работ и содержание предложенных работ, т.е. вопросы, которые необходимо проработать при составлении лабораторных работ, а также программное обеспечение, которое необходимо использовать при проведении лабораторных работ.

ЛИТЕРАТУРА

1. Портал «Российское образование» // Федеральный государственный образовательный стандарт высшего профессионального образования по специальности 090303 «информационная безопасность автоматизированных систем» [Электронный ресурс]. URL: http://www.edu.ru/db/cgi-bin/portal/spe/spe_new_list.plx?substr=090303&s t =all&qual=0

2. Обзор систем электронного документооборота [Электронный ресурс]. Режим доступа: http://www.ixbt.com/soft/sed.shtml

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ КОДЕ

С.С. Харченко, студент 5-го курса каф. КИБЭВС

Научный руководитель Е.М. Давыдова, доцент

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, ss.kharchenko@gmail.com

Сегодня вопросы безопасного программирования всплывают на поверхность все чаще и чаще. Но что такое безопасное программирование? Под безопасностью, как правило, понимают некоторое состояние защищенности как противоположную сторону опасности, защиту от угроз. Сегодня в программирование выделяют десятки основных видов угроз безопасности – как безопасности работы приложения, написанного на том или ином языке программирования, так и безопасности информационных потоков, циркулирующих в вашем приложении. Мнение специалистов в области защиты информации по поводу безопасного программирования расходятся и разнятся в том, что одни считают, что это является одной из наиболее актуальных проблем, другие же считают, что достаточно на этапе компоновки приложения довериться высокоинтеллектуальной среде разработке. Однако все они

сходятся в одном, что проблемы безопасности программирования существуют, а следовательно, необходимо этим заниматься. Тем более, что к этому располагает единственный, пожалуй, на сегодня документ, который носит сугубо рекомендательный характер и не отвечает на вопрос: «Как проводить испытания?». В РД НДВ [1] приводятся только основные положения и требования к уровням контроля при проведении испытаний на отсутствие недекларированных возможностей в программных изделиях. Анализ и выявление уязвимостей программного кода могут быть основным или добавочным методом тестирования программного обеспечения, называемым тестированием безопасности. Наиболее распространено применение анализаторов программного кода для выявления уязвимостей и недекларированных возможностей ПО. Основными способами анализа являются статистический и динамический анализ исходного кода, а также контроль целостности всего исходного кода.

Существует два кардинальных подхода поиска уязвимости в программном коде. Первый подход – «ручное сканирование», дает наилучшие результаты как в плане количества, так и качества, но существует большая проблема: это подход наиболее дорогостоящий и, что наиболее важно, долговременный. Проверка кода «вручную» должна считаться вспомогательным решением, а не лучшим подходом к поиску уязвимых мест кода или заменой другими подходами. Проверка кода также не должна рассматриваться в качестве замены моделирования угроз, фаззинга [2] или соблюдения рекомендаций по программированию.

По сравнению с другими подходами проверка кода должна использоваться преимущественно для наиболее важных областей и проблем, где эффективность других подходов ограничена. Второй подход – автоматизированный, представляет собой приложение, которое имеет ограниченный набор сигнатур уязвимостей и осуществляет поиск по заданным сигнатурам во всем программном коде. Данный подход в плане недостатков имеет только ограниченный набор сигнатур, но намного быстрее и дешевле первого. Также стоит отметить, что использование сигнатур имеет место быть не только при тестировании программного обеспечения, но и может являться вспомогательным инструментов для разработчиков при выпуске финальных версий программ. Но как объединить в себе все плюсы и исключить недостатки обоих подходов, объединив их в единую концепцию? Как выход предлагается создание Web-ресурса, на котором каждый желающий мог бы зарегистрироваться и добавлять сигнатуры уязвимостей. Чтобы исключить наплыв «ботов», зарегистрированному пользователю необходимо будет пройти тестирование по соответствующей области знаний и регулярно подтверждать свои умения и навыки.

Такое решение позволит получить регулярно обновляемую базу сигнатур. Также одним из плюсов такого решения будет отсутствие привязанности к конкретному языку программирования, чем страдают многие приложения, осуществляющие статический анализ кода. Структура информационного обмена проектируемой системы приведена на рис. 1.

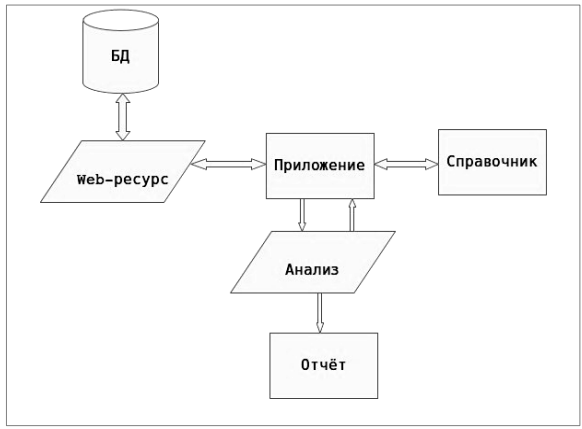


Рис. 1. Структура информационного обмена системы

Главная идея Web-ресурса заключается в следующем: использование ресурса возможно только в том случае, если вы внесли вклад в развитие проекта, то есть добавили хотя бы одну актуальную сигнатуру, а добавление сигнатур возможно только в том случае, если вы являетесь специалистом в данной области или же имеете опыт проектирования и программирования систем на языках высокого уровня. Схема жизненного цикла пользователя Web-ресурса приведена на рис. 2.

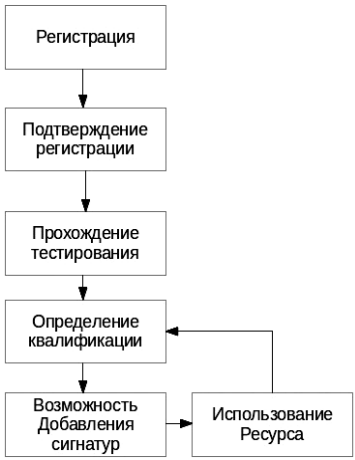


Рис. 2. Жизненный цикл пользователя Web-ресурса

При правильном подходе к определению квалификации разработанный подход позволит значительно увеличить скорость поиска уязвимостей, но самое главное, сделает обслуживание данной системы намного дешевле, чем при ручной обработке исходных кодов.

ЛИТЕРАТУРА

1. Руководящий документ. Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. М.: Гостехкомиссия России, 1998.

2. Саттон М., Грин А., Амини П. Fuzzing: исследование уязвимостей методом грубой силы: Пер. с англ. СПб.: Символ-Плюс, 2009. 560 с.

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ФУНКЦИОНИРОВАНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

А.О. Корсюк, студент 5-го курса;
М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, Xandrkors@gmail.com

С появлением тенденции перевода бумажного документооборота в электронный документооборот появилась необходимость установить отсутствие искажения информации в электронном документе с момента формирования и проверить принадлежность документа владельцу. В этих целях начали использовать электронную цифровую подпись (ЭЦП).

Для обеспечения безопасности и исключения подмены открытых ключей в соответствии с Федеральным законом «Об электронной цифровой подписи» создается доверительная организация – Удостоверяющий центр (УЦ), который хранит в себе все сертификаты открытых ключей пользователей. УЦ – основной компонент автоматизированных информационных систем с применением электронных цифровых подписей. Главная цель создания Удостоверяющего центра состоит в организации и поддержке безопасности защищенного, юридически значимого электронного обмена документами как внутри предприятий или организаций, так и между ними.

В организационной составляющей УЦ можно выделить 3 основных компонента:

1) организационная структура, отвечающая за обслуживание серверного и телекоммуникационного хозяйства (технический отдел). В неё входят: сервер ЦР, сервер ЦС, сервер репозитория и архив;

2) организационная структура, отвечающая за работу с владельцами электронной подписи (отдел технической поддержки пользовате-

лей УЦ). В неё входят: оператор ЦР, системный администратор, администратор УЦ;

3) организационная структура, отвечающая за управление удостоверяющим центром (отдел управления УЦ). В неё входят: руководитель УЦ, уполномоченное лицо УЦ, администратор ИБ.

Каждый из выделенных компонентов содержит набор организационно-распорядительных и технических задач.

С программно-технической стороны УЦ должен быть укомплектован:

– межсетевым экраном – необходим для защиты локальной сети УЦ от угроз Интернета или любой другой внешней сети;

– лицензионным программным обеспечением и операционной системой;

– сертифицированными программными и аппаратными средствами;

– антивирусом – для защиты УЦ от вирусов, троянских программ и червей;

– устройствами межсетевого взаимодействия – для объединения сетевых сегментов УЦ;

– VPN (Virtual Private Network) – для защищенного объединения распределенных компонентов УЦ, находящихся на большом расстоянии;

– UPS (Uninterruptible Power Supply) – оберегает технические компоненты УЦ от сбоев электросети;

– СУБД (Система управления базами данных) – устанавливается на тех компонентах, где расположена база данных. Необходима для работы с базами данных;

– HSM (Hardware Security Module) – для безопасного хранения корневого сертификата;

– CSP (Cryptographic Service Provider) – это специализированное программное обеспечение, предназначенное для решения криптографических задач УЦ.

ЛИТЕРАТУРА

1. Назначение удостоверяющего центра, порядок создания УЦ http://4by4.ru/ru/analytics/naznachenie-udostoveryayushchego-centra-poryadok-sozdaniya-uc

3. Межсетевой экран http://celnet.ru/firewall.php
4. VPN http://www.ip-1.ru/wiki/vpn.htm
5. UPS http://netler.ru/pc/ups.htm
6. HSM. Н. Жилкина. Ключи от царства. http://www.landmark.ru/article_folder.php?itemId=3358
7. CSP http://shipka.ru/csp.html

ПРОБЛЕМАТИКА СОВРЕМЕННЫХ СИСТЕМ МОНИТОРИНГА

А.С. Ковтун, аспирант
Научный руководитель А.А. Шелупанов, проф., д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, kas@udcs.ru

Информационно-вычислительные сети в настоящее время являются ключевыми практически в любой отрасли деятельности. С ростом возможностей сетей передачи данных растёт и сложность этих сетей. Как следствие, увеличение сложности сети повышает вероятность сбоя в составных элементах, что может повлечь за собой нежелательные последствия в виде отказа в предоставлении тех или иных услуг сетью. В связи с этим развитие эффективных методов наблюдения за состоянием элементов сети, а также создание систем, реализующих эти методы, является важной задачей. Существующие системы наблюдения за состоянием элементов сети (систем мониторинга) можно подразделить на два класса: простые системы мониторинга и системы мониторинга с прогнозированием. Для их разграничения необходимо сначала привести основную структуру любой системы мониторинга.

Состав системы мониторинга можно представить в виде трёх последовательных действий (модулей): сбор данных, анализ данных и реакция на результаты анализа. Наибольший интерес в этой системе представляет модуль анализа данных ввиду того, что сбор данных достаточно хорошо алгоритмизируется и уже существующие средства (такие протоколы, как SNMP, WMI) неплохо справляются со своей задачей, а реакция на результаты анализа сильно зависит не только от предметной области, но и частной задачи, решаемой системой мониторинга. В простых системах мониторинга анализ данных сводится, в общем случае, к проверке вхождения измеряемой величины в жёстко заданный диапазон. В случае если измеряемая величина выходит за заданный диапазон, система тем или иным путём генерирует сообщение обслуживающему персоналу. Диапазон разрешённых значений задаётся исходя из анализа наблюдаемого объекта. В некоторых случаях конфигурация системы позволяет иметь динамические верхнюю и/или нижнюю границу с целью подстраиваться под непрерывно изменяемую сеть.

Проблемой таких систем является тот факт, что реакция на выход величины из заданного диапазона следует только после установления самого факта выхода величины из диапазона, что накладывает свой отпечаток на оперативность решения проблемы обслуживающим персоналом либо системой автоматического управления сетью (СУС).

Решением этой проблемы должны стать системы мониторинга с прогнозированием. Такие системы имеют более сложный модуль анализа получаемых данных, который способен не только хранить предыдущие состояния наблюдаемого объекта, но также и анализировать эти состояния с целью предугадать поведение системы на определённый промежуток времени.

Анализ данных состоит из нескольких этапов: в первую очередь необходимо построить математическую модель наблюдаемого объекта (или объектов). После построения математической модели по накопленным данным за предыдущий период система должна решить задачу экстраполяции данных на заранее заданный промежуток времени вперёд, прогнозируя тем самым поведение системы. Дальнейшие действия системы могут быть основаны на анализе величины аберраций – отклонений реальной величины от предсказанной на определённом промежутке времени. В простейшем случае можно представить следующий алгоритм: если величина аберраций превышает определённый порог (в процентах от измеряемой величины), то это означает потенциальный сбой в наблюдаемом объекте и система посылает сигнал администратору о том, что показатели выходят за рамки предсказанных. Это ситуация, однако, может также означать штатную ситуацию, к примеру, в случае появления апериодической составляющей в измеряемых данных. Система в таком случае также пошлёт сигнал администратору, однако этот сигнал будет так называемым «ложным срабатыванием».

Такие сигналы требуют ручного отслеживания и анализа причины возникновения, чтобы понять, что он ложный. Это может отнять время у администратора. Именно ложные срабатывания являются основным недостатком систем мониторинга с прогнозированием, борьба с которыми подразумевает совершенствование как методов прогнозирования, так и методов построения моделей наблюдаемого объекта.

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ ОРГАНИЗАЦИИ НА ПРИМЕРЕ «РОСГОССТРАХ БАНКА». ПРОГРАММНЫЕ СРЕДСТВА

В.М. Козлов, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, bmpcorp9@gmail.com

В течение последних нескольких лет значительно возросла актуальность задачи обеспечения информационной безопасности в организациях банковской системы Российской Федерации. Это обусловлено и появлением ряда новых требований в области информационной безопасности, и возросшим числом угроз информационной безопасности.

Существует не так уж много стандартов информационной безопасности в банковской сфере, но те, что есть, представляют собой полный комплекс чётких требований к банковской организации и уже имеют, как правило, большой опыт внедрения и реализации их на практике [1].

Одним из таких стандартов, используемых в настоящее время в Российской Федерации, является стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС). СТО БР ИББС представляет собой комплекс документов, содержащих требования к информационной безопасности банковской организации и различные методики. В частности, стандарт содержит собственную методику оценки рисков банковской организации.

Данная методика предполагает проведение шести процедур [2]:

1. Определение типов информационных активов банковской организации – информации с реквизитами, имеющей ценность для банковской организации и находящейся в её распоряжении [3].

2. Определение перечня типов объектов среды для каждого выделенного типа актива – материальных объектов хранения, передачи, обработки, уничтожения информационного актива [3].

3. Определение перечня угроз для каждого типа объекта среды каждого информационного актива.

4. Экспертная оценка степени вероятности реализации (СВР) каждой угрозы по следующей шкале: нереализуемая (Н), минимальная (М), средняя (С), высокая (В), критическая (К).

5. Экспертная оценка степени тяжести последствий (СТП) нарушения информационной безопасности вследствие реализации угрозы по следующей шкале: минимальная (М), средняя (С), высокая (В), критическая (К).

6. Выделение на основании полученных оценок недопустимых рисков и выбор мер их уменьшения.

Данная методика была использована для анализа рисков банковской организации на примере операционного офиса «Томский» Новосибирского филиала ОАО «Росгосстрах Банк». Анализу подвергались только риски, связанные с программными средствами.

В частности, одним из выделенных в первой процедуре активов стали аутентификационные данные клиентов банка, необходимые для удалённой работы с сервисами банка.

В качестве объектов среды (связанных с программными средствами) для данного актива были выбраны данные, представленные в табл. 1.

Далее для данных объектов среды этого информационного актива были выделены угрозы, приведенные в табл. 2–4 вместе с проставленными оценками СВР и СТП.

Таблица 1

Типы объектов среды информационного актива

Уровень информационной инфраструктуры	Типы объектов среды
Уровень операционных систем и прикладных программ	Оперативная память, офисное программное обеспечение
Уровень файлов и баз данных	Файлы с информацией, содержащей коммерческую тайну

Таблица 2

Угрозы, связанные с работой браузера

Свойства ИБ	Источники угроз	Способы реализации	СВР	СТП
Конфиденциальность	Поставщики, провайдеры	Использование недекларированных возможностей браузера	Н	В
	Внутренние нарушители	Несанкционированное копирование	С	В
	Внешние нарушители	Заражение браузера или ОС вредоносным ПО	М	В
Доступность	Сбои и отказы ПО	Нарушение работы из-за внутренних ошибок и сбоев браузера	М	С
	Внешние нарушители	Заражение браузера или ОС вредоносным ПО	М	С

Таблица 3

Угрозы, связанные с работой сетевых протоколов

Свойства ИБ	Источники угроз	Способы реализации	СВР	СТП
Конфиденциальность	Провайдеры и внешние нарушители	Анализ пакетов во внешней сети	М	М
	Внутренние нарушители	Анализ пакетов во внутренней сети	М	М
Целостность	Провайдеры и внешние нарушители	Изменение пакетов во внешней сети	Н	С
	Внутренние нарушители	Изменение пакетов во внутренней сети	М	С

Таблица 4

Угрозы, связанные с оперативной памятью

Свойства ИБ	Источники угроз	Способы реализации	СВР	СТП
Конфиденциальность	Внешние нарушители	Заражение ОС вредоносным ПО	М	В
Целостность	Внешние нарушители	Заражение ОС вредоносным ПО	М	С

После выделения и оценивания угроз были выделены недопустимые риски. В частности, у данного актива недопустимым риском стало нарушение конфиденциальности внутренним нарушителем путём несанкционированного копирования данных во время ввода их в браузере. Защитной мерой в данном случае будет усиление организационных мер, например повышение ответственности за нарушение подобных правил.

Аналогично были проанализированы все остальные информационные активы банка, нарушение безопасности которых может быть связано с программными средствами. Было выявлено несколько недопустимых рисков и выбраны соответствующие защитные меры в дополнение к тем, которые уже применяются. Дальнейшая работа в банке предполагает реализацию этих защитных мер.

ЛИТЕРАТУРА

1.Все стандарты ИБ. Банки – LETA [Электронный ресурс]. Режим доступа: http://www.leta.ru/special-offers/for-banks/

2.Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности.

3.Рекомендации в области стандартизации Банка России «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

АКТУАЛЬНОСТЬ ПЕРЕХОДА К ЭЛЕКТРОННОМУ ДОКУМЕНТООБОРОТУ

Н.С. Козыренко*, *студентка 4-го курса*; *Н.С. Михайлов*, *аспирант
г. Томск, *ТУСУР*, *ФВС*, *каф. КИБЭВС*, *nattyk1991@gmail.com*

В современном обществе практически все формы взаимодействия, будь то между органами власти, или между органами государственного управления и частными лицами, или между деловыми партнерами, или в межличностных отношениях, оформляются документально.

Компьютеризация общества актуализирует задачу перехода к электронному документообороту. При этом важно, чтобы документ сохранял юридическую силу, поскольку в нем заключены документированные доказательства деловой, личной и иной деятельности, подтверждения возникновения отношений между субъектами, что может помочь при разрешении спорных вопросов.

Как правило, подлинность бумажных документов подтверждается таким неотъемлемым реквизитом документа, как собственноручная подпись. Однако п. 2 ст. 160 ГК РФ допускает использование при со-

вершении сделок электронной подписи (ЭП) либо иного аналога собственноручной подписи в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

Таким образом, существует правовая база, которая позволяет перевести документооборот организаций в электронный вид. Практическая возможность реализации этого процесса в Российской Федерации ведет свой отчет с момента подписания Федерального закона №1-ФЗ от 10.01.2002 «Об электронной цифровой подписи», а на данный момент регламентируется Федеральным законом Российской Федерации от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи».

Наиболее значимым препятствием к повсеместному применению ЭП является косность человеческого сознания. Тем не менее можно выделить наиболее перспективные сферы внедрения электронного документооборота:

– подписание юридически значимых документов;

– защита переписки пользователей;

– система сдачи отчетности в электронном виде;

– электронные торги;

– электронные платежные системы;

– получение государственных услуг в электронном виде (федеральная целевая программа «Электронная Россия», действующая до 2015 г.).

В данных сферах ЭП уже используется, но в ограниченных случаях, однако формирует хорошую основу для совершенствования необходимой нормативно-правовой базы, которая была бы прозрачна для пользователей и упрощала процессы получения сертификатов, использования и проверки электронных подписей.

Может показаться, что сохранение бумажного документооборота и рукописных подписей дешевле обеспечения всех уполномоченных лиц сертификатами ключей проверки ЭП, позволяющих формировать ЭП. С учетом несовершенства во многих случаях организации системы удостоверяющих центров, когда возникает необходимость выезда за пределы своего региона для получения сертификата ключа проверки ЭП, а также необходимости проведения организационных мероприятий внутри предприятий для исключения нарушений при использовании средств ЭП, переход к электронному документообороту действительно может составить внушительную статью расходов организации. Но при долгосрочных планах эти затраты должны окупиться.

Переход к электронному документообороту сокращает издержки, связанные с потреблением бумаги. Кроме того, были изучены официальные данные Почты России по стоимости и строкам пересылки бумажной корреспонденции [1], необходимость в которой неизбежно

возникает при установлении отношений с удаленными контрагентами, при взаимодействии с филиалами и пр. Стоимость одного отправления (от 50 руб. за одно заказное письмо и много выше в зависимости от пункта назначения) в объемах предприятия формирует значительную сумму. Более значимы сроки доставки. Даже на территории административных центров субъектов РФ гарантируемый срок доставки устанавливается в 2 дня. Пересылка корреспонденции между административными центрами субъектов РФ может достигать 11 дней. Не исключаются случаи задержек при доставке документов, которые приводят к потере актуальности последних, необходимости повторного оформления, в некоторых случаях к штрафным санкциям.

Очевидно, что передача документов в электронном виде выигрывает в скорости, сокращает время распространения управленческих решений, установления отношений с клиентами, подчиненными, дочерними организациями, что повышает эффективность работы предприятий, для коммерческих структур повышает конкурентоспособность и расширяет сферы влияния.

Помимо финансовых выгод использование ЭП вносит вклад в обеспечение информационной безопасности организаций, гарантируя защиту переписки пользователей (однозначную идентификацию участников информационного обмена, целостность передаваемой информации) [2].

Обобщая, можно выделить проблемы, которые может решить технология ЭП при использовании ее в информационных системах:

– обеспечение юридической значимости сделок, заключаемых в электронной форме;

– надежная аутентификация лиц в процессе информационного взаимодействия;

– обеспечение неотказности исполнителей документов для внутрикорпоративного делопроизводства;

– использование в качестве письменных доказательств документов в электронной форме при судебных и досудебных разбирательствах;

– обеспечение целостности и конфиденциальности информации при передаче ее в информационных системах общего пользования.

ЛИТЕРАТУРА

1. Официальный сайт Почты России. Сроки доставки [Электронный ресурс]. URL: http://www.russianpost.ru/rp/servise/ru/home/postuslug/termsdelivery (дата обращения: 1.03.2012 г.).

2. Сазонов А.В., Вусс Г.В., Кустов В.Н. Методология формирования и функционирования в сети Интренет трансграничного пространства доверия. М., 2012.

ПРИМЕНЕНИЕ ТЕСТОВ НА ПРОСТОТУ В ЗАЩИТЕ ИНФОРМАЦИИ

Д.В. Кручинин*, *аспирант
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, kdv@keva.tusur.ru

В настоящее время, в век информатизации и глобализации, человечество активно обменивается различной информацией, откуда возникает проблема целостности и конфиденциальности передаваемой информации. Поэтому защита информации от различных вредоносных действий является очень актуальным направлением. Одной из ветвей современной защиты информации являются криптографические системы с открытым ключом. Большинство таких криптосистем в качестве криптоключа используют составное число в виде произведения двух больших простых чисел.

Наиболее известной и часто применяемой криптосистемой с открытым ключом является алгоритм RSA, названный по первым буквам фамилий своих изобретателей – Ривеста (Rivest), Шамира (Samir) и Адлемана (Adleman) [1]. Криптосистема RSA – первая практическая реализация криптографии с открытым ключом на основе понятия однонаправленной функции с секретом, предложенного Диффи и Хеллманом [2].

Основу криптографической системы с открытым ключом RSA составляют практические трудности решения задачи о разложении чисел на множители (задача факторизации), которая является вычислительно однонаправленной задачей.

При использовании криптосистемы RSA каждому пользователю необходимо выработать свою пару открытых и секретных ключей. Процесс генерации ключей начинается с выбора двух больших простых чисел (p, q). Для этого с помощью генератора случайных чисел находится произвольное нечётное число требуемой разрядности. Далее определяется, является ли число простым, при помощи того или иного теста на простоту. Если тест на простоту отрицателен, то выбирается следующее случайное число, выдаваемое генератором случайных чисел. Далее вычисляется произведение этих двух простых чисел $n = pq$. Затем требуется взять случайное число e, взаимно простое с $\varphi(n)=(p-1)(q-1)$, и найти число d из условия $ed \equiv 1(\mathrm{mod}\,\varphi(n))$. Пара (n,e) объявляется открытым ключом и помещается в открытый каталог. Остальные числа $(p,q,\varphi(n),d)$ образуют секретный ключ. Для расшифровки достаточно знать пару (n, d). Поскольку успешное решение задачи факторизации (разложения) числа n позволяет полностью дешифровать схему RSA и определить секретный ключ, то выбор про-

стых чисел p и q во многом определяет стойкость шифрования. Более того, задача проверки произвольного числа на простоту в значительной степени определяет и скорость генерации криптоключей RSA [3].

Сегодня существует достаточно много способов определения простоты заданного числа, так называемых тестов на простоту. Все существующие можно разделить на следующие 2 большие группы: детерминированные и вероятностные тесты. Детерминированные тесты на простоту однозначно определяют, является ли заданное число простым или составным. Вероятностные тесты на простоту определяют является ли число простым с некоторой вероятностью, обычно при неоднократном повторении теста вероятность ошибки значительно уменьшается. Вероятностные тесты порой называют тестами на композитность (составность), поскольку если число не удовлетворяет условиям теста, то оно однозначно составное; если же удовлетворяет, то не обязательно оно простое.

Наиболее часто используемым тестом на простоту является вероятностный тест Рабина–Миллера [4]. Например, данный тест используется в вышеупомянутой криптосистеме RSA при генерации ключей.

В основе теста Рабина–Миллера лежит следующий критерий.

Число n называется сильно псевдопростым по основанию a, если выполняется условие: $a^t \equiv 1 (\mathrm{mod} n)$ или $\exists r, 0 \le r < s, a^{2^r t} \equiv -1 (\mathrm{mod} n)$.

Под псевдопростым числом понимается число, удовлетворяющее условиям теста при определенных значениях a. После повторения данного теста k раз при различных значениях a вероятность неотбраковки составного числа не превосходит $(1/4)^k$, но все же существует. Использование существующих детерминированных тестов на простоту нецелесообразно ввиду их большой вычислительной трудоемкости. Поэтому поиск качественного и быстрого теста на простоту заданного числа остается актуальной задачей не только в математике, но и в области криптографической защиты.

ЛИТЕРАТУРА

1. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and publickey cryptosystems // Communications of the ACM. 1978. Feb. Vol. 21, №2. P. 120–126.

2. Венбо Мао. Современная криптография: теория и практика. М.: Вильямс, 2005. 768 с.

3. Балабанов А.А., Агафонов А.Ф., Рыку В.А. Алгоритм быстрой генерации ключей в криптографической системе RSA // Вестник научно-технического развития. 2009. № 7 (23). С. 11–17.

4. Ященко В.В., Варновский Н.П., Нестеренко Ю.В. и др. Введение в криптографию / Под общ. ред. В.В. Ященко. М.: МЦНМО, 2000. 272 с.

ПРОЦЕСС АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

А.И. Кураленко, аспирант каф. РЗИ
г. Томск, ТУСУР, alkur@sibmail.com

С каждым днем все больше руководителей понимают необходимость обеспечения безопасности информации, циркулирующей внутри организации. Вызвано это, как правило, необходимостью защитить свои информацию, ведь нарушение конфиденциальности, целостности и доступности информации может привести к серьезным финансовым потерям организации, пострадает репутация, может нарушиться нормальный режим функционирования.

На сегодняшний момент проблема защиты информации решается путем создания в организации системы обеспечения информационной безопасности (далее – СОИБ). СОИБ должна функционировать в течение всего времени существования организации. СОИБ, как и любая система, в процессе своего функционирования нуждается в модернизации, периодических проверках работоспособности, целью которых является выявление уязвимых мест в системе, через которые возможна реализация угроз безопасности. И по результатам такой проверки даются рекомендации для дополнения, модернизации существующей системы защиты. Данный процесс возможен как на начальном этапе функционирования, так и в течение всего жизненного цикла СОИБ. Это процесс называется аудитом информационной безопасности (далее – ИБ).

Аудит ИБ – это периодический, независимый и документированный процесс получения свидетельств и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению ИБ [1]. Различают внешний и внутренний аудит. Внешний аудит – это, как правило, разовое мероприятие, проводимое по инициативе руководства организации. Внутренний аудит представляет собой деятельность, которая осуществляется в соответствии с планом (политикой безопасности организации), подготовка которого утверждается руководством организации.

Целями проведения аудита безопасности являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов СОИБ;
- оценка текущего уровня защищенности СОИБ;
- локализация узких мест в СОИБ;
- оценка соответствия СОИБ существующим стандартам в области ИБ;

• выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов СОИБ.

Аудит ИБ включает в себя следующие процедуры:

• инициирование процедуры аудита;
• сбор информации аудита;
• анализ данных аудита;
• выработка рекомендаций;
• подготовка аудиторского отчета.

Аудит инициируется руководством организации. Аудит представляет собой комплекс мероприятий, в которых участвуют подразделения организации. Поэтому на этапе инициирования процедуры аудита должны быть решены организационные вопросы взаимодействия подразделений с аудиторами и между собой. Также определяются границы проводимого аудита.

Этап сбора информации включают в себя сбор всей необходимой информации о СОИБ, в которой проводится аудит ИБ. Количество собираемой информации о системе определяется глубиной аудита ИБ. Данный этап является трудоемким, так как детально разбираются все процедуры и функции СОИБ.

Анализ данных аудита ИБ. Методы анализа данных определяются выбранными подходами к проведению аудита.

Первый подход базируется на анализе рисков. Опираясь на методы анализа рисков, аудитор определяет для обследуемой СОИБ индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной системы, среды ее функционирования и существующие в данной среде угрозы безопасности.

Второй подход опирается на использование стандартов информационной безопасности (ISO/IEC 27001, Cobit, ISO 17799 т.п.). Стандарты определяют базовый набор требований безопасности для широкого класса систем, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности СОИБ, который требуется обеспечить.

Третий подход предполагает комбинирование первых двух. Базовый набор требований безопасности, предъявляемых к СОИБ, определяется стандартом. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной системы, формируются на основе анализа рисков.

Рекомендации, выдаваемые аудитором по результатам анализа состояния защищенности СОИБ, определяются используемым подходом, особенностями обследуемой системы, степенью детализации, исполь-

зуемой при проведении аудита ИБ. Рекомендации аудитора должны быть конкретными и применимыми к данной СОИБ, экономически обоснованными, аргументированными и отсортированными по степени важности. Аудиторский отчет является основным результатом проведения аудита ИБ. Его качество характеризует качество работы аудитора. Аудиторский отчет должен содержать описание целей проведения аудита ИБ, характеристику обследуемой СОИБ, указание границ проведения аудита и используемых методов, результаты анализа данных аудита, выводы, обобщающие эти результаты и содержащие оценку уровня защищенности системы или соответствие ее требованиям стандартов, и, конечно, рекомендации по устранению существующих недостатков и совершенствованию СОИБ [2].

С помощью аудита ИБ можно определить текущий уровень защищенности СОИБ организации как на этапе развертывания системы, так и на протяжении всего времени работы. Это позволит дать соответствующие рекомендации по устранению уязвимых мест в системы защиты организации, предотвратить угрозы утечки информации, избежать финансовых потерь организации.

ЛИТЕРАТУРА

1. ГОСТ Р 50922-2006 «Защита информации. Термины и определения».
2. Курило А.П. Аудит информационной безопасности. М.: БДЦ-пресс, 2006. 304 с.

ВНЕДРЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА ЗАЩИТЫ «SPECTOR 360»

А.Н. Кузьменко*, *студент
г. Томск, *ТУСУР*, *ФВС*, *каф. КИБЭВС asd@mail.ru*

Информационная безопасность предприятия, независимо от рода деятельности организации, размеров денежных оборотов, а также принадлежности к субъектам малого и крупного предпринимательства, строится, прежде всего, на понимании структуры информатизации. Работа по информационному обеспечению в современном технологичном мире является приоритетным направлением, т.к. позволяет «держать руку на пульсе» всех бизнес-процессов, а также обеспечивать оперативность потоков информации, поступающих или исходящих, что увеличивает эффективность ведения бизнеса. Ввиду этих факторов содержание отделов информатизации (в каждом предприятии наименования подразделений могут разниться, но суть остается одинаковой) – одно из важнейших направлений развития предприятия любого рода деятельности, которое стремится к совершенствованию

своих процессов, смотрит в завтрашний день. Чем эффективнее работают ваши информационные процессы, тем эффективнее ваш бизнес.

Однако в растущем информационном обществе, где давно уже установилось правило: «Кто владеет информацией, тот владеет миром», можно говорить о том, что именно информационные процессы приобретают и определяют ценность. Ценность выражается в том, что вы получаете некое преимущество, которое позволяет вести конкурентную борьбу, оперативно реагировать на изменения. Именно поэтому эффективности функционирования, поддержки, модернизации информационных процессов уделяется большое внимание, выделяются соответствующие бюджеты, которые измеряются не в тысячах и не в сотнях тысяч денежных единиц, а в миллионах. Можно даже говорить о некой моде на информатизацию.

Растущая ценность информации влечет соответствующие риски. Наряду с незаконным изъятием денежных средств из банка, в век информационного общества осуществляется «кража» информации, которая материализуется в дальнейшем путем получения преимущества или прямой выгоды. Информация становится финансовым инструментом. Поэтому помимо самой информатизации необходимо уделять внимание и защите информации. Построение эффективных систем информационной безопасности, определяющих саму информатизацию бизнеса организаций (для снижения рисков утечки информации, ее искажения и т.д.), становится не менее важным направлением и даже более весомым при построении информационных систем (ИС). Следует учитывать максимально возможное количество рисков при построении таких систем не в ущерб функционированию.

Системы защиты информации должны учитывать не только явно возможные каналы утечки, искажения информации, а также охватывать косвенные. Внимание следует уделять построению защиты, ориентированной на угрозы извне, а также и на угрозы изнутри. Эффективность всей системы определяется эффективностью самого слабого звена. Несомненно, таким звеном всегда будет являться человеческий фактор. Именно ему необходимо уделять больше внимания при разработке, внедрении и сопровождении всех систем. Одним из главных рисков становится сам человек – сотрудник, так называемый инсайдер. Инсайдер умышленно или неумышленно может осуществлять деятельность по искажению, уничтожению информации, циркулирующей при информационных процессах.

В ходе осуществления работ было принято решение о выполнении должностных обязанностей сотрудника компании ФСК ЕЭС МЭС Западной Сибири службы ИТС отдела информатизации по осуществлению мероприятий, направленных на поддержание работоспособности

существующих информационных систем, ознакомление со структурой службы ИТС, структурой информационных систем, потоков информации, циркулирующих в системе. Выполнение должностных обязанностей способствовало осуществлению мероприятий, проводимых при внедрении программного комплекса «SPECTOR 360» для мониторинга действий сотрудников и внутренних расследований.

ЛИТЕРАТУРА

1. Официальный сайт компании представителя в России «SpectorSoft» [Электронный ресурс]. Режим доступа: http://www.headtechnology.ru

2. Официальный сайт компании «SpectorSoft» [Электронный ресурс]. Режим доступа: http://www.spectorsoft.com

3. Официальный сайт продукта «SPECTOR 360» [Электронный ресурс]. Режим доступа: http://www.spector360.com

ОЦЕНКА ЭФФЕКТИВНОСТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МЕТОДОВ ТЕОРИИ ГРАФОВ

А.С. Лукьянов, преподаватель каф. инфокоммуникационных систем и технологий, к.т.н.;

А.О. Авсентьев, адъюнкт каф. информационной безопасности

г. Воронеж, Воронежский институт МВД России, las92@yandex.ru

Современный период развития цивилизованного общества характеризует процесс информатизации. Результатом этих бурных процессов, охватывающих все сферы общественных и производственных отношений, является постепенный переход развитых стран мира к постиндустриальному «информационному обществу», которое характеризуется обилием информации, циркулирующей по коммуникационным каналам связи, а также наличием всех необходимых средств для ее хранения, передачи, обработки и использования. В связи с этим широкое применение получают информационные системы (ИС), которые имеют оценки эффективности их функционирования. Среди показателей эффективности важное место занимает оценка целостности информации.

Под целостностью информации понимается состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [1].

В качестве числовой характеристики показателя целостности можно принять $C = \begin{cases} 1, & \text{если целостность сохранена,} \\ 0, & \text{если целостность нарушена.} \end{cases}$

Решение любой задачи по обеспечению защиты информации может быть осуществлено только на основе информации о защищаемом объекте. Для описания объектов, представляющих собой множества с заданными на них отношениями, используются методы теории графов. Представим структуру ИС с помощью ориентированного графа так, что вершины соответствуют узлам $V=\{v_1,v_2,...,v_n\}$ – множество элементов (узлов), а дуги – каналам связи $E=\{e_1,e_2,...,e_m\}$, где $e_i=(v_{i_1},v_{i_2}),i=\overline{1,m}$ – множество бинарных отношений (линий связи) между элементами ИС. Тогда $G=(V,E)$ – граф, представляющий собой фрагмент структурной модели ИС. Будем считать, что отношение E в общем случае не является симметричным, поэтому G – ориентированный граф (рис. 1).

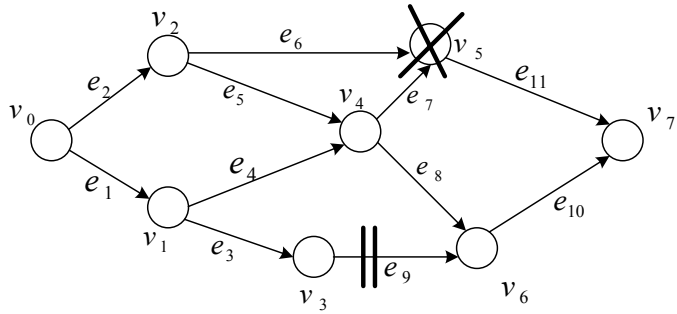


Рис. 1. Модель ИС, представленная в виде графа

В момент передачи информации с помощью ИС ее узлы и каналы связи могут выходить из строя как от умышленного воздействия на них, так и вследствие естественных причин. Исходя из определения будем считать, что целостность сохраняется, если остается хотя бы один маршрут ее передачи из начального узла в конечный. На языке теории графов это означает, что существует путь между вершинами, моделирующими указанные узлы.

Рассмотрим пример. Пусть фрагмент ИС моделируется с помощью графа, изображенного на рис. 1. Требуется осуществить передачу информации из узла, моделируемого вершиной v_0, в узел, моделируемый вершиной v_7. Предположим, что узел v_5, канал связи между узлами v_3 и v_6 повреждены.

Используем для проверки существования пути алгоритм поиска в ширину. Для этого можно реализовать схему, аналогичную методу поиска кратчайшего пути [2] (веса дуг будем считать единичными),

предполагая осуществление пометок вершин. Если вершина v_7 получила окончательную ненулевую пометку, то, следовательно, путь между v_0 и v_7 существует. Результаты решения задачи для рассматриваемого примера приведены в таблице.

Результаты решения

Шаг	Вершина							
	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7
0	0	∞	∞	∞	∞	∞	∞	∞
1		1	1	∞	∞	∞	∞	∞
2				2	2	∞	∞	∞
3							3	∞
4								4

Таким образом, искомый путь существует и, следовательно, можно говорить о сохранении целостности информации, т.е. C = 1.

ЛИТЕРАТУРА

1. Специальные требования и рекомендации. Информационная технология. Основные термины и определения в области технической защите Р 50.1.053. 2005.

2. Практические задания по дискретной математике: учеб. пособие / В.В. Меньших, О.В. Пьянков. Воронеж: Воронежский институт МВД России, 2007. 155 с.

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ОТНОШЕНИЯМИ С КЛИЕНТАМИ В СЕТЕВОМ МАРКЕТИНГЕ

А.С. Лыбина, М.Ю. Пьянкова,
Е.М. Толстокулакова, студентки 5-го курса ФСУ
Научный руководитель М.В. Григорьева, доцент каф. АСУ
г. Томск, ТУСУР, alexsmile31@mail.ru

В настоящее время многие сетевые компании имеют сайты, которые содержат информацию о реализуемой продукции и предоставляют возможность о контроле работы дистрибьюторов компании. Данные сайты поддерживают именно работу компании, но не дистрибьютора.

Поэтому было принято решение о создании CRM-системы, автоматизирующей работу дистрибьютора. Система «Дистрибьютор» была декомпозирована на 4 подсистемы [1]. В рамках данной статьи представлена подсистема «Работа с контактами».

Данная подсистема предназначена для ведения учета клиентов и контактов с ними, учета задач, составления расписания, оформления договоров и учета распределения обучающего материала. Входами для функционирования этой подсистемы являются данные о потенциаль-

ных клиентах, факт контакта, факт наличия обучающего материала. Дистрибьютор под воздействием управляющей информации о событии, правилах ведения бизнеса и существующих обучающих материалов формирует списки покупателей и дистрибьюторов, расписание, отчет о наличии обучающего материала, рассчитывает оценки эффективности контакта и оформляет договоры.

Декомпозиция данной подсистемы представлена на рис. 1 в виде контекстной SADT-диаграммы уровня A1.

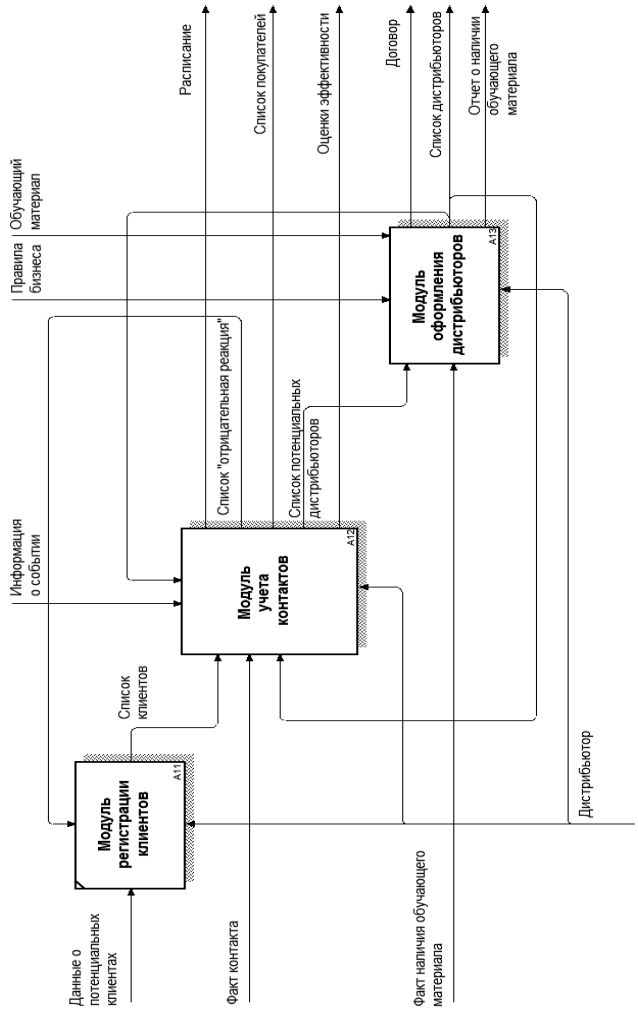


Рис. 1. Декомпозиция подсистемы «Работа с клиентами»

Как мы видим, подсистема состоит из трех модулей:

1. *Модуль регистрации клиентов.* На основании данных о потенциальных клиентах, исключая тех, кто ранее проявил негативную реакцию, дистрибьютор формирует список клиентов.

2. *Модуль учета контактов*. На основании списка клиентов, списка дистрибьюторов и факта контакта дистрибьютор планирует контакт, обрабатывает результаты контакта и оценивает его эффективность. Из модуля выходят расписание, список клиентов с отрицательной реакцией, список покупателей, список потенциальных дистрибьюторов и оценки эффективности контакта.

3. *Модуль оформления дистрибьюторов*. Дистрибьютор оформляет договоры и учитывает распределение обучающего материала. На входе в модуль-список потенциальных дистрибьюторов, факт наличия обучающего материала. На выходе – договоры, список дистрибьюторов и отчет о наличии обучающего материала.

Модуль учета контактов решает следующие задачи:

1. Планирование контакта. Коммуникационная деятельность дистрибьютора включает информационные встречи с клиентами, презентации продукции, рабочие встречи или так называемые «школы бизнеса», открытые встречи, различные семинары, звонки, приглашения. На основании имеющихся списков клиентов дистрибьютор планирует контакт, учитывая информацию о событии. На выходе он получает расписание и информацию о предстоящем контакте, содержащую дату, время, место и список приглашенных клиентов.

2. Обработка результатов контакта. После осуществления контакта дистрибьютор проводит анализ изменения стадий взаимоотношений с клиентами.

3. Оценка эффективности контакта. Предусмотрена возможность оценки эффективности контакта по совокупности следующих показателей: количество клиентов, изменение стадий взаимоотношения с покупателями, отношение количества потерянных покупателей к общему количеству клиентов (коэффициент удержания покупателей), количество появившихся заказов покупателей.

Декомпозиция модуля представлена на SADT-диаграмме на рис. 2.

В *модуле оформления дистрибьюторов* происходит заключение договора на основании бизнес-правил компании, а также ведется учет наличия обучающего материала.

Итак, проведя анализ информационной модели, бизнес-процессов, функционального состава ИС на предмет выявления информации и данных, которые будут храниться в базе данных, была создана концептуальная модель системы. Итогом является конфигурация в «1С: Предприятие», схема метаданных которой представлена на рис. 3.

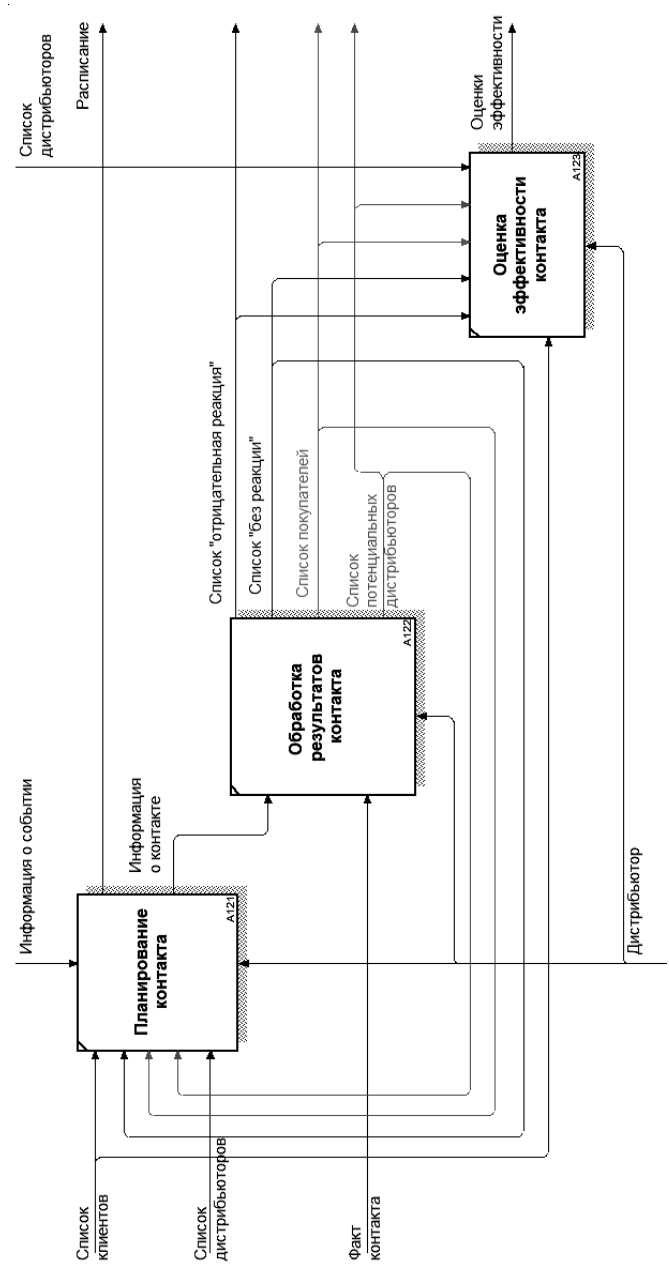


Рис. 2. Декомпозиция модуля учета контактов

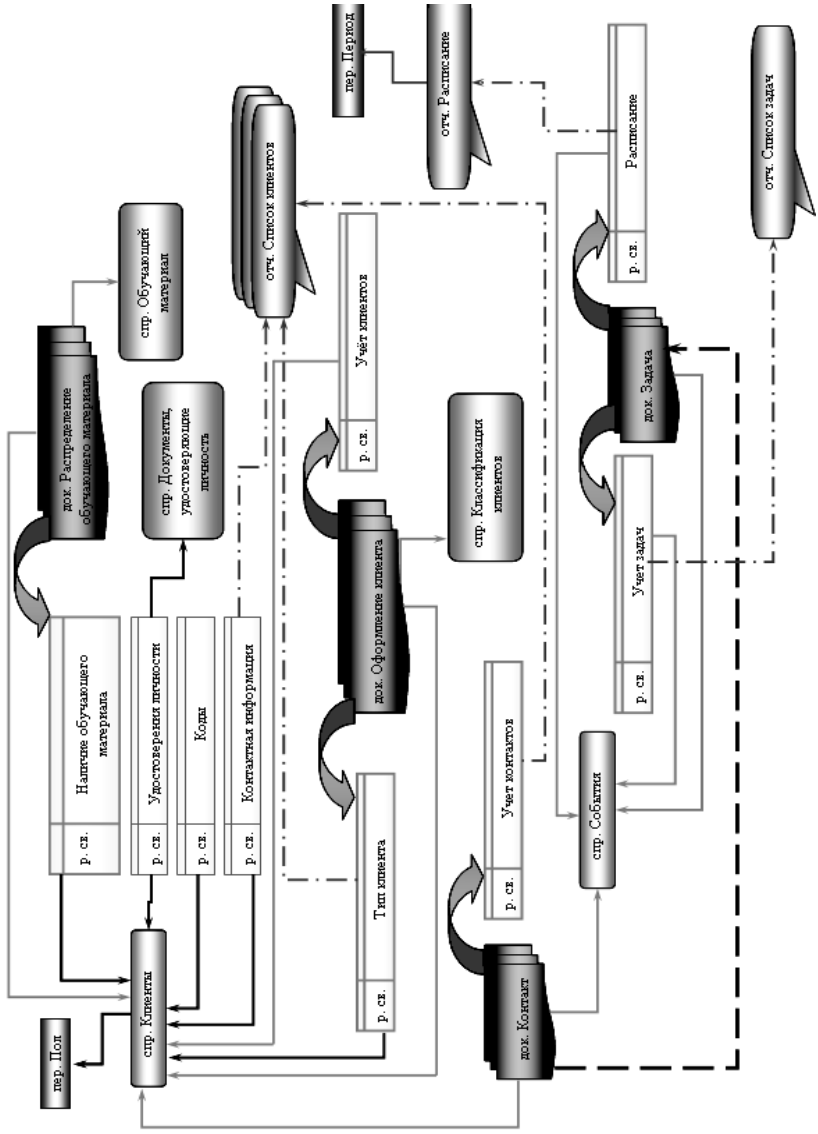


Рис. 3. Схема метаданных конфигурации

ЛИТЕРАТУРА

1. Григорьева М.В. Сетевые технологии в экономике прямых продаж и их автоматизация // Доклады ТУСУРа. 2011. №1 (23). Июнь. Томск: Том. гос. ун-т систем упр. и радиоэлектроники, 2011. С. 131–136.

РАЗРАБОТКА СИСТЕМЫ КЛАССИФИКАЦИИ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

И.Е. Макаров, студент 5-го курса каф. ИБ
г. Новосибирск, НГУЭУ, ИПИ, makfess@gmail.com

В современном мире информационных технологий средства антивирусной защиты стали одним из наиболее важных компонентов системы защиты информации на предприятии по причине того, что вредоносные программы являются одним из наиболее распространенных и часто встречающихся видов угроз. Рассмотрим, какие законодательные акты регулируют использование средств антивирусной защиты.

1. Специальные требования и рекомендации по технической защите конфиденциальной информации. В данном документе рекомендуется использовать средства антивирусной защиты, в случае если ваша система подключена к сети международного обмена.

2. Приказ ФСТЭК России от 5.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных». Данный документ указывает на обязательное использование средства антивирусной защиты в том случае, если ваша ИСПДн подключена к сети международного обмена.

3. Стандарт банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» от 21.06.2010. Данный документ требует установить и настроить средства антивирусной защиты на всех рабочих местах и серверах автоматизированной банковской системы, для которых это предусмотрено технологическим процессом, и рекомендует использование средств антивирусной защиты разных производителей.

Средства антивирусной защиты могут и должны получать сертификаты ФСТЭК России, для того чтобы их использование стало возможным для защиты, к примеру, сведений в ИСПДн К3 или выше. В 1998 г. Гостехкомиссия при Президенте Российской Федерации (нынешняя ФСТЭК России) разработала проект руководящего документа «Антивирусные средства. Показатели защищенности и требования по защите от вирусов», но документ так и не был закончен, а собранные тогда данные полностью устарели за четырнадцать лет в динамически меняющемся мире информационных технологий. Целью данной работы является разработка методики формирования требований к системам антивирусной защиты. Данная методика предназначена для упрощения процесса выбора средства антивирусной защиты в процессе построения системы защиты информации на предприятии. Методика будет являться базой для разработки информационно-справочной системы, помогающей при выборе средства антивирусной защиты. При

формировании ответа информационно-справочная система будет руководствоваться такими показателями, как данная методика, количество рабочих станций, файловых серверов, шлюзов и почтовых клиентов, расположенных в организации, системными требованиями средств антивирусной защиты, а также их стоимость для наиболее точного выбора с точки зрения техноэкономического обоснования.

Данная методика и информационно-справочная система, основанная на ней, не будут рассматривать сведения, составляющие государственную тайну.

При разработке концепции классификации средств антивирусной защиты использовался руководящий документ от 25.07.1997 «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Данный документ использовался ввиду его концептуальной схожести с разрабатываемой методикой.

Для проведения классификации средств антивирусной защиты используется деление на четыре класса:

Q – средства антивирусной защиты, обеспечивающие безопасность рабочих станций;

W – средства антивирусной защиты, обеспечивающие безопасность почтовых серверов;

E – средства антивирусной защиты, обеспечивающие безопасность файловых серверов;

R – средства антивирусной защиты, обеспечивающие безопасность интернет-шлюзов.

Каждый из классов подразделяется на четыре группы:

1 – для защиты сведений в ИСПДн класса К1;

2 – для защиты сведений в ИСПДн класса К2;

3 – для защиты сведений в ИСПДн класса К3;

4 – для защиты сведений в ИСПДн класса К4 и сведений конфиденциального характера.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕРВИС-ОРИЕНТИРОВАННОЙ АРХИТЕКТУРЫ (SOA)

К.А. Нечаев*, *студент 5-го курса; Д.Д. Зыков*, *доцент
г. Томск, *ТУСУР*, *ФВС*, *каф. КИБЭВС, akadelpher@gmail.com*

Сервис-ориентированная архитектура (в дальнейшем – SOA, service-oriented architecture) является модульным подходом в разработке программного обеспечения (ПО). Данный подход основан на ис-

пользовании сервисов со стандартизованными интерфейсами. SOA является парадигмой организации и использования распределенных возможностей, которые могут находиться под контролем различных доменов [1]. В общем случае под сервис-ориентированной архитектурой понимают такую организацию приложения, при которой информационные ресурсы доставляются потребителям посредством сетевых сервисов.

Примерами сервисов могут являться такие узлы, как сервис складских операций, сервис управления сотрудниками, сервис взаимодействия с системами, изначально не разрабатываемые с целью использования в сервис-ориентированной среде. Сервисы принимают запросы и возвращают результат. Главная особенность этого процесса заключается в том, что с точки зрения клиента архитектура не должна быть привязана к определенной технологии.

Если при разработке архитектуры SOA с самого начала сконцентрироваться на использовании традиционных механизмов обеспечения безопасности, таких как межсетевые экраны, системы обнаружения вторжений и мониторинг безопасности, добиться обеспечения информационной безопасности будет достаточно сложно. Дело в том, что чем больше признаков SOA архитектуры имеет разрабатываемая система, тем слабее её безопасность. Сложность традиционной (не-SOA) системы часто прячет от посторонних глаз множество ошибок реализации, усложняя лицам, пытающимся нанести ущерб системе, их обнаружение. А при их обнаружении может оказаться, что получаемые данные трудно пригодны для анализа.

Данная архитектура подразумевает публичный доступ к сервисам, практически делая невозможным защиту с помощью межсетевых экранов, путем предоставления не только точек входа в сервисы, но и подробного описания языка запросов к сервисам (WSDL). Это предоставляет злоумышленникам более простую архитектуру, которую проще скомпрометировать.

Для того чтобы адаптировать существующие методы обеспечения информационной безопасности, были разработаны спецификации и ряд стандартов, называемых WS-Security (Web-Service Security, безопасность Web-сервисов), призванных обобщить методы защиты Web-сервисов.

WS-Security описывает способ обеспечения безопасности Web-сервисов не на транспортном уровне (как это делается в HTTPS), а на уровне сообщений.

WS-Security определяет механизм добавления трех уровней обеспечения безопасностей сообщений, передаваемых Web-сервисами: токены аутентификации, шифрование XML, цифровые подписи XML-

документов. Стандарт не обязывает использование конкретных типов токенов, шифрования и цифровых подписей, но предоставляет способы по стандартизованному использованию этих алгоритмов в сообщениях, передаваемых сервисами. Так как вся информация, связанная с безопасностью, хранится в теле зашифрованного сообщения, необходимость в защите каналов передачи (например, использование протокола HTTPS) сообщений отпадает. Сообщения будут защищены, если они передаются по открытому каналу HTTP, в сообщении электронной почты, на CD-диске и т.д.

Стандарт WS-Federation [2] расширяет возможности WS-Security, обобщая ряд других стандартов (WS-Trust, WS-SecurityPolicy). Эти спецификации определяют механизмы для кодификации утверждений о клиенте как токены безопасности, которые могут быть использованы для защиты и авторизации запросов веб-сервисов в соответствии с политикой безопасности.

На рис. 1 изображено представление модели сервиса токенов безопасности, определенной в WS-Trust. Каждая стрелка представляет возможное взаимодействие между участниками. Каждый участник имеет собственные политики, которые комбинируются для того, чтобы определить токены безопасности и ассоциированные утверждения, требуемые для взаимодействия по определенному пути. С точки зрения клиента поток взаимодействия начинается с идентификации Web-сервиса или провайдера ресурса, к которому клиент хочет получить доступ. Клиент спрашивает провайдер ресурсов о его политиках для определения требований безопасности.

Рис. 1. Модель сервиса токенов безопасности

Используя выражения WS-SecurityPolicy, клиент может проверить, имеет ли он токен безопасности, который соответствует требованиям для доступа к провайдеру ресурса. Если клиент не имеет необходимого токена, он может запросить его у соответствующего сервиса токенов безопасности, который может быть определен в политике про-

вайдера ресурсов. Каждый сервис токенов безопасности имеет собственную ассоциированную политику и является Web-сервисом, клиент может запросить требования безопасности на запрос определенного типа токена для использования.

Таким образом, основная цель этих спецификаций состоит в обеспечении общей инфраструктуры для выполнения операций аутентификации и авторизации участников информационного обмена в сервис-ориентированной архитектуре. Общий протокол обеспечивает экономию в разработке, тестировании, интеграции и сопровождении защищенных продуктов для поставщиков и клиентов.

ЛИТЕРАТУРА

1. Reference Model for Service Oriented Architecture 1.0 [Электронный ресурс]. Версия спецификации 1. 2 августа 2006 г. Режим доступа: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm

2. Web Services Federation Language (WS-Federation) [Электронный ресурс]. Режим доступа: http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-Federation-V1-1B.pdf?S_TACT=105AGX04&S_CMP=LP

БЕЗОПАСНОСТЬ СИСТЕМ ПЛАТЕЖЕЙ VISA, MASTERCARD

Т.В. Остапчук, студентка 5-го курса;
М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, littletanchik@mail.ru

Пластиковая карта – один из самых динамично развивающихся инновационных банковских продуктов во всем мире, с каждым годом обнаруживаются новые возможности использования данного инструмента расчетов. Основная функция пластиковой карточки – обеспечение идентификации использующего ее лица как субъекта платежной системы.

Сейчас на долю американских платежных систем Visa и Mastercard приходится 85% платежей в России по пластиковым картам. Данные системы позволяют осуществлять разного рода финансовые операции как в банкоматах и магазинах, так и в сети Интернет.

Использование банковских карт для платежей в сети Интернет предполагает использование самых передовых технологий осуществления транзакций, доступных лишь банкам и крупным международным финансовым учреждениям. Остановимся немного на аспектах безопасности использования банковских карт, точнее, на двух решениях в области безопасности транзакций:

- трехзначный код безопасности CVV2 или CVC2;
- протокол 3-D Secure.

Card Verification Value 2 [1] (CVV2 для Visa International) и Card Verification Code 2 (CVC2 для MasterCard Worldwide) – это трёхзначный цифровой код для проверки подлинности карты платёжной системы, сгенерированный по специальному алгоритму. Наносится код на полосу для подписи держателя после номера карты либо после последних 4 цифр номера карты способом индент-печати. По своей сути CVV2 и CVC2 ничем не отличаются, но тем не менее имеют разные названия. Данный код – это самостоятельный элемент, то есть он не является продолжением номера банковской карты. Его, в отличие от ПИН-кода, нельзя никак поменять, кроме как перевыпустить карту. На практике данный код выступает как защитный элемент при осуществлении транзакций в среде CNP (card not present).

Для того чтобы подтвердить аутентичность предъявителя данных карты в сети, в настоящее время рассматриваются другие возможности, прежде всего связанные с получением некоего кода или запроса другим способом, заранее согласованным законным держателем карты и банком. Например, использование разового пароля, полученного в банкомате или посредством SMS, подтверждение транзакции в системе интернет-банкинга банка-эмитента карты или на отдельном защищённом сайте.

3-D Secure [2] – это протокол обработки интернет-транзакций, разработанный Visa и одобренный MasterCard. Он предназначен для обеспечения безопасности интернет-платежей, выполняемых с использованием кредитных или дебетовых карт. Услуги, основанные на данном протоколе для Visa – Verified by Visa и для MasterCard – MasterCard SecureCode.

Модель 3-D Secure реализована на основе 3 доменов, в которых происходит проверка транзакций:

- домен эмитента;
- домен эквайера;
- домен взаимодействия.

Каждый домен является важной частью процесса передачи информации в общей 3-D Secure-инфраструктуре. Для каждого домена определена собственная сфера ответственности в проведении транзакций:

- в домене эмитента банк-эмитент ответственен за аутентификацию покупателя и предоставление верной информации для проведения транзакции;
- в домене эквайера онлайн-продавец ответствен за коммерческие отношения с покупателем, а также гарантию того, что покупатель был направлен в верный банк-эмитент для верификации. В этом же домене эквайер несёт ответственность за согласование проведения транзакции через традиционные сети Visa или MasterCard;

– в домене взаимодействия платежная система Visa или MasterCard ответственна за сохранность информации по каждому эмитенту (банк держателя карты, интернет-адрес эмитента) и предоставление данной информации для вынесения решения в случае конфликтных ситуаций.

При оплате покупки по технологии 3D Secure аутентификация держателя карты осуществляется на специальном сервере банка-эмитента, выпустившего карту. Для аутентификации клиента требуется пароль, выданный держателю карты банком-эмитентом. Таким образом, в случае платежа с использованием 3DS организация электронной коммерции (интернет-магазин) не будет нести ответственность в результате мошеннических операций, так как аутентификация держателя карты происходит на стороне банка-эмитента. Технология 3D Secure, по утверждению международных платежных систем Visa Int. (Verified By Visa) и MasterCard Worldwide (SecureCode), является наиболее безопасной из всех существующих, а это, безусловно, влияет на конкурентоспособность интернет-магазинов и лояльность картодержателей.

ЛИТЕРАТУРА

1. Visa Card Verification Value 2 – CVV2 // UniBul merchant services URL: https://www.unibulmerchantservices.com/visa-card-verification-value-2-cvv2/ (дата обращения: 05.03.12).

2. Протокол 3-D Secure // Computel URL: http://www.computel.ru/decision/ssb/thales/3dsecure/ (дата обращения: 05.03.12).

СЕГМЕНТАЦИЯ РЕЧЕВОГО СИГНАЛА

Р.В. Петриченко*, *студент 5-го курса

г. Томск, *ТУСУР*, *ФВС*, *каф. КИБЭВС, roman-vp@rambler.ru*

В настоящее время для практически любых исследований в области распознавания либо синтеза речи необходим качественный и объемный отсегментированный речевой корпус. Логично, хотя и трудоемко, использовать ручную сегментацию [1]. Первоначально необходимо обеспечить базовые функции хранения и редактирования сегментации.

Для использования данных ручной сегментации минимально необходимо хранить транскрипцию каждого звука, его время начала и окончания [2]. Хранимый объем информации можно уменьшить, используя в качестве времени завершения участка время начала следующего. Это возможно благодаря тому, что вся звуковая запись поделена на сегменты непрерывно. Если на каком-либо участке не наблюдается

речь, то используется транскрипция «(пауза)». Пример получившейся структуры хранения данных сегментации представлен на рис. 1.

	1	…	n-1	n	
массив транскрипций	к	…	м'	им2	
массив времени	0	…	60.58	60.64	60.71

Рис. 1. Упрощенная структурная схема

Элементу с номером n–1, соответствует транскрипция «м'», время начала сегмента 60.58 и время окончания 60.64.

Важным является сохранение логической целостности сегментации. Ее нарушения возможны при изменении описания элемента и добавлении нового. Проще говоря, сегменты должны быть представлены в памяти в том же порядке, в котором они представлены на временной шкале.

На операцию изменения описания участка сегментации достаточно наложить ограничение, позволяющее задавать значение времени начала сегмента только в границах от начала предыдущего элемента до начала последующего.

Для удовлетворения поставленных нами ограничений при добавлении нового сегмента необходимо расположить его соответственно времени начала звучания. Эта задача была решена простым алгоритмом: Элементы, находящиеся на временной шкале до добавляемого остаются на своих местах, а после – сдвигаются на 1.

Для наглядности была добавлена возможность отображения сегментации на различных графиках (осциллограмма, результат маскировки и т.д.). Пример работы графического модуля представлен на рис. 2.

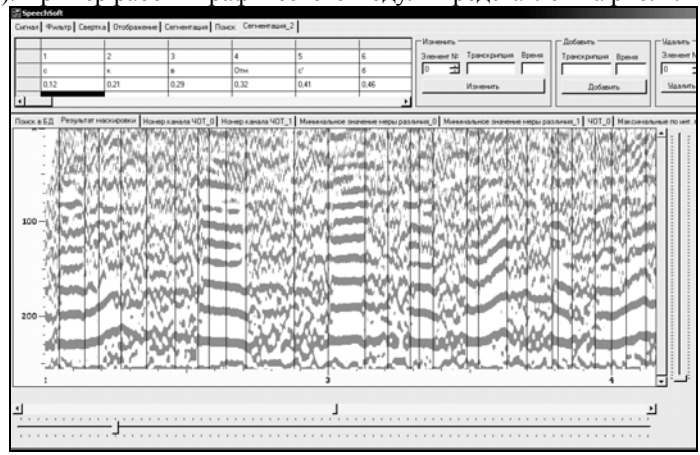


Рис. 2. Пример работы графического модуля

В дальнейшем описанные функции позволят существенно расширить и вносить правки в сегментированный речевой корпус. Данная необходимость продиктована требованием проводить исследования и тестирование алгоритмов распознавания звуков на объемном речевом корпусе.

ЛИТЕРАТУРА

1. Хлебников В.С. Реализация речевого корпуса для научно-исследовательской работы: Дипломная работа. 2011.

2. Черных Д.В. Программный комплекс для исследования речевых сигналов: Дипломная работа. 2011.

РЕЧЕВОЙ ПОЛИГРАФ

К.С. Рошкован, Д.В. Поляков, С.А. Рубанов, В.И. Наханов, студенты 4-го курса; Р.В. Мещеряков, доцент

г. Томск, ТУСУР, каф. КИБЭВС, ФВС

«Детектором лжи» именуют в народе аппарат полиграф, который чутко реагирует на степень правдивости человека во время ответов на задаваемые вопросы. Речевой полиграф позволяет анализировать человеческую речь. Считается, что если подозреваемый сообщает заведомую ложь, у него изменяется состояние голосовых связок, которые производят несколько искаженный звук за счет нерегулярного изменения основной частоты вибрации.

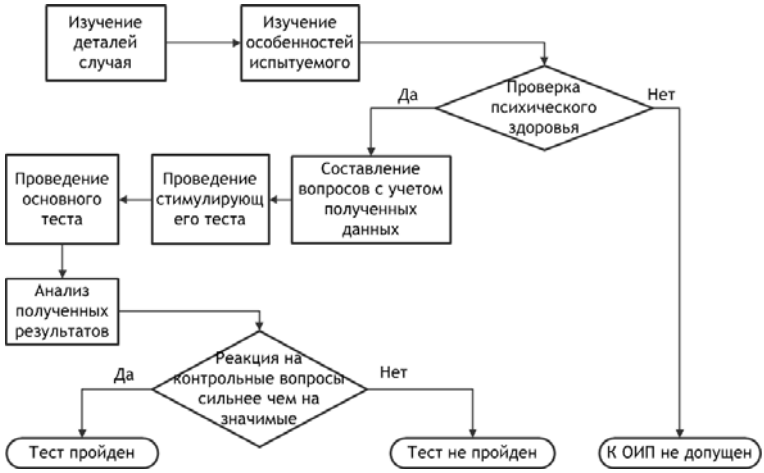


Рис. 1. Методика проведения опроса

Опрос с использованием полиграфа – это эффективное средство оценки достоверности информации, полученной ранее от человека, позволяющее выявить скрываемые сведения, особенно в тех случаях, когда их невозможно или затруднительно получить иными, традиционными путями. Особенно актуально в качестве меры отбора и проверки кадров при допуске к оперативно-розыскной деятельности и работе со сведениями, составляющими государственную тайну.

После ознакомления с понятием полиграфа, методикой проведения опросов, нормативно-правовой базой для проведения опросов была протестирована работа речевого полиграфа на контрольной группе студентов.

Рис. 2. Пример определения частоты основного тона

В ходе проделанной работы изучен речевой полиграф и обоснована целесообразность его применения. Изучена методика проведения опросов на речевом полиграфе и нормативно-правовая база для проведения опросов с использованием полиграфа (рис. 1, 2). Проведен опрос на контрольной группе студентов. Посчитана достоверность речевого полиграфа – 86%.

ЛИТЕРАТУРА

1. Нормативно-правовое обеспечение использования полиграфов в РФ [Электронный ресурс]. Режим доступа: http://www.fsb.ru Яз. рус.

2. Методика тестирования на полиграфе [Электронный ресурс]. Режим доступа: http://www.polarg.ru Яз. рус.

3. Информационный бюллетень Следственного комитета при МВД России. № 2(128).

4. Принцип работы полиграфа [Электронный ресурс]. Режим доступа: http://www.liedetector.com Яз. рус.

5. Потапова Р.К. Речь: коммуникация, информация, кибернетика. М.: Радио и связь, 1997. 528 с.

МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ

Е.В. Попова, студентка 5-го курса
г. Томск, ТУСУР, каф. КИБЭВС, sebastianbah@gmail.com

При построении систем защиты информации важное значение имеет определение угроз, которые оказывают непосредственное влияние на объект защиты, так как финансовые вложения в средства защиты от фантомных опасностей могут повлечь за собой значимые потери денежных средств компании и затруднить работу персонала. Таким образом, глубокий анализ и всестороннее рассмотрение проблемы при определении актуальных угроз является принципиальным моментом в процессе построения системы защиты информации.

Одним из способов определения актуальных угроз является оценка вероятности реализации угрозы, исходя из эмпирических знаний о данной угрозе, в совокупности с оценкой опасности каждой угрозы, эти количественные показатели дают представление о том, насколько сильно угроза и ее реализация могут повлиять на работоспособность системы и насколько весомые потери понесет от этого организация. Данный метод описан в методике определения актуальных угроз, описанной ФСТЭК [1].

Однако методика, предложенная ФСТЭК, имеет недостатки и спорные моменты, что усложняет процесс оценки и делает итоговые результаты неточными. Предлагаемая методика является переработкой методики ФСТЭКа, при неизменной внутренней структуре, избавляясь от ее недостатков, изменяя вид исходных данных и приемы их обработки.

Так, для оценки угроз как таковых требуется их представление в удобном для анализа виде, поэтому первым шагом методики является преобразование общей модели угроз исходя из классического представления реализации угрозы, а именно декомпозиция угроз на канал реализации угрозы и используемую для ее реализации уязвимость системы. Это упрощает как построение частной модели угроз, так и дальнейший анализ системы.

Далее, после построения частной модели угроз, исходя из анализа системы проводится оценка угроз. Критерии оценки угроз меняются незначительно, так, вместо критерия вероятности осуществления угрозы, оценить который представляется возможным только после долгосрочного анализа системы в работе, вводится критерий возможности осуществления угрозы, который складывается из оценок возможности использования уязвимости, ассоциированной с данной угрозой, и возможности реализации канала реализации данной угрозы. Критерий опасности осуществления угрозы остается без изменения.

Также изменяется способ оценки угрозы, в отличие от непосредственной абсолютной качественной оценки, переводимой в количественную по каждому критерию, а затем в общую качественную с достаточно размытыми границами качественной шкалы, в данной методике используется метод попарного сравнения [2], который дает количественную оценку угроз по критериям. Это позволяет отказаться от абсолютных оценок и говорит о большей степени объективности этих оценок.

Можно говорить, что подобная модификация методики устраняет недостатки родительской и при этом оставляет возможность собственной модификации, если это потребуется, дает более надежные результаты и делает процесс оценки более наглядным.

ЛИТЕРАТУРА

1. ФСТЭК. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [от 14.02.2008].

2. Шелупанов А.А., Шумский А.А. Основы системного анализа: учеб. пособие. Томск: Том. межвуз. центр дистанционного образования, 2005. 225 с.

ИНТЕГРАЦИЯ РЕЧЕВОГО КОРПУСА И ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ИССЛЕДОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ

И.А. Рахманенко, студент 5-го курса

Научный руководитель А.А. Конев, доцент, к.т.н.

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

Актуальной темой научных исследований в области информационных технологий является распознавание речи. Знания о различных параметрах речевого сигнала позволили бы решить ряд важных задач в различных областях человеческой деятельности: контроль доступа по голосу и выделение ключевых слов в слитном потоке речи будут полезны в сфере безопасности, синтез речи найдет применение в связи, медицине и кибернетике, распознавание речи – при решении задач управления ЭВМ и др.

В данной работе была произведена доработка программного комплекса для исследования речевых сигналов, был создан модуль, позволяющий производить работу с речевым корпусом и производить поиск и выбор для обработки сигналов, удовлетворяющих определенным критериям. Речевой корпус – это совокупность речевого материала и базы данных, содержащей детальное структурированное описание этого материала. Речевой материал – это речевые сигналы, данные о дикторах, речевые единицы и звуковой алфавит.

Благодаря добавлению модуля взаимодействия с речевым корпусом стала возможна реализация модуля поиска речевых сигналов, находящихся в базе данных. Также стали возможны загрузка и сохранение ручной и автоматической сегментации, что позволит в дальнейшем разработать модуль распознавания звука по его параметрическому описанию.

Модуль взаимодействия с базой данных речевого корпуса на данный момент позволяет загружать ручную сегментацию речевого сигнала, что позволяет отображать сегментацию в графическом виде, а также производить сравнение результата автоматической сегментации и эталонной ручной.

Добавление модуля поиска позволило исследовать речевые сигналы, схожие по выбранным параметрам. При реализации модуля распознавания звуков модуль поиска позволит уточнять результаты распознавания звуков.

Модуль поиска позволяет производить поиск по следующим параметрам: акустическое окружение, пол диктора, транскрипция речевой единицы, скорость речи, дефект произнесения, отрывок речевой единицы, возраст диктора. Также планируется увеличение числа параметров поиска, т.к. база данных речевого корпуса содержит большое количество данных о дикторе, условиях записи, параметрах записывающего устройства и т.д.

Кроме того, модуль поиска может быть расширен поиском по типу, характеру, месту образования звуков: лабиализация гласных звуков, место образования согласных звуков, возможные типы подъема языка при произнесении гласных, разделение гласных на типы по рядам, возможные значения мягкости речевой единицы.

В перспективе работы над комплексом для исследования речевых сигналов – создание модулей сегментации сигнала на звуки и распознавания звука по его параметрическому описанию.

Модуль распознавания звука по его параметрическому описанию предназначен для определения отдельных звуков в сегментированном звуковом сигнале. В случае успешной реализации данного модуля будет возможно распознавание отдельных слов или предложений. Однако успех распознавания слова зависит от качественной характеристики распознавания звуков, входящих в это слово.

Проектируемый модуль должен производить распознавание звука в соответствии с его параметрическим описанием. Параметрические описания других звуков хранятся в базе данных речевого корпуса. На основе сравнения параметров этих звуков и звуков в определяемом сегменте и должно происходить определение соответствия сегмента и звука. Наиболее точным должен быть результат распознавания на ос-

нове поиска звуков с похожими параметрами акустического окружения, пола, возраста диктора, других условий.

В результате выполнения задачи интеграции речевого корпуса и программного комплекса для исследования речевых сигналов были реализованы модуль поиска и модуль взаимодействия с речевым корпусом. Данные модули увеличивают функционал программного комплекса для исследования речевых сигналов, что позволит продвинуться в работе в области распознавания речи.

ЛИТЕРАТУРА

1. Агуров П. В. C#. Разработка компонентов в MS Visual Studio 2005/2008. СПб.: БХВ-Петербург, 2008. 480 с.

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

3. Конев А.А., Мещеряков Р.В., Тиунов С.Д. Исследование параметров ударных гласных звуков // Сб. тр. XXIV сессии Российского акустического общества. Т. III. М.: ГЕОС, 2011. С. 31–34.

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

5. Борри Х. Firebird: руководство разработчика баз данных: Пер. с англ. СПб.: БХВ-Петербург, 2006. 1104 с.

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ОТ УТЕЧЕК

Д.Ю. Рихтер, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, rihter.denis@gmail.com

В наш век развития информационных технологий все компании переходят на электронные документы. Это касается не только коммерческих организаций, но и государственных. Сегодня специалисты различных компаний обмениваются документами и информацией с помощью электронной почты, департаменты отдельных корпораций держат электронные документы в корпоративной сети. Такой тип обмена и хранения информации наиболее удобен, так как сразу решает многие вопросы документооборота. Однако есть и недостатки: сегодня информация очень мобильна, поэтому документ в цифровом виде легко скопировать на оптический или флеш-носитель и вынести за пределы офиса [1].

На рис. 1 показано распределение утечек по каналам за 2011 г. по данным Infowatch [2].

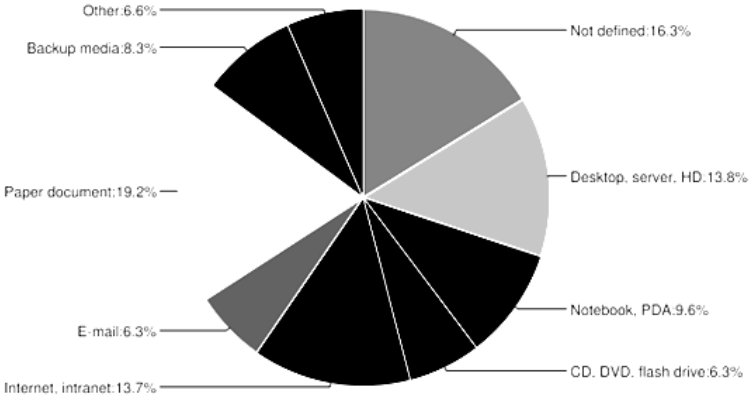


Рис. 1. Распределение утечек по каналам за 2011 г.

Исходя из данных, можно сделать вывод, что большинство утечек происходит через бумажные носители, жёсткие диски и Интернет. Большинство компаний регламентирует процессы создания резервных копий информации, но забывает о необходимости создания списка лиц, допущенных к работе с данными копиями, и их прав. Как следствие 8,3% всех утечек осуществляется через резервные копии.

Наиболее перспективным решением по обеспечению эффективной защиты от утечек информации являются DLP (Data Leak Prevention) и IRM (Information Rights Management).

Решения DLP и IRM решают схожие проблемы разными путями и несут в себе взаимодополняющие особенности:

– DLP хорошо подходит для ситуаций, когда организация не знает местонахождения принадлежащей ей конфиденциальной информации. В этом случае DLP поможет выявить каналы распространения этой информации и принять меры по предотвращению утечки;

– DLP осуществляет фильтрацию содержимого одномоментно, например при обмене информацией с партнером посредством электронного письма;

– IRM хорошо подходит для ситуаций, когда организация имеет относительно четко определенный бизнес. Защита при помощи IRM конфиденциальных документов или электронных писем гарантирует, что все копии останутся защищенными независимо от их местонахождения;

– IRM продолжает работать за пределами периметров защиты предприятия, что позволяет контролировать жизненный цикл и невозможность тиражирования защищенных документов. IRM обеспечивает

постоянную защиту, и доступ к информации может быть отменен в любое время.

Таким образом, данные решения не решают задачу защиты от утечек полностью, поскольку имеют определенные недостатки. Однако если осуществить интеграцию данных решений, мы получим систему, которая сможет автоматически классифицировать информацию и шифровать ее с различными правами доступа в зависимости от содержимого.

В результате для дальнейшего исследования была выбрана технология Microsoft Right Management System [3].

ЛИТЕРАТУРА

1. [Электронный ресурс]. Защита конфиденциальной информации: как избежать утечек. Режим доступа: http://www.star-force.ru/solutions/content/sf_content/confidencial/

2. [Электронный ресурс]. Распределение утечек по каналам 2011. Режим доступа: http://infowatch.livejournal.com/285877.html

3. [Электронный ресурс]. AD RMS: Ч. 1. Развертывание. Режим доступа: http://technet.microsoft.com/ru-ru/library/ee922691.aspx

РАЗРАБОТКА МЕТОДИКИ ПОСТРОЕНИЯ ОПТИМАЛЬНОЙ НАДЕЖНОЙ СТРУКТУРЫ ПОДСИСТЕМЫ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

А.А. Рогожин*, *адъюнкт каф. автоматизированных информационных систем ОВД

г. Воронеж, *Воронежский институт МВД России*, *raa_tsbs@list.ru*

Повышение вероятности утечки или нарушения целостности конфиденциальной информации, сосредоточенной на объектах информатизации (ОИ), обусловлено недостаточным финансированием мероприятий по комплексной физической защите таких объектов (зданий, помещений), в частности по установке интегрированных систем безопасности (ИСБ). Собственниками ОИ выполняются лишь обязательные требования по установке систем охранно-пожарной сигнализации (или подсистем ОПС ИСБ). Собственник ОИ заинтересован во внедрении качественной и надежной системы ОПС при минимальных затратах. Отсюда вытекает необходимость решения данной оптимизационной задачи.

В большинстве случаев, как видно из рис. 1, система ОПС состоит из приемно-контрольного прибора (ПКП), извещателей охранных

(ИО), извещателей пожарных (ИП), средств оповещения (СО), *n*-количества независимых шлейфов сигнализации (ШС).

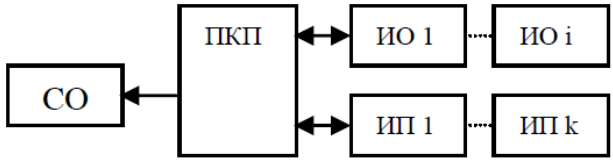


Рис. 1. Обобщенная структурная схема системы ОПС

В охранных ШС, в основном, все *i*-е элементы соединены последовательно (используются нормально-замкнутые извещатели охранные). В пожарных ШС все *k*-е элементы соединены как последовательно (например, тепловые ИП), так и параллельно (например, дымовые ИП).

Количественным критерием качества функционирования системы ОПС является показатель надежности – вероятность безотказной работы.

«Надежностным» эквивалентом системы ОПС может являться ШС с последовательной или параллельной структурой соединения элементов.

Для оптимального выбора способа повышения надежности системы ОПС необходимо знать оперативное время работы системы и наработку на отказ элементов. Для охранной сигнализации (ОС) целесообразнее использовать известные методы резервирования элементов из-за частых отключений (снятий с охраны в рабочее время) и, соответственно, небольшого времени оперативной работы. Для пожарной сигнализации (ПС) целесообразнее использовать подбор высоконадежных элементов ввиду непрерывной работы (работа без права снятия с охраны).

Возможна постановка двух следующих задач, связанных с построением оптимальной структуры системы ОС при резервировании:

• Требуется обеспечить вероятность безотказной работы системы ОС не менее заданной при минимальных затратах на резервные элементы.

• Требуется обеспечить максимально возможную вероятность безотказной работы системы ОС при заданных затратах на резервные элементы.

Первая задача может быть сформулирована в следующей форме – найти минимум функции (1):

$$W = \sum_{i=1}^{n} (w_i m_i + w_i^0), \qquad (1)$$

при условии (2):

$$P = \prod_{i=1}^{n} p_i(m_i) \geq P_{\text{тр}} \ . \qquad (2)$$

Вторая задача формулируется так – найти максимум функции (3):

$$P = \prod_{i=1}^{n} p_i(m_i) \ , \qquad (3)$$

при условии (4):

$$W = \sum_{i=1}^{n} (w_i m_i + w_i^0) \leq W_{\text{тр}} \ , \qquad (4)$$

где P – вероятность безотказной работы системы ОС; $P_{\text{тр}}$ – требуемое значение вероятности безотказной работы системы ОС; W – стоимость системы ОС; $W_{\text{тр}}$ – требуемое значение стоимости системы ОС; m – число резервных элементов на i-м участке системы ОС; n – число различных участков системы ОС; w_i – стоимость одного элемента i-го участка системы ОС; $p_i(m_i)$ – вероятность безотказной работы i-го участка системы ОС при наличии на нем m резервных элементов; w°– начальная стоимость i-го участка.

Одним из наиболее удобных методов решения задач оптимального резервирования является *метод наискорейшего спуска* [1].

Модель создания оптимальной резервированной системы ОС можно представить в виде следующего многошагового процесса. Рассматривается некоторая исходная система ОС, у которой на каждом участке не имеется сначала ни одного резервного элемента. На первом шаге отыскивается такой участок системы, прибавление к которому одного резервного элемента дает наибольший «удельный» выигрыш в приросте вероятности безотказной работы. На втором шаге отыскивается следующий участок в системе (включая и тот, у которого уже есть резервный элемент), который характеризуется наибольшим приростом вероятности безотказной работы системы ОС при добавлении одного резервного элемента. Аналогичным образом процесс продолжается далее.

Процесс прекращается на таком шаге $M\left(M = \sum_{i=1}^{n} m_i\right)$, когда для первой задачи выполняется условие (5):

$$P^{(M-1)} \prec P_{\text{тр}} \leq P^{(M)} \qquad (5)$$

или же для второй задачи выполняется условие (6):

$$W^{(M)} \leq W_{\text{тр}} \leq W^{(M+1)} \ . \qquad (6)$$

Зная вероятность безотказной работы и стоимость входящих в систему элементов (по техническим паспортам), появляется возможность построить на ОИ высоконадежную структуру системы ОС в соответствии с финансовыми возможностями заказчика.

ЛИТЕРАТУРА

1. Надежность технических систем: учеб. пособие для вузов технических специальностей / Под общ. ред. Е.В. Сугака и Н.В. Василенко. Красноярск : НИИ СУВПТ, 2001. 608 с.

2. Шишонок Н.А. Основы теории надежности и эксплуатации радиоэлектронной техники / Н.А. Шишонок, В.Ф. Репкин, Л.Л. Барвинский. М.: Сов. радио, 1964. 550 с.

ШАБЛОНЫ СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ

К.С. Рошкован*, *студент 4-го курса;
М.А. Сопов*, *ст. преподаватель
г. Томск, *ТУСУР*, *ФВС*, *каф. КИБЭВС*, *surgutkit@gmail.com*

В 21-м столетии «электронные» отношения становятся все более привычными, они проникают в широкий круг сфер человеческой жизнедеятельности, в том числе в сферу коммуникаций. В данном контексте наибольшее значение приобретает задача формирования доверия между субъектами различных систем. Фундаментом такого доверия является надежная инфраструктура безопасности, к которой относятся системы, приложения и процессы, обеспечивающие надежную, защищенную обработку транзакций.

Инфраструктура безопасности для распространения открытых ключей, управления электронными сертификатами и ключами пользователей получила название инфраструктуры открытых ключей – Public Key Infrastructure (PKI). Она представляет собой комплексную систему, сервисы которой реализуются и предоставляются с использованием технологии открытых ключей (рис. 1). Цель PKI состоит в управлении ключами и сертификатами, посредством которого организация может поддерживать надежную сетевую среду. PKI позволяет использовать сервисы шифрования и выработки цифровой подписи согласованно с широким кругом приложений, функционирующих в среде открытых ключей [1].

В классическом варианте PKI представлена следующими компонентами:

1) центр сертификации;
2) центр регистрации;
3) репозиторий сертификатов;

4) архив сертификатов;
5) конечные пользователи.

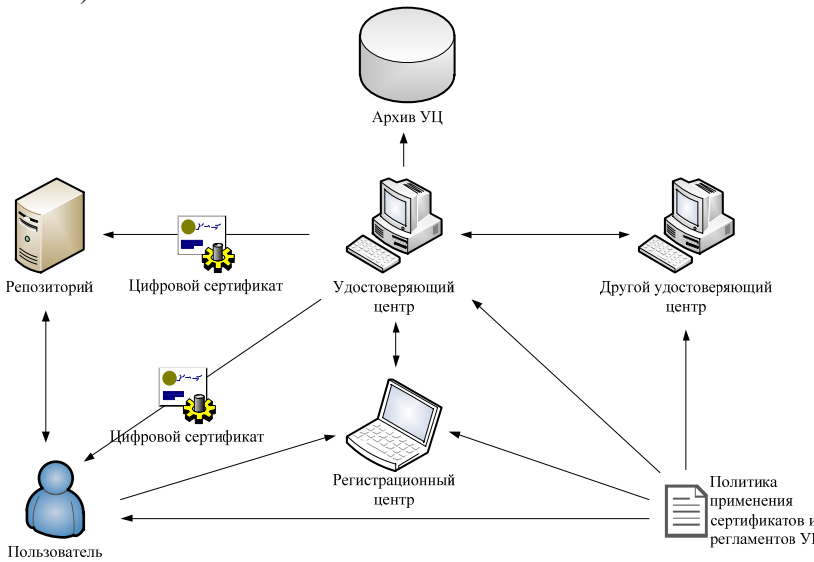


Рис. 1. Схема взаимодействия компонентов PKI

Центральный звеном является удостоверяющий центр, в PKI это главный управляющий компонент. В России действуют примерно 300 удостоверяющих центров, в том числе федеральные, региональные, ведомственные, УЦ коммерческих предприятий.

Сегодня очень остро стоит проблема миграции с ФЗ-1 «Об электронной цифровой подписи» на ФЗ-63 «О цифровой подписи». Если первый легализовывал электронно-цифровую подпись, то теперь она по умолчанию не является квалифицированной. Для этого необходимо пройти дополнительную процедуру. На данный момент де-факто существуют четыре вида электронной подписи: простая, усиленная неквалифицированная, усиленная квалифицированная по 63-ФЗ, электронная цифровая подпись по 1-ФЗ. Усиленная квалифицированная электронная подпись не может быть легитимной, пока не прошла процедура аккредитации [2]. На данном переходном этапе в целях создания условий мягкой адаптации необходимо устранить противоречия нормативно-правового регулирования деятельности УЦ.

Для большинства УЦ сфера государственных и муниципальных услуг является определяющей. В первую очередь, это системы сдачи различных форм отчетности физических и юридических лиц, электронные торги, в частности, системы государственного заказа. Приход

на этот рынок «Ростелекома» серьезно озадачивает владельцев УЦ, пользуясь значительной господдержкой, он может занять доминирующее положение на рынке услуг удостоверяющих центров.

Не меньшей является проблема определения единых требований к удостоверяющему центру, создание равных условий для оказания услуг УЦ, способствующих развитию здоровой конкуренции и повышению качества услуг, а также организация единого пространства доверия для осуществления деятельности в рамках получениям пользователями государственных услуг [3].

ЛИТЕРАТУРА

1. Полянская О.Ю., Горбатов В.С., Инфраструктуры открытых ключей: учеб. М.: Лаборатория знаний, 2007.

2. Карпов А.Г. ЗАО «АНК». Удостоверяющие центры и сервисы на основе в PKI в России: статистика и тенденции // Информационные матер. VII Междунар. науч.-практ. конф. «PKI – Форум 2009».

3. Новожилов С.Н. Практика удостоверяющего центра. Реалии бытия // Информационные матер. IX Междунар. науч.-практ. конф. «PKI – Форум 2011».

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ЗАЩИЩЕННЫХ ПРОТОКОЛОВ В ТЕРМИНАЛЬНЫХ СИСТЕМАХ И ТОНКИХ КЛИЕНТАХ

С.А. Рожков, директор ООО «Deep Systems»;
А.В. Рожков, проф. ЮУрГУ
г. Челябинск, ЮУрГУ, zserg@wtpro.ru, great.ros.marine@gmail.com

В последнее время в связи с накоплением огромного парка морально устаревшего, но вполне работоспособного оборудования, второе рождение переживает идея мэйнфреймов – больших серверов, обслуживающих парк маломощных терминалов. Эту же идею развивает ставшая модной в последнее время технология облачных вычислений, захватившая около 10% рынка IT-инфраструктуры. Общемировой рынок электронных информационных услуг оценивается в полтриллиона долларов в годовом исчислении.

Россия активно включилась в процесс информатизации управления и торговли. Мощный толчок этому дало принятие Федерального закона «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ (ред. от 03.12.2011 № 383-ФЗ). Зримым воплощением электронизации и информатизации стал мегапроект «Универсальная электронная карта», поддерживаемый тандемом банков во главе со Сбербанком России.

В свете этого защита недорогих оригинальных терминальных систем является весьма актуальной задачей.

Напомним, что терминалом называется устройство ввода и отображения информации. По сути дела – это бездисковая (без HDD-дисковая) рабочая станция, загрузка которой осуществляется по сети. Все прикладные программы выполняются на терминальном сервере, но для пользователя все выглядит так, как если бы компьютер с такой же вычислительной мощностью, как сервер, стоял у него на столе.

Созданная одним из авторов статьи, им же развиваемая и продвигаемая на рынке система WTPRO [1], поддерживает четыре терминальных протокола – два текстовых: telnet – небезопасный протокол, ssh – защищенный аналог telnet и два графических: RDP – удаленный рабочий стол Windows, VNC – открытый протокол для доступа как к Windows, так и к UNIX серверам.

Возможность тонкой настройки терминальной системы на едином сервере, почти полное исключение человеческого фактора позволяют заблокировать многие угрозы НСД. Вместе с тем терминальная система подвержена новым атакам, актуальным только для нее. Источником большинства проблем безопасности является то, что на терминале нет предустановленной ОС – она загружается по сети. Используемые при этом протоколы разрабатывались в 80-х годах прошлого века и не обеспечивают необходимого сегодня уровня защищенности. Собственно говоря, угрозу безопасности начинает представлять и фонНеймановская архитектура компьютерного «железа» и сама методология функционирования многих современных ОС.

Таким образом, с математической точки зрения требуется изучить протоколы загрузки ОС, протоколы взаимодействия сервер – тонкий клиент, протоколы аутентификации, найти слабости этих протоколов и предложить алгоритмы ликвидации узких мест. После этого провести математически строгое доказательство корректности предложенных улучшений. Идеально, если при этом будет построена элегантная математическая система, что-то вреде нагруженного ориентированного графа, на котором задано действие конечного автомата, построенного по хорошо известной группе или другой алгебраической системе в духе академика А.И. Мальцева.

Сверх этого необходимо построить модели внешнего и внутреннего нарушителя и модель «прочих стихийный угроз»: отказ оборудования, встроенные закладки, недокументированные возможности, ошибки персонала, стихийные бедствия, неоткрытые законы природы и т.д.

Проблема в том, что нет математически полноценных методов анализа протоколов. Даже протоколов криптографических. Критерием истины продолжает оставаться практика.

Следующим препятствием является цена решения вопроса и простота использования решения, т.е. расходы на обучение персонала.

1. Прежде всего необходимо контролировать целостность загружаемой ОС. Современные аппаратные терминальные клиенты, такие как НОРМА, HP, ТОНК и т.д., не поддерживают средств доверенной загрузки ОС. Аналогично этих средств и нет в распространенных программных терминальных клиентов, таких как Thinstation, WTWARE, 2X, LTSP, OpenThinClient, WinCE. Работы в направлении доверенной загрузки ОС ведут ОКБ САПР – разработчик системы «Аккорд» и компания Астра-СТ – разработчик терминальной системы «Мираж» (Mirage).

Существующие реализации терминальных клиентов, такие как Thinstation, WTWARE, 2X, LTSP, OpenThinClient и т.д., не поддерживают взаимную идентификацию терминального клиента и сервера.

Компания Астра-СТ предлагает комплексный подход – реализацию сертифицированного терминального сервера и терминального клиента. Для доверенной загрузки ОС используются расширения протокола DHCP и идентификация по МАК-адресу терминального клиента.

К минусам данной реализации можно отнести следующее:

• невозможность использования терминального клиента на серверах, отличных от Mirage;

• протокол UDP, по которому происходит загрузка образа ОС, ненадежен;

• идентификацию по МАК-адресу можно обойти, подменив его.

Одним из авторов этой статьи разработаны расширения для виртуальных каналов RDP протокола, расширяющие функциональные возможности сервера терминалов, позволяющие производить идентификацию и аутентификацию клиента и сервера. Их практическое удобство состоит в том, что пользователь работает с графической, легко различаемой информацией. Идея реализована в [2].

В свою очередь в работе [3] предложена модель и работающий в ней алгоритм, позволяющий локально формализовать проблему анализа протоколов взаимодействия двух субъектов. Например, сервера и терминального клиента.

Каждое сообщение сервера и клиента является некоторым двоичным словом. Пусть у нас взаимодействуют два субъекта. Как принято в криптографии – Алиса и Боб (A и B).

A посылает некоторое бинарное v сообщение B. В свою очередь, B, проанализировав его, отсылает A модифицированное сообщение $w = f(v)$.

В работе рассматриваются две возможные формализации данного взаимодействия, позволяющие применить стандартные методы дискретной математики и теории групп.

Первое, пусть сообщения, которыми обмениваются субъекты, имеют фиксированную длину. Данная ситуация хорошо моделируется стандартной процедурой, когда необходимо расставить флаги в интерфейсе взаимодействия. Если считать, что флаг принят – это 1, флаг сброшен – 0, то протокол взаимодействия является функцией обработки *n*-мерного бинарного вектора. То есть $f:Z_2^n \to Z_2^n$ – отображение, заданное в линейном пространстве. Поскольку нет никаких надежд, что это отображение является линейным, то лучше рассматривать двоичный вектор *v* как код бинарного дерева *T*. При этом сообщения длины *n* будут образовывать *n*-слой T_n дерева *T*. В этом случае взаимодействие будет описываться некоторым отображением дерева *T* в себя: $f:T \to T$.

Если дополнительно разбить каждую трансакцию взаимодействия на элементарные трансакции, при которых в слове *v* изменяется только один символ, то мы получим отображение *f*, являющееся автоморфизмом дерева *T*.

Если система взаимодействия работает штатно, то среди автоморфизмов Aut *T* дерева *T* выделяется подмножество *True* допустимых взаимодействий. Если же в процессе взаимодействия возникло взаимодействие $h \notin True$, то система выдает сигнал опасности.

Не слишком большой натяжкой является допущение, что выполнение друг за другом (суперпозиция) двух допустимых преобразований *f* и *g* снова будет допустимым преобразованием $f \circ g$ и что тождественное преобразование (т.е. отсутствие реальных преобразований) тоже является допустимым преобразованием. В любом случае True является, с алгебраической точки зрения, как минимум моноидом.

Обратимость преобразования *f*, т.е. восстановление прообраза v по известному сообщению *w* = *f*(*v*), возможно далеко не всегда. Часто обработка разных допустимых запросов на выходе имеет одну и ту же последовательность допустимых бит. Впрочем, и здесь часто, можно выбрать некую естественную (каноническую) ветвь многозначной функции f^{-1}. В этом случае некоторое семейство подмножеств $Gset = \{G \mid G \subseteq True\}$ моноида True будет состоять из множеств, порождающих группы $gr(G) \leq AutT$.

Вторая математическая модель более проста в использовании и не требует глубокой детализации протокола взаимодействия. Множество

преобразований при транзакциях субъектов можно представить в виде дерева Forest возможных исходов. Вершиной дерева Forest будет исходное сообщение *v* Алисы. Всевозможные ответы Боба $W=\{w|w\in W\}$ конкатенируем с сообщением *v* и получаем первый слой дерева Forest $\text{Forest}_1=\{vw|w\in W\}$. Множество ответов $U=\{u|u\in U\}$ Алисы на ответы Боба конкатенируем во второй слой дерева $\text{Forest}_2=\{vwu|w\in W,u\in U\}$ и т.д.

Возникающее дерево Forest будет слойно однородным с фиксированной начальной вершиной – кодом запуска протокола. Выполнение протокола будет случайным блужданием по дереву Forest.

Сложность состоит в том, что количество вершин в этом дереве растет экспоненциально и равно произведению чисел $|W|\cdot|U|\cdot...$ и даже при 5 проходах протокола и при 10 возможных исходах каждой трансакции получится порядка 100 тысяч вершин.

Следующее упрощение ситуации состоит в том, что разные ответы Алисы и Боба при взаимодействии имеют существенно различную вероятность. Проведя серию натурных экспериментов, можно составить таблицу вероятностей (вернее, условных вероятностей) исходов событий, принадлежащих множествам *W*, *U*, … После этого ввести новую кодировку дерева Forest, например классическим кодом Хаффмана. В этом случае дерево Forest преобразуется в двоичное дерево *F*. Двоичное дерево *F* будет иметь ту же мощность, что и дерево Forest. Но, отбросив его ветви, вероятность попадания на которые будет меньше некоторой пороговой величины, например, 10^{-3}, мы сможем существенно прорядить дерево *F*. Во многих важных для практики случаях до мощности $|W|+|U|+...$. Назовем такое проряженное дерево логарифмическим деревом *LF*.

В работе получены некоторые интересные результаты, анализа протоков аутентификации в тонком клиенте WTPRO на языке автоморфизмов деревьев *T* и *LF*.

ЛИТЕРАТУРА

1. Рожков С.А. Терминальная система «ElinuxT»: Свидетельство об официальной регистрации программы для ЭВМ № 2006611848. Зарегистрировано в Реестре программ 30.05.2006.

2. Рожков С.А. Терминальная система ElinuxT: Свидетельство об отраслевой регистрации разработки № 5491. Гос. координац. центр информ. технологий. Отраслевой фонд алгоритмов и программ. М., 2005. 29.12.05, № 50200501788.

3. Рожков А.В. Применение теории групп в задачах защиты информации // Наука ЮурГУ: матер. 60-й юбилейной науч. конф. Секция технических наук. Челябинск: Изд-во ЮурГУ, 2008. Т. 2. С. 111–118.

РАЗРАБОТКА МОДЕЛИ НАРУШИТЕЛЯ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

М.С. Саблин, студент 5-го курса; В.Г. Миронова, аспирант
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, mvg@security.tomsk.ru

Проблема обеспечения защиты информации является одной из важнейших при построении надежной информационной структуры организации. Она охватывает как физическую защиту данных и системных программ, так и защиту от несанкционированного доступа к данным, передаваемым по линиям связи и находящимся на накопителях.

Построение системы защиты информации (СЗИ) для информационной системы (ИС) трудоемкий процесс, который включает в себя три этапа (рис. 1).

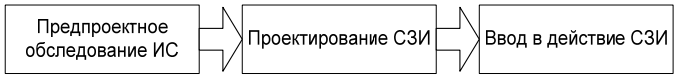


Рис. 1. Этапы создания СЗИ

Предпроектное обследование включается в себя:

- классификацию ИС;
- разработку организационно-распорядительной документации;
- определение степени исходной защищенности ИСПДн;
- разработку модели нарушителя безопасности информации;
- разработку частной модели угроз безопасности ПДн;
- разработку частного технического задания [1].

При проведении обследования необходимо учитывать множество аспектов, таких как:

- ценность защищаемой информации;
- объем защищаемой информации;
- структура ИС;
- месторасположение ИС и возможность передачи информации;
- имеющиеся средства защиты информации.

В статье будут рассмотрены вопросы, связанные с разработкой модели нарушителя безопасности информации.

Согласно [3] «нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку». Под нарушителем в общем виде можно рассматривать лицо или группу лиц, которые в результате предумышленных или непредумышленных действий обеспечивают реализацию угроз информационной безопасности.

Модель нарушителя может иметь различную степень детализации. Выделяют три основные степени:

– Содержательная модель нарушителей отражает систему принятых руководством объекта, ведомства взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия. Данная модель чаще всего называется неформальной.

– Сценарии воздействия нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.

– Математическая модель воздействия нарушителей представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, параметрически характеризующих результаты действий, и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны. Именно этот вид модели используется для количественных оценок уязвимости объекта и эффективности охраны [8].

Неформальная модель нарушителя в автоматизированной системе. Данная модель самая простая для понимания, она не ограничена ни какими рамками и содержит в своем составе наиболее полное описание характеристик нарушителя (табл. 1).

Таблица 1

Классификация нарушителей

Тип нарушителя	Категория нарушителя	Описание
Внешний нарушитель	Выделяют одну категорию (N0)	Не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители
Внутренний нарушитель	Всего выделяют 8 категорий (N1…N8)	Нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн

При разработке данной модели определяются такие параметры как предположения о категориях лиц, к которым может принадлежать нарушитель.

Модель нарушителя согласно [9].

Данная модель может быть использована при оценке уязвимости системы защиты (элемента системы защиты) к нападению злоумышленника. Основной особенностью данной модели является оценка действия нарушителя по двум основным критериям:

– идентификация уязвимости;
– использование уязвимости.

Согласно [5] нарушители безопасности делятся по уровню доступа (табл. 2).

Таблица 2

Пример формирования модели нарушителей

Тип нарушителя	Описание	Должность
Внешний нарушитель	Не имеющих доступа к ИСПДн	Лица, не являющиеся сотрудниками и не имеющие права доступа в КЗ
Внутренний нарушитель	Нарушитель первой категории, имеющий санкционированный доступ к ИСПДн, но не имеющий доступа к ПДн	Должностные лица, обеспечивающие нормальное функционирование ИСПДн
Внутренний нарушитель	Нарушитель пятой категории, зарегистрированные пользователи с полномочиями системного администратора ИСПДн	Системный администратор ИСПДн

Основными факторами, необходимыми для идентификации / использования уязвимости являются:

- время, затрачиваемое на идентификацию уязвимости;
- техническая компетентность специалиста;
- знание проекта и функционирования объекта;
- доступ к объекту;
- аппаратные средства/программное обеспечение или другое оборудование, требуемое для анализа/использования уязвимости.

На основании данных факторов в числовом эквиваленте вычисляется потенциал нападения. Далее определяется рейтинг уязвимости системы защиты к нападению.

Дополнительные факторы включают в себя тип нарушителя, положение по отношению к объекту защиты и место действия.

Примером дополнительного фактора может являться информация о предполагаемом месте расположения злоумышленника во время реализации атаки.

Результатом разработки неформальной модели нарушителя выделяют категории лиц, к которым относится нарушитель, также выясня-

ется, чем мотивированы действия нарушителя, определяются квалификация нарушителя и его техническая оснащенность. Из дополнительных параметров можно определить, в какое время нарушитель совершил атаку на ИС и откуда.

Построение модели нарушителя безопасности информации позволяет решить следующие задачи:

– определение категории (типы) нарушителей, которые могут воздействовать на объект;

– цели, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и проч.;

– типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе.

ЛИТЕРАТУРА

1. Миронова В.Г., Шелупанов А.А. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Докл. Том. гос. ун-та систем управления и радиоэлектроники. 2010. №2(22). Ч. 1. С. 257–259.

2. Шелупанов А.А., Миронова В.Г. и др. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Докл. Том. гос. ун-та систем управления и радиоэлектроники. 2010. №1(21). Ч. 1.С. 14–22.

3. Методическиие рекомендации ФСБ.

4. Миронова В.Г., Шелупанов А.А. Анализ этапов предпроектного обследования информационной системы персональных данных // Вестник СибГАУ им. М.Ф. Решетнева. 2011. №2(35). С. 45–48.

5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

6. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

7. Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных. Приказ Федеральной службы по техническому и экспертному контролю Российской Федерации от 5 февраля 2010 г. № 58.

8. ru.wikipedia.org/wiki/Модель_нарушителя.

9. Общая методология оценки безопасности информационных технологий. Утверждена ФСТЭК России.

РЕЧЕВЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ СТУДЕНТОВ – НОСИТЕЛЕЙ РУССКОГО ЯЗЫКА ПРОИЗНОШЕНИЮ НА ИНОСТРАННОМ ЯЗЫКЕ

Л.Р. Салиева, студентка 1-го курса
г. Томск, ТУСУР, luiza_94@mail.ru

Английский язык уже не первый год остается одним из самых востребованных языков в мире. В глобализированном мире английский является языком межкультурных коммуникаций. В образовательных политиках многих стран мира знание английского все чаще относят к базовым. Выучив язык, овладев немалым словарным запасом, научившись понимать и общаться непосредственно с носителями языка, понимаешь, насколько их интонация и произношение отличны от твоих. В это время многие сталкиваются с проблемой произношения.

Развитие современных технологий дает нам возможность более детального изучения иностранного языка, в том числе и произношения. Идея создания технологии, способной распознать речь, не дает покоя многим уже долгое время. Но разработчики систем автоматического распознавания речи давно столкнулись с проблемой универсальности речи. Системы неспособны распознавать мужскую и женскую речь одновременно. Необходимо учитывать, что произношение зависит от множества параметров, одними из которых являются пол, возраст и особенности диалекта. В качестве решения данной проблемы было предложено создание речевого корпуса, который был бы практически применим для исследований в области речевых технологий, с целью последующего обучения иностранным языкам. Речевой корпус представляет собой множество речевых фрагментов, которые являются базовой единицей при распознавании речи.

Создание данного речевого корпуса – весьма трудоемкий процесс, занимающий значительное количество времени и требующий записи и ручной сегментации базы речи. Создание корпуса основывается на знании международного фонетического алфавита, который применим не только к английскому языку. Точность и правильность сегментации во многом определяют качество и надежность распознавания речи. Каждое слово, произнесенное диктором, разбивается на отрезки-сегменты, которым присваивается некоторый символ, соответствующий символу международного фонетического алфавита. Целесообразным было использование наборов фраз, в совокупности содержащих все звуки английского языка. Речевой корпус будет использован для лингвистического анализа на предмет выявления лексических или синтаксических ошибок при освоении английского языка.

В будущем на основе данного речевого корпуса планируется создание системы распознавания речи с целью оценки уровня владения языком, обнаружения и последующей коррекции обнаруженных ошибок, а также обучения студентов правильному произношению английской речи. Данная система будет полезна для выработки планов и методических приемов для дальнейшей коррекции в обучении языку.

ЗАЩИТА .NET ПРИЛОЖЕНИЙ

А.А. Шадрин, студент 5-го курса
Научный руководитель Е.М. Давыдова, доцент, к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС

.NET сборка для злоумышленника, как открытая книга: при помощи специальных утилит, например Reflector, дизассемблирование и обратная разработка кода представляет довольную простую задачу.

Для разработчиков очень важно защитить .NET сборку от дизассемблирования и от нелегального использования.

Сегодня существует несколько подходов к решению данной проблемы. Большинство разработчиков используют различные модули, контролирующие доступ пользователей с помощью серийных номеров, ключей активации и т.п. В Интернете существует множество программ, позволяющих нелегально пользоваться программным обеспечением с помощью генераторов ключей активации, кряков, патчей, и др. Кроме этого, некоторые легальные пользователи обнародуют свои серийные номера.

Эти очевидные недостатки привели к созданию аппаратной защиты программного обеспечения в виде электронного ключа.

Электронный ключ (также аппаратный ключ) предназначен для защиты программного обеспечения и данных от копирования, нелегального использования и несанкционированного распространения.

Электронных ключей довольно большое количество, приведем некоторые линейки продуктов: CodeMeter от WIBU-SYSTEMS, Guardant от компании «Актив», HASP от Aladdin (SafeNet с 31 марта 2010 г.), LOCK от Astroma Ltd., Rockey от Feitian, SenseLock от Seculab.

Выбор электронного ключа довольно непростая задача, у каждого ключа есть свои плюсы и минусы, но все же выбор зависит в основном от нужд разработчика в качестве защиты. Вариантов ключей существует довольно большое количество: ключи со встроенными часами, с собственной флэш-памятью, с возможностью загружать код внутрь ключа, различные форм-факторы ключа и др.

Для некоторых существующих ключей можно найти эмуляторы, для некоторых программ, защищенных с помощью электронных ключей, существуют кряки, но развитие не стоит на месте и компании-разработчики усовершенствуют свою защиту и свои технологии.

Довольно часто защищенные с помощью электронного ключа программы бывают взломаны по причине использования только стандартных функций и средств защиты ключа, нежелания разработчика дополнять свой код дополнительными возможностями ключа, периодически обновлять и менять защиту своего приложения. Это основные причины, которые способствуют созданию кряков, патчей и т.п.

Электронный ключ защищает .NET приложение в основном только от копирования, нелегального использования и несанкционированного распространения. От дизассемблирования .NET сборки частично защищает шифрование, используемое совместно с защитой ключа, но шифрование всей сборки заметно замедляет работу приложения, из-за этого приходится отказываться от полного шифрования сборки и использовать шифрование лишь частично.

Незашифрованный код .NET приложения по-прежнему может быть дизассемблирован, для затруднения дизассемблирования и дополнения к защите, созданной с помощью электронного ключа, рекомендуется использовать обфускаторы.

ЛИТЕРАТУРА

1. Скляров Д.В. Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2004. 288 с.

2. 10-й ключ [Электронный ресурс]. Кстати говоря... // URL: http://www.dsnavigator.ru/kstaty/ (дата обращения: 26.02.2012).

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ КАДРОВОГО ДЕЛОПРОИЗВОДСТВА

Б.В. Шефф, В.Г. Миронова

г. Томск, ТУСУР, ФВС, mvg@security.tomsk.ru

Деятельность большинства организаций связана с использованием при обработке и передаче данных информации о сотрудниках, клиентах, поставщиках и т.д.

Персональные данные (ПДн) – это важная информация о человеке, поэтому с целью соблюдения конституционных прав и свобод граждан РФ государство требует от организаций и физических лиц обеспечить надежную защиту ПДн. Федеральный закон №152-ФЗ «О пер-

сональных данных», вступивший в силу в январе 2007 г. четко определил понятия «персональные данные», «оператор персональных данных» и «информационная система персональных данных» [1].

Статья 19 Федерального закона возлагает на оператора ПДн ответственность по обеспечению безопасности ПДн. Обеспечение безопасности ПДн достигается путем построения адекватной системы защиты персональных данных (СЗПДн), которая позволяет исключить действия, результат выполнения которых может привести к негативным последствиям для субъекта ПДн.

Требования к обеспечению безопасности ПДн указаны в Постановлении Правительства Российской Федерации № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и в нормативно-методических документах Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и Федеральной службы безопасности (ФСБ России).

В соответствии с рекомендациями ФСТЭК России обеспечение защиты ИСПДн и ПДн включает следующие этапы:

1. Предпроектный этап:
– обследование ИСПДн;
– классификация ИСПДн;
– разработка организационно-распорядительной документации;
– определение степени исходной защищенности ИСПДн;
– разработка частной модели угроз безопасности ПДн;
– разработка плана мероприятий по обеспечению защиты ПДн.
2. Этап проектирования и реализации:
– разработка технического задания;
– разработка технического проекта;
– разработка нормативной и регламентирующей документации.
3. Этап ввода в действие:
– опытная эксплуатация системы защиты ПДн;
– внедрение технических средств защиты ПДн;
– приемо-сдаточные испытания;
– оценка соответствия требованиям по безопасности информации;
– обучение персонала.

Основополагающим этапом построения СЗПДн является предпроектный этап, в который входят:

– обследование ИСПДн
– классификация ИСПДн;
– разработка организационно-распорядительной документации;
– определение степени исходной защищенности ИСПДн;
– разработка частной модели угроз безопасности ПДн.

Классификация ИСПДн проводится оператором ПДн согласно [2] и включает в себя следующее:

– сбор и анализ исходных данных об ИСПДн;

– присвоение ИСПДн соответствующего класса ИСПДн согласно требованиям [2];

– документальное оформление – акт классификации ИСПДн.

Под сбором и анализом исходных данных об ИСПДн будем понимать следующие сведения:

– категория обрабатываемых ПДн (категория 1; категория 2; категория 3; категория 4) [2];

– объем обрабатываемых ПДн (1, 2, 3 – количество субъектов, ПДн которых обрабатываются в ИСПДн);

– наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена;

– режим разграничения прав доступа пользователей ИСПДн;

– заданные оператором характеристики безопасности ПДн;

– структура ИСПДн (ИСПДн – автономная локальная либо распределенная);

– режим обработки ПДн;

– местонахождение технических средств ИСПДн [3].

Следующий шаг в предпроектного этапа – разработка организационно-распорядительной документации по защите ПДн, которая включает в себя:

1) приказ о защите ПДн;
2) приказ о подразделении по защите ПДн;
3) приказ о назначении ответственных лиц за обработку ПДн;
4) политику информационной безопасности;
5) приказ о проведении внутренней проверки;
6) положение о разграничении прав доступа к обрабатываемым персональным данным;
7) план мероприятий по защите ПДн;
8) уведомление о обработке ПДн;
9) должностные инструкции сотрудников, обрабатывающих ПДн;
10) порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;
11) план внутренних проверок состояния защиты ПДн;
12) журнал учета обращений субъектов ПДн о выполнении их законных прав;
13) перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации;
14) электронный журнал обращений пользователей информационной системы к ПДн;
15) и т.д.

Заключительным шагом предпроектного этапа является построение модели угроз безопасности ПДн согласно [4, 5] и формирование требований к СЗПД согласно [6].

Возьмем, например, ИСПДн «1С: Предприятие», которая предназначена для ведения кадрового и бухгалтерского учета сотрудников организации.

Предположим, что ИСПДн «1С: Предприятие» обладает следующими классификационными признаками:

– категория обрабатываемых ПДн – категория 2, поскольку в ИСПДн «1С: Предприятие» содержится следующая информация: ФИО, место жительства, телефон, должность, № банковской карты, ИНН, дата и место рождения;

– объем обрабатываемых ПДн – 3, в системе обрабатывается не более 100 000 записей ПДн;

– наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена – есть;

– режим разграничения прав доступа пользователей ИСПДн – с разграничением прав доступа;

– заданные оператором характеристики безопасности ПДн – ИСПДн является специальной ИСПДн;

– структура ИСПДн – локальная (комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа);

– режим обработки ПДн – многопользовательский;

– местонахождение технических средств ИСПДн – все технические средства находятся в пределах Российской Федерации.

Согласно [2] ИСПДн «1С: Предприятие» имеет класс 3. Класс 3 (К3) – ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн.

Далее определяем уровень исходной защищенности (Y_1) (табл. 1).

ИСПДн «1С: Предприятие» имеет средний уровень исходной защищенности, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» ($Y_1 = 5$).

Для ИСПДн «1С: Предприятие» рассмотрим некоторые из возможных угроз, а именно:

– угроза утечки видовой информации с экрана дисплея;
– угроза несанкционированного копирования информации;
– угроза анализа сетевого трафика;
– угроза «отказ в обслуживании»;
– угроза внедрения по сети вредоносных программ.

Таблица 1

Исходный уровень защищенности

№ п/п	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению	Высокий
2	По наличию соединения с сетями общего пользования	Средний
3	По встроенным (легальным) операциям с записями баз ПДн	Средний
4	По разграничению доступа к ПДн	Средний
5	По наличию соединений с другими базами ПДн иных ИСПДн	Высокий
6	По уровню (обезличивания) ПДн	Низкий
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Высокий

Определим вероятность их реализации (Y_2). И по итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2) рассчитаем коэффициент реализуемости угрозы (Y). Коэффициент реализуемости угрозы определяется соотношением

$$Y = (Y_1 + Y_2)/20.$$

Таблица 2

Определение актуальных угроз безопасности ПДн

№	Наименование угрозы безопасности ПДн	Y_2	Коэф. реализ.	Опасность	Актуальность
1	Угроза утечки видовой информации с экрана дисплея	2	0,35	Низкая	Неактуальная
2	Угроза несанкционированного копирования информации	5	0,5	Высокая	Актуальная
3	Угроза анализа сетевого трафика	5	0,5	Средняя	Актуальная
4	Угроза «отказ в обслуживании»	2	0,35	Низкая	Неактуальная
5	Угроза внедрения по сети вредоносных программ	5	0,5	Средняя	Актуальная

Оценка опасности угроз безопасности ПДн производится экспертом (специалистом по защите информации) и определяется вербальным показателем опасности (табл. 2).

В соответствии с правилами определения актуальности угрозы безопасности для ИСПДн «1С: Предприятие» определяются актуальные и неактуальные угрозы.

Исходя из анализа представленного перечня угроз безопасности ПДн, были выявлены следующие актуальные угрозы:

1. Угроза несанкционированного копирования информации.

2. Угроза анализа сетевого трафика.

3. Угроза внедрения по сети вредоносных программ.

Требования по нейтрализации угроз безопасности ПДн представлены в [6]. Согласно этим требованиям необходимо проектировать СЗПДн.

ЛИТЕРАТУРА

1. О персональных данных // Федеральный закон № 152-ФЗ, утвержден Президентом Российской Федерации 27 июля 2006 г.

2. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

3. Шелупанов А.А., Миронова В.Г., Ерохин С.С., Мицель А.А. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Доклады Том. гос. ун-та систем управления и радиоэлектроники. 2010. №1(21), ч. 1. С. 14–22.

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

6. Приказ ФСТЭК РФ от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». Зарегистрирован в Минюсте РФ 19.02.2010 № 16456.

7. Миронова В.Г., Шелупанов А.А. Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Доклады Том. гос. ун-та систем управления и радиоэлектроники. 2010. №2(22), ч. 1. С. 257–259.

8. Миронова В.Г., Шелупанов А.А. Анализ этапов предпроектного обследования информационной системы персональных данных // Вестник СибГАУ им. М.Ф. Решетнева. 2011. №2(35). С. 45–48.

ПРОЕКТИРОВАНИЕ АВТОНОМНОГО УСТРОЙСТВА ДЛЯ ПОДКЛЮЧЕНИЯ К UTP

В.Е. Шильненков*, *студент 5-го курса;
Р.В. Мещеряков*, *доцент*, *д.т.н.
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, shilnenkov.v@gmail.com

Ethernet (описывается стандартами IEEE группы 802.3) – пакетная технология передачи данных преимущественно локальных компьютерных сетей.

В настоящее время технология Ethernet 100BASE-TX является самой распространённой для подключения клиентов к высокоскоростному Интернету (Beeline, Tomica, TTK+, Tomtel и др.), построения локальных вычислительных сетей.

Вопросам защиты «витой пары» уделяется минимальное внимание. У злоумышленника в большинстве случаев есть полный физический доступ к UPT (рис. 1) с возможностью незаметного подключения.

Рис. 1. Щиток в подъезде

На данный момент в Интернете можно найти инструкции по созданию устройств для подключения и перехвата данных, проходящих по UTP. Основаны они на использовании роутеров (точек доступа) управляемых коммутаторов. Для их работы необходим доступ к постоянному источнику тока (розетка 220 В), что в большинстве случаев невозможно. Также на выставке CeBIT, прошедшей в 2007 г. в Германии, публике было представлено устройство для бесконтактного снятия данных, проходящих по UTP. К сожалению, найти какую-либо подробную информацию по внутреннему устройству и принципу функционирования не удалось.

Целью проекта является создание автономного специализированного устройства для несанкционированного подключения к UTP и перехвата проходящих данных с последующим сохранением на внутренней памяти устройства.

ЛИТЕРАТУРА

1. Лазарев А. «Сети» Спецификации IEEE 802.3u Auto-Negotiation и 802.3x Flow Control [Электронный ресурс]. Режим доступа: http://ivt.psati.ru/metods/Seti_EVM/El_Uch_Seti_Lazarev/lan/5/ (дата обращения: 16.02.2012).

2. burokrat@real.xakep.ru «Витой снифер» [Электронный ресурс]. Режим доступа: http://www.magxak.ru/xa106/128/1.htm (дата обращения: 16.02.2012).

3. IEEE Standard. Local and metropolitan area networks [Электронный ресурс]. Режим доступа: http://ece251switch.googlecode.com/svn-history/r200/trunk/docs/802.3-2005_section1.pdf. (дата обращения: 12.02.2012).

РАЗГРАНИЧЕНИЕ ДОСТУПА В INTERNET С ИСПОЛЬЗОВАНИЕМ VPN И NPS

И.Н. Шишкин, студент 5-го курса

Научный руководитель М.И. Мельников, аспирант каф. КИБЭВС

г. Томск, ТУСУР, каф. КИБЭВС, sin@keva.tusur.ru

Разграничение доступа в сеть Internet из локальной сети является одной из важнейших задач системного администратора. Для запрета доступа к определённым ресурсам сети (социальным сетям, развлекательным порталам) можно использовать различные межсетевые экраны. В том случае, когда требуется не только запрет на доступ к определённым ресурсам, но и предоставление доступа с помощью аутентификации пользователя, задача разграничения доступа усложняется.

К способам разграничения доступа в Internet можно предъявить следующие требования:

1) простота использования с точки зрения пользователя;

2) удобство администрирования;

3) надёжность;

4) сохранение истории работы каждого пользователя.

В качестве примеров технологий, позволяющих разграничить доступ в Internet и при этом производить аутентификацию пользователя, можно привести:

1) прокси-сервер с аутентификацией;

2) Virtual Private Network (VPN).

Недостатком прокси-серверов является то, что для их использования необходимо производить дополнительную настройку программ. Кроме того, некоторые программы могут не иметь возможности настройки прокси-сервера. Также веб-браузеры будут требовать авторизации пользователя при каждом запуске. Всё это усложняет работу конечного пользователя.

В этом случае использование VPN удобнее, так как подключение нужно запускать один раз (процесс запуска можно автоматизировать средствами операционной системы).

В большинстве крупных компаний локальная сеть представляет собой домен Windows NT, в котором содержится служба каталогов

Active Directory. В данном случае служба каталогов является мощным инструментом для администрирования сети и может использоваться для аутентификации пользователей не только в домене, но и для подключения к VPN.

В данном случае сервер VPN может быть реализован по любой технологии, главное, чтобы он поддерживал авторизацию с помощью RADIUS, то есть содержал в себе RADIUS-клиент.

Для того чтобы пользователи могли авторизовываться с помощью своих учётных данных из Active Directory, в домене Windows NT должен содержаться сервер политики сети (NPS). Для реализации рассматриваемой задачи:

1) NPS должен быть сконфигурирован как RADIUS-сервер;

2) NPS должен быть зарегистрирован в Active Directory;

3) в NPS должен быть зарегистрирован RADIUS-клиент VPN-сервера.

Пример реализации такой технологии разграничения доступа в Internet приведён на рис. 1.

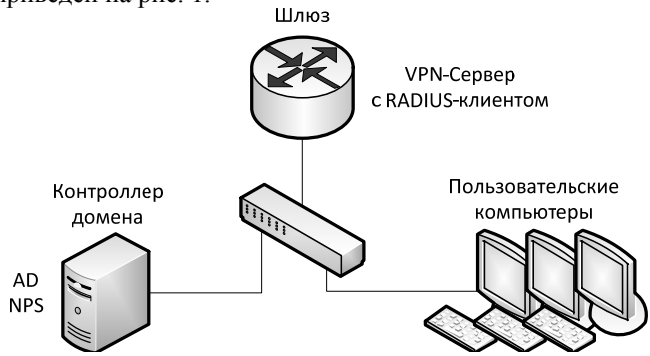


Рис. 1. Реализация разделения доступа к сети Internet

В данной реализации контроллер домена содержит не только службу каталогов Active Directory, но и сервер политики сети NPS.

На клиентских компьютерах настроен стандартный инструмент Windows для подключения к VPN. Для удобства пользователей в настройках подключения к VPN указано: «использовать автоматически имя входа и пароль Windows». IP-адреса для VPN подключения хранятся в AD. Таким образом можно отслеживать и запоминать действия пользователей с помощью Traffic Flow.

При использовании VPN и NPS для разграничения доступа к сети Internet можно значительно упростить работу системного администратора, так как в данном случае для управления доменом Windows NT и доступа в Internet используется единый инструмент – Active Directory.

ЛИТЕРАТУРА

1. Статья «Configuring Server 2008 for RADIUS Authentication». [Электронный ресурс]. Режим доступа: http://www.bunkerhollow.com/blogs/matt/archive/2008/06/04/configuring-server-2008-for-radius-authentication.aspx свободный. (Дата обращения: 1.03.2012).

ОЦЕНКА ЗАЩИЩЁННОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ И ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ АСУ ТП ГАЗОВОЙ ОТРАСЛИ

В.В. Шишкин, студент 5-го курса;
С.В. Кирсанов, зам. начальника отдела информационной безопасности СКЗ ООО «Газпромтрансгаз Томск»
г. Томск, ТУСУР, каф. КИБЭВС, jcd3nt0n@gmail.com

Развитие информационных технологий привело к тому, что на сегодняшний момент большинство информационных систем строится на базе стандартных технических средств. Эта тенденция также затронула и автоматизированные системы управления технологическими процессами (далее – АСУ ТП). В традиционных АСУ ТП широкое применение получили универсальные SCADA-системы (от англ. Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных), которые работают на распространённом оборудовании и программном обеспечении, а также предоставляют простой интерфейс для управления и программирования, что в итоге задало некоторые тенденции в области обеспечения информационной безопасности АСУ ТП:

- минимальный учет требований обеспечения информационной безопасности при проектировании АСУ ТП;
- отсутствие утверждённого стандарта, регулирующего требования к обеспечению информационной безопасности в АСУ ТП;
- длительный срок эксплуатации систем и их элементов (15–20 лет);
- подключение АСУ ТП к корпоративным или информационно-телекоммуникационным сетям;
- многообразие компонентов и программных средств, используемых в системах;
- появление «атак», направленных преимущественно на производственные системы;
- нацеленность вредоносного программного обеспечения на определённые системы или предприятия различных областей деятельности;
- невозможность выявления имеющихся и неизвестных уязвимостей и проблем в условиях постоянного усложнения систем и их закрытости;

• привнесение уязвимостей распространённых аппаратных и программных средств при их использовании в системах;

• влияние на работоспособность системы использования сторонних средств защиты информации, что во многих случаях недопустимо.

Эти факторы поставили ряд вопросов в области информационных технологий перед исследователями и специалистами.

Исторически сложилось, что при создании систем автоматизации производства вопросы информационной безопасности АСУ ТП практически не рассматривались, вместо этого внимание разработчиков было направлено на физическую безопасность систем (электро-, пожарная, промышленная безопасность). Однако существующие реалии требуют пристального внимания к решению проблем в области обеспечения информационной безопасности АСУ ТП, но для этого потребуется достаточно длительный срок до утверждения всех требований, реализации их в аппаратных и программных средствах и замены используемых систем и компонентов новыми. В то же время уже сегодня возникает задача оценки состояния защищённости эксплуатируемых АСУ ТП, которые создавались без учёта требований нормативных документов, регламентирующих вопросы информационной безопасности. Для этого необходим комплекс мероприятий по оценке состояния защищённости АСУ ТП, который в общем виде включает в себя определённый перечень организационно-технических мер, направленных на:

− идентификацию, классификацию и описание угроз информационной безопасности АСУ ТП и её компонентов (составление модели угроз, модели злоумышленника и т.п.) в соответствии с нормативно-правовыми актами государственных регуляторов и эксплуатирующих организаций [1, 2];

− инвентаризацию и классификацию подлежащих защите объектов типового комплекса АСУ ТП согласно классификации, регламентируемой нормативно-правовыми документами государственных регуляторов и эксплуатирующих организаций [1, 2];

− составление списка участвующих в процессе оценки состояния защищённости специалистов и разделение областей их ответственности согласно организационной структуре организации;

− составление списка оцениваемых показателей, влияющих на защищённость подлежащих защите объектов типового комплекса АСУ ТП, согласно нормативно-правовым документам государственных регуляторов и организаций [1, 2];

− описание методики проведения оценки состояния защищённости типового комплекса АСУ ТП, включая математический аппарат для вычисления итоговых значений на основе оцениваемых показателей;

− составление инструкций для отдельных подразделений организации по применению методики к объектам защиты, которые находятся в зоне ответственности этих подразделений;

− составление документов, регламентирующих действия по улучшению и планированию информационной безопасности, согласно результатам, полученным в процессе оценки состояния защищённости типового комплекса АСУ ТП;

− регламентирование содержания и оформления отчётной документации, используемой в процессе оценки состояния защищённости типового комплекса АСУ ТП.

Реализация вышеперечисленных организационно-технических мер позволит эффективнее обеспечивать информационную безопасность типовых комплексов АСУ ТП организации.

ЛИТЕРАТУРА

1. Р Газпром 4.2-0-003–2009. Система обеспечения информационной безопасности ОАО «Газпром». Типовая политика информационной безопасности автоматизированной системы управления технологическими процессами.

2. СТО Газпром 4.2-2-002–2009. Система обеспечения информационной безопасности ОАО «Газпром». Требования к автоматизированным системам управления технологическими процессами.

ЗАЩИЩЕННЫЙ УДАЛЕННЫЙ ДОСТУП К ЛАБОРАТОРНОМУ СЕТЕВОМУ ОБОРУДОВАНИЮ

И.С. Шитов, аспирант

г. Томск, ТУСУР, каф. РЗИ, fstudyz@gmail.com

На сегодняшний момент практически у каждой организации есть своя локальная сеть, включающая несколько сетевых устройств. Условия постоянного роста количества сетей и разнообразия имеющегося на рынке сетевого оборудования повышают требования к квалификации специалистов, занимающихся проектированием и администрированием сетей.

Практическая работа с различным лабораторным сетевым оборудованием позволяет обучающемуся сделать осознанный выбор сетевого оборудования при проектировании сетевой инфраструктуры за счет знания особенностей конкретных моделей сетевых устройств, а применение дистанционной формы обучения в данном случае может упростить, за счет автоматизации, организацию учебного процесса без потери эффективности обучения. Существуют коммерческие системы для обеспечения такой формы обучения [1], однако эти системы не лишены недостатков. В данной статье рассмотрена реализация систе-

мы удаленного доступа к сетевому оборудованию, обладающей большей гибкостью по сравнению с аналогами и построенной на основе свободно распространяемых программных средств.

Для ограничения доступа к сетевому оборудованию от постороннего вмешательства необходимо соблюдение следующих базовых требований безопасности: конфиденциальность (шифрование) и контроль целостности передаваемой информации, а также взаимная аутентификация на этапе подключения. Исходя из указанных выше требований, а также критериев простоты развертывания и использования, наиболее подходящим протоколом для защищенного удаленного доступа является протокол SSH.

Протокол SSH предусматривает установление соединения с шифрованием по алгоритмам AES, Blowfish, 3DES и др., контролем целостности по алгоритмам sha1 и md5, аутентификацией сервера по открытому ключу [2, 3]. Таким образом, аутентификация клиента по паролю будет выполняться уже по защищенному каналу.

Для аутентификации всех обучающихся создается одна системная учетная запись на SSH-сервере с правами пользователя, используемая обучающимся для подключения к SSH-серверу в течение выделенного для него времени. Для каждого обучающегося в заданное время устанавливается персональный пароль на систему учетную запись. Для предотвращения выполнения команд обучающимися на SSH-сервере необходимо заменить командную оболочку, к которой пользователь может получить доступ сразу после успешной аутентификации [4]. Примером такой оболочки для операционных систем семейства Linux является Iron Bars Shell, которая позволяет администратору устанавливать список разрешенных для выполнения команд [5].

Доступ к сетевому оборудованию обеспечивается SSH-сервером благодаря механизму перенаправления TCP-соединений, доступному после успешной аутентификации клиента. Для этого SSH-клиент открывает заданный пользователем локальный порт, все данные с которого будут отправляться SSH-серверу с отметкой о последующей передаче на запрошенные ip-адрес и порт [4].

На рис. 1 приведена схема защищенного удаленного доступа к сетевому оборудованию: приложение подключается к локальному порту 5555, который был открыт SSH-клиентом для перенаправления соединений к сетевому устройству с ip-адресом 10.0.0.1 на 80-й порт. Ко всем поступающим на порт 5555 данным добавляются служебные данные о перенаправлении (включающие ip-адрес 10.0.0.1 и порт 80). Получившийся массив данных передается по защищенному каналу до SSH-сервера, который считывает и удаляет служебные данные, а оставшиеся данные передает на считанные ip-адрес и порт.

Замкнутость сети на рис. 1 подразумевает невозможность установления исходящих соединений с какими-либо устройствами вне сети с оборудованием, входящие соединения возможны только от SSH-сервера.

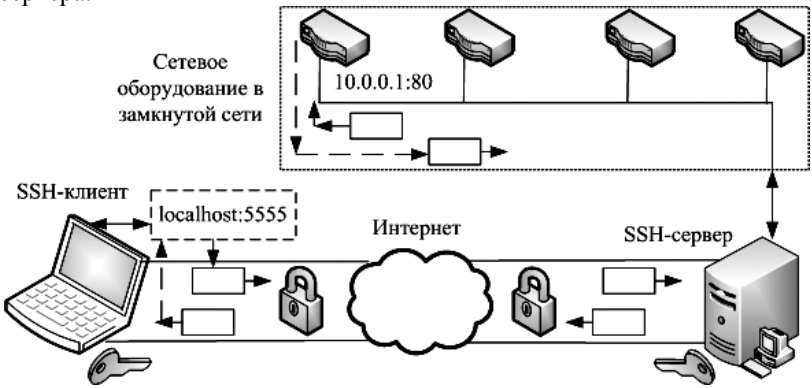


Рис. 1. Схема защищенного удаленного доступа к сетевому оборудованию

Для автоматизации управления временем удаленного доступа используется самостоятельно разработанное Web-приложение на языке PHP, доступное по протоколам HTTP/TLS и использующее механизм сессий для аутентификации. Администратор регистрирует пользователей в Web-приложении и назначает каждому из них временной промежуток для удаленного доступа к сетевому оборудованию. Указанное начальное время передается от PHP-сценария планировщику заданий операционной системы с задачей сгенерировать и установить новый пароль для системной учетной записи, а время окончания – с задачей отключения пользователя из системы, генерирования и установки нового случайного пароля для системной учетной записи, сохранения конфигурации сетевого оборудования и ее сброса в исходное состояние. Сохраненная в отдельный файл конфигурация становится доступна администратору через Web-интерфейс для анализа выполненной работы.

Пароли пользователей, хранящиеся в базе данных Web-приложения, хэшируются по алгоритму md5 и шифруются по симметричному алгоритму ГОСТ 28147–89 (режим CBC) с паролем администратора в качестве ключа шифрования. Шифрование, реализованное за счет PHP-модуля mcrypt, применяется к паролю от системной учетной записи, хранящемуся в базе данных Web-приложения и передаваемому в дальнейшем пользователю, с паролем пользователя в качестве ключа шифрования.

Вся информация для подключения передается пользователю через Web-приложение в виде пакетного (batch) файла, запуск которого в операционных системах семейства Windows установит сеанс связи с SSH-сервером с помощью SSH-клиента plink, а также откроет локальные порты, подключения к которым будут перенаправлены до сетевого оборудования.

Реализованный защищенный удаленный доступ предоставляет возможность подключения одному пользователю к сетевому лабораторному оборудованию в запланированное по расписанию время, предусматривает сохранение результата работы и подготовку сетевого оборудования для следующего пользователя, а также учитывает сформулированные требования безопасности.

ЛИТЕРАТУРА

1. NETLAB+ Product Overview [Электронный ресурс]. URL: http://netdevgroup.com/products/index.html (дата обращения: 10.02.2012).

2. RFC 4251. The Secure Shell (SSH) Protocol Architecture [Электронный ресурс]. URL: http://www.ietf.org/rfc/rfc4251.txt (дата обращения: 13.02.2012).

3. RFC 4253. The Secure Shell (SSH) Transport Layer Protocol [Электронный ресурс]. URL: http://www.ietf.org/rfc/rfc4253.txt (дата обращения: 15.02.2012).

4. RFC 4254. The Secure Shell (SSH) Connection Protocol [Электронный ресурс]. URL: http://www.ietf.org/rfc/rfc4254.txt (дата обращения: 20.02.2012).

5. Iron Bars Shell Features [Электронный ресурс]. URL: http://ibsh.sourceforge.net/feat.html (дата обращения: 10.02.2012).

МЕТОДИКА ДЕКОМПИЛЯЦИИ БИНАРНОГО КОДА И ЕЕ ПРИМЕНЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М.О. Шудрак, И.А. Лубкин, аспиранты

Научный руководитель В.В. Золотарев, доцент, к.т.н.

г. Красноярск, СибГАУ им. М.Ф. Решетнева, каф. БИТ, ИИТК, slender.bit@mail.ru

Сегодняь применение декомпиляция бинарного кода в сфере информационной безопасности ограничено, ввиду наличия в этом процессе ряда фундаментальных проблем.

Анализ бинарного кода является не тривиальной задачей, в силу того что в процессе компиляции исходного кода программы теряется важная с точки зрения анализа информация [1]. Таким образом, полученная в ходе декомпиляции информация часто не представляет практического интереса.

Однако декомпиляция занимает важное место в сфере информационной безопасности и может быть успешно использована в следующих областях:

- защита программного обеспечения;
- анализ вредоносных объектов;
- поиск уязвимостей.

В данной статье предлагается новый подход к декомпиляции бинарного кода и его применение к областям, которые описаны выше.

Процесс анализа бинарного кода требует некоторого уровня его абстракции от машинного кода к человеку [2]. Таким образом, основная идея описываемой методики заключается в том, что декомпиляция бинарного кода не требует представления машинного кода на языке высокого уровня, достаточно восстановить алгоритм функционирования участка анализируемого кода (тем самым добиться соответствующего уровня абстракции).

Методика интерпретации инструкций, предложенная авторами данной статьи, рассматривает инструкции как совокупность элементарных операций над ресурсами, где в качестве ресурса могут выступать регистры, память или регистры флагов процессора. Рассмотрим алгоритм работы декомпилятора подробно (рис. 1).

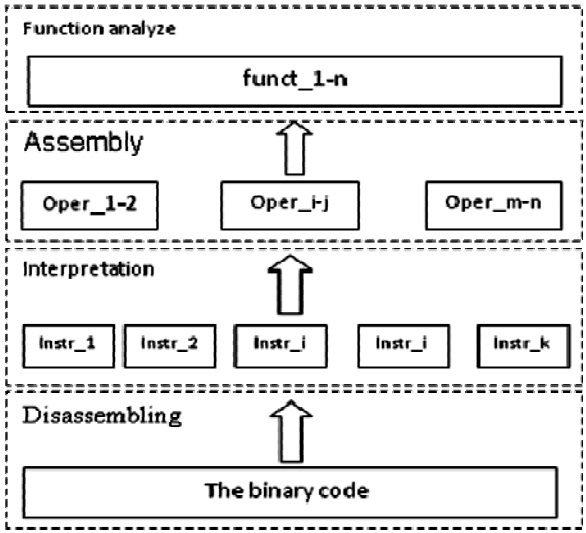


Рис. 1. Алгоритм анализа кода

Все операции в рамках методики были сгруппированы в общий базис, описывающий все множество возможных инструкций [3].

Для отображения информации об инструкции предлагается следующая схема: ресурс, соответствующий регистру, обозначается фигурными скобками, в которые заключён его номер. Ресурс оперативной памяти обозначается квадратными скобками, в которые заключён адрес ресурса. Номер такого ресурса выносится за скобки. Результат отделяется знаком «=». Операции и константы записываются «как есть».

Представленная форма записи позволяет представлять инструкции в виде математических формул. Например, инструкции add eax,ecx и inc eax запишутся в виде:

$$P2 = P1 + P0, \quad (1)$$

$$P3 = P2 + 1. \quad (2)$$

Тем самым наглядно показан процесс преобразования информации для участка машинного кода.

За этапом интерпретации согласно предлагаемому алгоритму декомпиляции следует этап сборки, идея такого процесса состоит в том, что ресурс – источник одной операции может выступать в роли приёмника в другой операции, таким образом, устанавливая связь между операциями на участке кода.

Развивая методику сборки, для установки связи между операциями было предложено использовать аппарат синтаксических деревьев для описания преобразований над ресурсами. В таком дереве узлы представляют собой операторы из базового набора операций, описанного выше, а листья соответствуют ресурсам или константам. Рассмотрим следующий пример для описания предложенного аппарата:

$$P2 = P0 + P1, \quad (3)$$

$$P4 = P2 * P3. \quad (4)$$

В результате итоговое выражение будет иметь вид

$$P4 = (P0+P1)*P3. \quad (5)$$

Синтаксическое дерево примет вид, как на рис. 2.

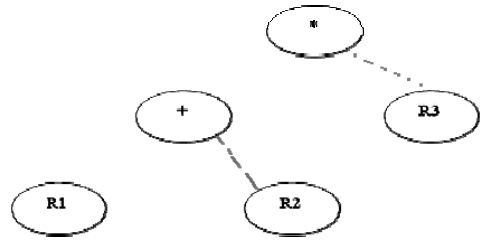


Рис. 2. Запись операций в виде бинарного дерева

Таким образом, для формирования итогового выражения необходимо осуществить рекурсивный проход по дереву вида {левый лист, узел, правый лист}. Выход из узла дерева формирует скобки в итого-

вом выражении. Такие деревья необходимо формировать для каждого ресурса, являющегося выходным.

Для определения выходных ресурсов можно использовать несколько утверждений:

1. Выходным называется тот ресурс, который не является промежуточным.

2. В качестве выходных ресурсов можно рассматривать ресурсы памяти (в том числе стек программы), регистры общего назначения, так как чаще всего он является выходным ресурсом при вызове функций.

В процессе полиморфной генерации бинарного кода встает задача учета ресурсов процессора, для обеспечения неизменности алгоритма работы участка кода, на котором производится генерация.

Для учета ресурсов процессора необходимо учитывать не только регистры и флаги процессора, но и регистры, которые используются для адресации памяти (например, mov [eax], 3), так как изменение регистров, используемых для адресации в памяти, в некоторых случаях, может привести к нарушению алгоритма работы участка кода.

Таким образом, для учета ресурсов процессора необходимо учитывать их изменения после каждой инструкции.

Для учета ресурсов процессора используется битовая маска регистров общего назначения, таким образом, для генерации кода возможно использовать только те регистры, чей флаг не взведен. Также стоит отметить, что регистры, чей флаг взведен, нельзя использовать в качестве приемника информации, в качестве источника информации для других регистров их использование оправдано, так как такая пересылка информации не вносит изменений в алгоритм работы участка кода.

Апробация вышеописанной методики проводилась на двух следующих задачах:

- защита участка программного кода;
- автоматизированный анализ полиморфного кода.

На практике любая атака на программное обеспечение основывается на предварительном анализе защитного механизма приложения, зачастую с использованием дизассемблирования бинарного кода. Цель такого исследования заключается в том, чтобы восстановить алгоритм защиты, выделить его слабые стороны или недокументированные возможности для его последующей модификации и (или) автоматизации процесса преодоления. Такое преодоление гарантированно достигается за конечное время вследствие конечности программы, а время, за которое злоумышленник преодолеет систему, зависит от сложности этой системы и его квалификации. Способствует такой ситуации широкий выбор инструментов для исследования программного кода.

Технология полиморфной генерации кода позволяет проводить запутывающие преобразование в бинарном коде защищаемого объекта. В рамках данной работы производится встраивание (вставка запутывающих инструкций между инструкциями защищаемого кода) запутывающего кода в бинарный код защищаемого объекта. Такое встраивания позволяет увеличить время, за которое злоумышленник восстановит алгоритм защиты, за счет усложнения исследуемого кода.

Методика генерации кода (описанная ранее) была реализована в виде программного средства, которое включает в себя ряд базовых модулей, таких как анализатор кода и генератор полиморфного кода, а также базу данных, содержащую набор инструкций и соответствующий им алгоритм.

Полученные результаты позволяют говорить об эффективности предложенной методики, количество операций на участке кода, количество входных и выходных ресурсов, а также результирующих формул возросло, что непременно приведет к росту ресурсов требуемых для исследования данного участка кода, что повышает защищенность описываемого участка от исследования.

Второй вариант апробации предложенной методики заключается в автоматизации анализа секций полиморфного кода вируса.

Полиморфный вирусный код – это код, который модифицирует сам себя (свое бинарное представление), при этом алгоритм, выполняемый участком кода, остается неизменным. Такой алгоритм представляет собой сигнатуру полиморфного вируса и может быть использоваться для обнаружения вируса.

Необходимо отметить, что для обнаружения полиморфного кода необходимо руководствоваться следующим утверждением: полиморфный код – это код, который не имеет выходных ресурсов и не участвует в их формировании.

Таким образом, используя вышеописанную методику декомпиляции бинарного кода, а также утверждение о полиморфном коде, была реализована программа, позволяющая детектировать полиморфные инструкции вирусного кода в автоматизированном режиме. Реализованное средство позволяет детектировать полиморфные инструкции без ручного (с использованием средств дизассемблирования) анализа вирусного кода. Однако необходимо отметить, что на данный момент описанное детектирование возможно лишь на линейных участках полиморфного кода (участок кода, без использования ветвления и вызова подпрограмм).

Таким образом, в данной статье были описана методика декомпиляции бинарного кода посредством применения оригинального алгоритма представления инструкции в алгоритмическом виде.

Необходимо отметить, что описанная методика декомпиляции может найти широкое применение в различных аспектах информационной безопасности, особенно в разделах, касающихся защиты программного обеспечения и анализа вредоносного кода, что и было продемонстрировано в предыдущих разделах.

ЛИТЕРАТУРА

1. Stiff G., Vahid F. New decompilation technique for binary-level co-processor generation / Computer-Aided Design, 2005. ICCAD 2005. IEEE/ACM International, San Jose, CA 2005.

2. Cifuentes C., Waddington T., Van Emmerik M. Computer security analysis through decompilation and high-level debugging / Reverse Engineering, 2001. Proceedings. Eighth Working Conference on,. un Microsyst. Labs, Palo Alto, CA, 2001.

3. Шудрак М.О., Лубкин И.А. Методика генерации полиморфного кода для защиты программного обеспечения // Решетневские чтения СибГАУ. 2-е изд. Красноярск, 2010. 566 с.

АНАЛИЗ ПОДХОДОВ К РЕАЛИЗАЦИИ ОБНАРУЖЕНИЯ СЕТЕВОГО ВТОРЖЕНИЯ

А.О. Шумская*, *студентка 4-го курса

Научный руководитель Г.А. Праскурин, ст. преподаватель

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, anastasia91@sibmail.com

Подобно тому, как важно защищать от вторжений свое жилище, устанавливая замки и сигнализацию, следует понимать важность защиты целостности и безопасности компьютерных систем и данных.

Доступ к сети Интернет облегчает передачу информации и работу системы, но в то же время делает ее более уязвимой. Чтобы администраторы безопасности узнавали о взломе и реагировали на него в реальном времени, им необходимы средства оповещения. Такими предупреждающими системами являются системы обнаружения вторжения (СОВ).

Традиционно в СОВ выделяют следующие основные элементы:

- подсистема сбора информации, которая используется для сбора первичной информации о работе защищаемой системы;
- подсистема анализа (обнаружения), которая осуществляет поиск атак и вторжений в защищаемую систему;
- подсистема представления данных (пользовательский интерфейс), которая информирует пользователя о состоянии защищаемой системы.

Для подсистемы анализа современных систем обнаружения вторжения выделяются 2 метода: обнаружение аномалий в защищаемой системе и поиск злоупотреблений [1].

В первом случае для защищаемой системы на основе совокупности параметров оценки формируется «образ» нормального функционирования. В современных СОВ выделяют несколько способов построения «образа»:

- накопление наиболее характерной статистической информации для каждого параметра оценки;
- обучение нейронных сетей значениями параметров оценки;
- событийное представление.

Следует отметить, что в обнаружении значительную роль играет множество параметров оценки. Поэтому в обнаружении аномалий одной из главных задач является выбор оптимального множества параметров оценки. В настоящее время используется эвристическое определение этого множества, использование которого должно дать наиболее эффективное и точное распознавание вторжений. Сложность выбора можно объяснить тем, что его составляющие зависят от типов обнаруживаемых вторжений. Поэтому одна и та же совокупность параметров не будет адекватной для всех типов вторжений.

Другой не менее важной задачей является определение общего показателя аномальности. Общая оценка аномальности должна определяться из расчета множества параметров оценки. Один из возможных методов – использование статистики Байеса.

Цель второго направления (обнаружение злоупотреблений) – поиск последовательностей событий, определенных как этапы реализации вторжения.

В отличие от обнаружения аномалии в данном случае образ – это представление несанкционированных действий злоумышленника, он также называется сигнатурой вторжения. Формируется сигнатура на основе тех же входных данных, что и при обнаружении аномалий, то есть на значениях параметров оценки. Они полезны не только при обнаружении вторжений, но и при выявлении попыток совершения незаконных действий (частичное совпадение сигнатур).

Наибольшее распространение СОВ получают в комплексе с другими средствами обеспечения безопасности информации. И хотя имеются некоторые перекрытия выполняемых функций, особенно с межсетевыми экранами, которые уже выполняют некоторые ограниченные функции обнаружения вторжений, поднимая тревогу, когда «срабатывает» соответствующее правило, отличие задач СОВ в том, что в них реализована всего одна функция, но она должна быть реализована качественно. Обнаружение вторжений в реальном масштабе времени,

особенно на высоких сетевых скоростях, требует значительного количества выделенных ресурсов, которые не может обеспечить ни один из межсетевых экранов, кроме самых дорогих и сложных.

ЛИТЕРАТУРА

1. Бобров А. Системы обнаружения вторжений [Электронный ресурс] / Институт механики сплошных сред. Электрон. текст. дан. [Б.м.], 2011. URL: http://www.icmm.ru/~masich/win/lexion/ids/ids.html (дата обращения: 01.03.2012).

РАЗРАБОТКА МЕТОДИКИ АНАЛИЗА ЗАЩИЩЕННОСТИ СЕТИ

Э.Р. Заитова, М.А. Швецова, Е.Г. Шубникова, студентки 4-го курса
Научный руководитель Г.А. Праскурин, ст. преподаватель каф. КИБЭВС
г. Томск, ТУСУР, ФВС, каф. РЗИ, zugzwangname@gmail.com

Анализ защищенности сети необходим при контроле и мониторинге защищенности компьютерных сетей (работающих как с секретной, так и с конфиденциальной информацией), при аттестации автоматизированных систем (компьютерных сетей) и сертификации средств вычислительной техники по требованиям действующих нормативных документов и требует обработки большого объема данных в условиях дефицита времени.

Актуальной задачей является разработка подхода, объединяющего множество моделей и методику для реализации детального анализа защищенности компьютерных сетей, решение которой остро необходимо, так как использование средств автоматизации детального анализа защищенности будет обеспечивать более высокий уровень безопасности компьютерных сетей [1].

Цель проекта: разработка методики анализа защищенности компьютерных сетей.

Для достижения данной цели необходимо решить следующие задачи:

− создание модели анализируемой компьютерной сети;

− разработка моделей компьютерных атак и нарушителя для анализируемой компьютерной сети;

− анализ существующих методов и средств анализа защищенности;

− разработка методики анализа защищенности сети.

Методика анализа защищенности сети позволит проектировщику и/или системному администратору сети определять уязвимости в используемом программном и аппаратном обеспечении, выявлять «узкие» места в безопасности компьютерной сети, моделировать поведение нарушителей, на основе чего принимать решения по составу ис-

пользуемых или планируемых к использованию средств обеспечения безопасности в комплексном сочетании [2].

Большинство систем анализа защищенности (XSpider, Internet Scanner, LanGuard, Nessus) обнаруживают уязвимости в операционных системах, а также в наиболее распространенном прикладном ПО. Существуют два основных подхода, при помощи которых системы анализа защищенности обнаруживают уязвимости: сканирование и зондирование.

При сканировании система анализа защищенности пытается определить наличие уязвимости по косвенным признакам, то есть без фактического подтверждения ее наличия – это пассивный анализ. Данный подход является наиболее быстрым и простым в реализации. При зондировании система анализа защищенности имитирует ту атаку, которая использует проверяемую уязвимость, то есть происходит активный анализ. Данный подход медленнее сканирования, но позволяет убедиться, присутствует или нет на анализируемом компьютере уязвимость.

При проведении сканирования сети был использован сетевой сканер Xspider (для выявления уязвимостей). Для проверки факта обращения сканера к соответствующему порту был применен сетевой анализатор трафика Wireshark (сниффер) – программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа либо только анализа сетевого трафика, предназначенного для других узлов.

После изучения основных инструментов атаки на компьютерные сети и средств защиты от них были разработаны модели атак с использованием различных схем действий злоумышленника, а также и способы защиты от этих атак. Например, была реализована атака ARP-spoofing – техника сетевой атаки, применяемая преимущественно в Ethernet, но возможная и в других сетях, использующих протокол ARP, основанная на использовании недостатков этого протокола и позволяющая перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена. Пример защиты от такой атаки – реализация защиты пакетов на сетевом уровне путем настройки службы IPSec.

До настоящего момента были рассмотрены требования нормативно-правовых документов к средствам защиты информации в компьютерных сетях, работающих с информацией разных степеней конфиденциальности. После чего были изучены сертифицированные средства защиты информации; исследованы наиболее распространенные СЗИ (demo-версии) по различным категориям. В частности, были рассмот-

рены средство антивирусной защиты DrWEB и программный комплекс VIPNet Custom.

Планируется, что результатом данного проекта станет методика анализа защищенности сети, позволяющая объективно оценивать различные показатели защищенности сети. Используя полученную методику, можно будет сделать выводы как о безопасности конкретного узла (рабочего места), так и о сети в целом.

При применении методики будут проведены всесторонние исследования системы с целью обнаружения уязвимостей, которые могут привести к нарушениям политики безопасности, и оценка возможности реализации атак.

Анализируя полученные результаты исследования с использованием методики, пользователь сможет сделать выводы:

− о характере выявленных уязвимостей, а также оценить возможные последствия их использования потенциальным нарушителем;

− о способах нейтрализации выявленных уязвимостей или снижения риска реализации угроз информационной безопасности;

− о состоянии защищенности критичных ресурсов и узлов сети от угроз, источники которых находятся как внутри исследуемой сети, так и вне ее.

Такая методика может применяться для однократного и постоянного мониторинга безопасности сети.

Областью применения результатов может стать и практическая, и научно-исследовательская деятельность. В практической сфере методика будет полезна для системных администраторов, экспертов и аналитиков по вопросам компьютерной безопасности, ответственных за анализ состояния информационной безопасности в целом. В научно-исследовательской деятельности методика может найти применение как составляющая часть мониторинга информационной безопасности предприятия, в области защиты сетей от несанкционированного доступа, а также для создания новых средств защиты.

Проект ГПО КИБЭВС-1003 – «Анализ защищенности сети».

ЛИТЕРАТУРА

1. Анализ защищенности вычислительной сети и методика его проведения // ITSEC.RU информационная безопасность. http://www.itsec.ru/articles2/Oborandteh/analiz_zaschischen_vy4islit_seti_metodika_ego_provedhttp://www.itsec.ru/articles2/Oborandteh/analiz_zaschischen_vy4islit_seti_metodika_ego_provedhttp://www.itsec.ru/articles2/Oborandteh/analiz_zaschischen_vy4islit_seti_metodika_ego_proved (дата обращения: 01.03.2012).

2. Котенко И.В., Степашкин М.В. Интеллектуальная система анализа защищенности компьютерных сетей на различных этапах жизненного цикла // Тр. междунар. науч.-техн. конф. «Интеллектуальные системы (AIS-05)» и «Интеллектуальные САПР (CAD-2005)». М.: Физматлит, 2005.

ФОРМАЛИЗАЦИЯ ПРОЦЕДУРЫ ВЫБОРА СОТРУДНИКА

А.А. Сметанин, аспирант каф. ВТ

Научный руководитель Е.Ф. Стукалина, доцент каф. СТИБ, к.т.н.

г. Ижевск, ИжГТУ, ИВТ, smtnin@gmail.com

Без объективной процедуры подбора персонала построить надежную систему защиты невозможно. В последние годы появился новый термин «инсайдер», означающий, что злоумышленник находится внутри контура безопасности, т.е. имеет легальный доступ ко всем процедурам идентификации и аутентификации. Процедура выявления такого нарушителя крайне сложна. Кроме того, согласно статистике чаще всего на предприятии имеют дело с так называемыми непредумышленными нарушителями информационной безопасности. Причины таких угроз хорошо изучены [1] и связаны с отсутствием трудовой дисциплины, непрофессионализмом и т. д. Вместе с тем в большинстве случаев работника подбирают по интуиции, по совету знакомых, по внешним признакам, используют метод «проб и ошибок». В данной ситуации важно применять некую методику подбора персонала, которая позволила бы автоматизировать процесс подбора и работы с персоналом и в дальнейшем минимизировала бы угрозы информационной безопасности в ее кадровой составляющей.

Представим процедуру подбора персонала в виде бизнес-процесса (рис. 1). Здесь на входе имеем некоторый набор входных параметров {Pu}, которые описывают претендента, и набор требований работодателя к претенденту {Pw}, а на выходе – управленческое решение по предъявленному кандидату.

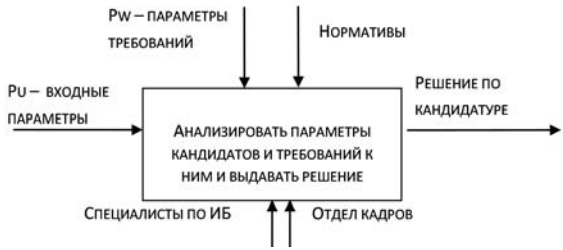


Рис. 1. Схема бизнес-процесса по подбору персонала

Для реализации процесса смоделируем систему отбора кандидатов.

Рассмотрим один из известных методов оценки качественных параметров путем перевода их в количественные с использованием балльной шкалы, описанный в [2]. Тогда параметры персонала T_i будем оценивать в баллах по формуле

$$T_i = \sum_j^n pt_j \ ,$$

где T_i – текущий показатель, pt_j – характеристика показателя.

Пусть максимальное значение показателя будет равно единице, тогда, основываясь на существующих методиках [1] подбора персонала, можно выставить средние константные значения показателей для инженерно-технических работников, которые можно представить в виде множества весов {0,7; 0,5; 0,9; 0,8; 0,6; 0,4}. Наличие количественных характеристик оценки кандидата дает необходимую формализацию, что позволяет выделить причинно-следственную связь принятия решений и в будущем автоматизировать этот процесс.

Традиционно для ранжирования кандидатов по их соответствию вакансии рассчитывается рейтинг как среднее арифметическое взвешенное:

$$P = \frac{\sum_i^n T_i X_i}{T_i},$$

где P – итоговый показатель эффективности и качества труда кандидата; X_i – оценочные критерии работы кандидата; T_i – коэффициенты весомости параметров, по которым проводится отбор.

Однако в настоящее время все большую популярность приобретают системы принятия решений на основе нечеткой логики, в частности, использование нечетких бинарных отношений. Использование нечетких входных данных упрощает процедуру формализации оценки кандидата, т.е. оценка по представленным выше показателям является достаточной. Такой подход позволяет сконцентрироваться на моделировании соответствия кандидата должности [3].

Следует отметить, что в настоящее время информационные технологии охватывают все большее количество пользователей. Вследствие этого можно считать, что каждый человек трудоспособного возраста где-то «засветился» или «засветится» в социальных сетях, форумах, твитерах и пр. Такая информация может стать хорошим дополнением к общему образу кандидата в сотрудники или для действующего персонала. Это позволит наполнить формализованную оценку кандидата актуальными данными, используя свободные источники информации.

Предложенные выше методики позволят создать автоматизированную систему подбора кадров, основанную на использовании современных методов анализа общедоступной информации, что снизит

трудоемкость процесса подбора персонала и повысит уровень защищенности информационных систем предприятия от угрозы внутренних утечек информации.

ЛИТЕРАТУРА

1. Белов Е.Б. Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. М.: Горячая линия – Телеком, 2006. 544 с.

2. Кабушкин Н.И. Основы менеджмента. М.: Новое знание, 2009. 336 с.

3. Круглов В.В., Дли М.И., Голунов Р.Ю. Нечёткая логика и искусственные нейронные сети. М.:Физматлит, 2001. 221 с.

СТРУКТУРА И ФУНКЦИИ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ

А.К. Новохрестов*, *Д.Ю. Минина*, *И.А. Сологуб*, *студенты 3-го курса

Научный руководитель М.А. Сопов, ст. преподаватель

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, pound_2007@mail.ru

В настоящее время быстро растет число коммерческих банков (КБ). В подавляющем числе КБ используются те или иные средства автоматизации, обычно в виде автоматизированных банковских систем (АБС). Степень автоматизации, а также ее технологическая база в разных банках сильно различаются.

Для успешного развития и устойчивости в конкурентной борьбе требуются комплексные системы. Такие системы, как правило, дают возможность подключения дополнительных модулей, предназначенных для облегчения работы банковского персонала и для автоматизации более сложных банковских операций.

Структурная схема АБС представлена на рис. 1. Схема составлена на основании изучения описаний реальных АБС (информации с официальных сайтов).

На основании имеющейся структуры АБС были выделены следующие функции:

1. Сбор, обработка и хранение информации о каждом клиенте – ведение подробного «досье» на каждого клиента, которое может включать в себя любую информацию об оплатах, кредитах, переводах и т.д.

2. Розничные банковские услуги – услуги, которые предоставляются пользователям малым, а также средним предприятиям. Для управления услугами данного сектора необходимы гибкие информационные технологии, которые способны быстро реагировать на изменяющиеся запросы бизнеса, а также на требования конкретной страны и рынка.

3. Предоставление единого интерфейса для всех сотрудников.

4. Создание единой программной среды для удобного взаимодействия операционных блоков.

Рис. 1. Структура АБС

5. Дистанционное банковское обслуживание – предоставление банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (т.е. без его визита в банк), чаще всего с использованием компьютерных и телефонных сетей.

6. Постоянное взаимодействие с другими банками.

7. Управление рисками и стратегическое планирование – идентификация, анализ рисков и принятие решений, которые включают максимизацию положительных и минимизацию отрицательных последствий наступления рисковых событий.

8. Предоставление отчетности – система отчетности позволяет получить любую информацию, хранимую в системе, обработанную и представленную в максимально удобной форме.

9. Работа с ценными бумагами на фондовом рынке.

10. Управление деятельностью банка.

11. Обеспечение безопасности.

Проект ГПО КИБЭВС-1103 – «Инженерия баз данных».

ЛИТЕРАТУРА

1. http://www.banki-delo.ru – Банковское дело – информация о банковской деятельности и банковских системах мира.

2. http://www.bankclub.ru – Клуб банковских аналитиков – информация об инновациях в банковской сфере, терминах, относящихся к банковской деятельности, методах анализа.

3. http://www.diasoft.ru – Diasoft – информция об АБС, разработанных компанией Diasoft.

АНАЛИЗ МЕТОДОВ ПОИСКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ КОДЕ

И.С. Созинова, С.Е. Черепанов, студенты 3-го курса

Научный руководитель Е.М. Давыдова, доцент каф. КИБЭВС, к.т.н.

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

Классификация уязвимостей программного обеспечения (ПО) специфической направленности [1], применимая для поиска уязвимостей в ПО, имеет следующий вид:

1) уязвимости по этапам создания ПО: определение требований, проектирование, реализация, тестирование, сопровождение;

2) уязвимости по способу возникновения: постоянные, непреднамеренные, преднамеренные;

3) уязвимости по типам воздействия: спуфинг-атака, брут-форс-атака, компрометация системы, внедрение в сессию пользователя, повышение привилегий, раскрытие системных данных, раскрытие важных данных, отказ в обслуживании, межсайтовый скриптинг, неавторизованное изменение данных, обход ограничений безопасности;

4) уязвимости по векторам атаки: локальные, удаленные, локальная сеть.

На основе полученной классификации можно получить схему взаимодействия включенных в нее критериев (рис. 1).

В настоящее время остро встает проблема проверки исходного кода на всевозможные уязвимости, обзор которых можно сделать при помощи ранее разработанной классификации. Основной же причиной возникновения уязвимостей по-прежнему является сжатость сроков создания программного обеспечения.

Как известно, тестирование программного продукта можно осуществлять двумя способами: ручная проверка, автоматизированное тестирование [2]. Но задач поиска уязвимостей сводится к отысканию автоматизированного решения.

Итак, в дальнейшем будем говорить об автоматизированном решении проблем поиска уязвимостей.

Схема методик поиска уязвимостей, существующих на данный момент, приводится на рис. 2.

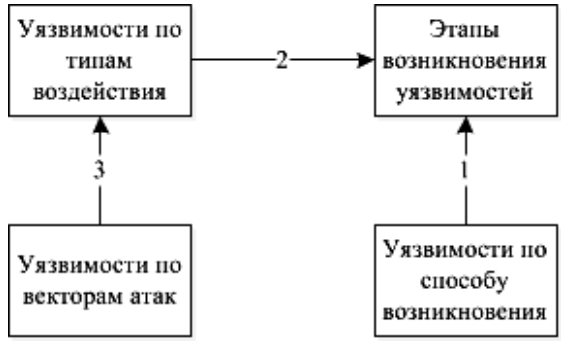


Рис. 1. Схема взаимодействия критериев классификации уязвимостей ПО: *1* – на каждом этапе жизненного цикла уязвимости могут быть заложены как преднамеренно, так и непреднамеренно, также не исключено наличие постоянных уязвимостей; *2* – для каждой уязвимости каждого этапа существует свой тип воздействия; *3* – для каждого типа воздействия существует свой вектор атаки

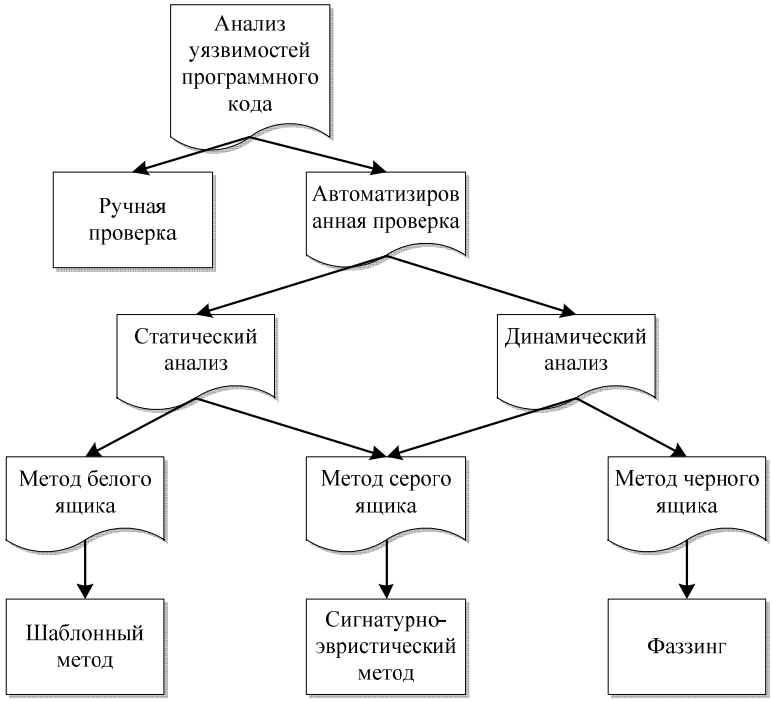


Рис. 2. Схема методик поиска уязвимостей

Статический анализ кода – анализ кода без его исполнения на его корректность. Недостатки:

– чем более динамичен язык, тем более расплывчатое представление мы можем получить о коде из статического анализа, отсюда проблемы ложных срабатываний;

– недостаточная интеллектуальность

– пропуск некоторых уязвимостей.

Особенность: результаты статического анализа по сложности интерпретации сопоставимы с исходными текстами [3].

Динамический анализ кода – проверка уже скомпилированной программы при исполнении.

Особенность: дополнительно требует составления и реализации соответствующих тестов маршрутов [3].

Решение проблемы выбора между статистическим и динамическим анализом.

Набор данных, подготовленный при функциональном тестировании, использовать для динамического анализа исходного кода. При этом провести статический анализ исходного кода [4].

Следствие: приемлемое покрытие исходного кода.

Итак, исследования выявили ряд недостатков в применяемых на сегодняшний момент методиках отыскания уязвимостей, которые используют различные сканеры и анализаторы кода. Были рассмотрены основные недостатки применения того или иного подхода, на основе чего можно судить о подходах к усовершенствованию сканера уязвимостей. При этом необходимо соблюсти основные критерии качественного анализа ПО: точность и полнота.

ЛИТЕРАТУРА

1. Созинова И.С., Черепанов С.Е. Классификация уязвимостей программного обеспечения // Современные тенденции в науке: новый взгляд: сб. науч. тр. по матер. междунар. заоч. науч.-практ. конф. 29 ноября 2011 г.: в 9 ч. Ч. 7 / М-во обр. и науки РФ. Тамбов: Изд-во ТРОО «Бизнес – Наука – Общество», 2011. 163 с.

2. Дастин Э., Рэшка Д., Пол Д. Автоматизированное тестирование программного обеспечения. М.: Лори, 2003.

3. Марков А., Миронов С., Цирлов В. Выявление уязвимостей в программном коде. Открытые системы.

4. Статический vs. динамический анализ. Хакеру.ru

О РЕШЕНИИ ЗАДАЧИ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ И КЛАССИФИКАЦИИ НАРУШИТЕЛЯ ПРАВ ДОСТУПА В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

А.П. Стефаров, аспирант каф. САиИО
Научный руководитель В.Г. Жуков, доцент каф. БИТ, к.т.н.
г. Красноярск, СибГАУ, vadimzhukov@mail.ru

Основной задачей исследований в области информационной безопасности является разработка новых и совершенствование имеющихся методов и средств защиты информации. Одной из задач мероприятий по защите информации является построение системы защиты информации.

Система защиты информации направлена на противодействие угрозам информационной безопасности, источниками которых, в том числе, являются нарушители. Она строится на основании модели нарушителя и модели угроз.

Алгоритм построения модели угроз и нарушителей, необходимый для построения системы защиты, представлен на рис. 1.

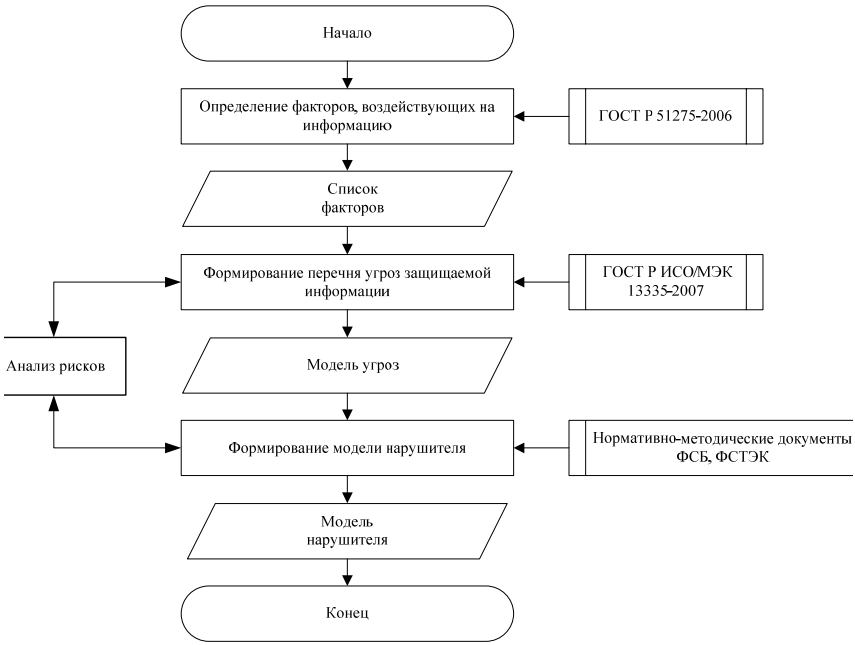


Рис. 1. Алгоритм построения модели угроз и нарушителей

На сегодняшний момент модель нарушителя носит неформальный характер. Результаты анализа государственных стандартов, нормативно-методических документов ФСТЭК России и ФСБ России, научно-технической литературы показали, что предложенные подходы, несмотря на то, что имеют ряд общих классификационных признаков, неполно описывают нарушителей, а категории нарушителей, описанные в различных источниках, не являются коррелированными.

Предложенная в [1] классификация нарушителей наиболее полно охватывает аспекты, которые рассмотрены научным сообществом и отражены в нормативно-методической документации, а также позволяет однозначно классифицировать нарушителя.

При построении модели угроз предлагается классифицировать угрозы, источником которых является нарушитель, в соответствии с уровнями воздействия нарушителей, полностью описанными в [1], что позволит упростить процедуру взаимодействия моделей угроз и нарушителей, необходимую для построения перечня актуальных угроз.

На основании полученных данных от модели угроз (уровни воздействия нарушителей, на которых существуют угрозы, перечень угроз) производится соотношение угроз с возможностями нарушителя той или иной категории.

Таким образом, предлагается провести классификацию нарушителей в соответствии с их уровнями воздействия на автоматизированную систему.

Основная идея подхода

Перечень угроз, классифицированных в соответствии с уровнями воздействия нарушителей, представляется в следующем виде:

$\{Y_i, L_1, L_2, L_3, L_4, L_5, L_6, L_7, L_8, L_9, L_{10}\}$, $i = [1; N]$,

где N – количество актуальных угроз; L_j – флаг, для обозначения j-го уровня воздействия нарушителей, для которого актуальна Y_i угроза, $j = [1; 10]$.

Методика определения категории нарушителя

В общем случае, процесс определения категории нарушителя сводится к следующему алгоритму:

1. Выбирается признак классификации из множества $L = (L_1, L_2, L_3, L_4, L_5, L_6, L_7, L_8, L_9, L_{10})$.

2. По значению выбранного j-го признака множество угроз Y_i разбивается на подмножества Y_{ij}.

3. Формируется вектор l существования актуальных угроз j-му уровню воздействия нарушителя по следующему правилу: j-й элемент вектора l равен единице, в случае если $|Y_{ij}|>0$ и нулю иначе.

4. Используя вектор l, определяется максимальная категория нарушителя в соответствии с таблицей, начиная с нарушителя первой категории (H_1).

Соотношение категорий нарушителя и уровней воздействия нарушителей

	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	L_9	L_{10}
H_1	**1**	**1**	0	0	0	0	0	0	0	0
H_2	**1**	**1**	0	0	**1**	**1**	0	0	0	0
H_3	**1**	**1**	0	**1**	**1**	**1**	0	0	0	0
H_4	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	0
H_5	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0
H_6	**1**	**1**	**1**	**1**	**1**	**1**	**1**	0	0	**1**
$H_{\text{внешн}}$	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Таким образом, строится перечень актуальных угроз для каждой категории нарушителей. В случае если были произведены исключения субъектов атак из числа потенциальных нарушителей, то представляется возможным уменьшить максимальную категорию нарушителя, а следовательно, и уменьшить количество актуальных угроз.

Однако предложенный подход достаточно статичен и требует периодического пересмотра автоматизированной системы, что не очень удобно на практике. Таким образом, дополнительно возникает задача разработки самонастраивающегося алгоритма оценки и классификации угроз и нарушителей. Предлагается использовать алгоритм, рассматривающий автоматизированную систему как две сопряженные подсистемы – «консервативную» и «оперативную».

«Консервативной подсистемой» будет являться АС, состоящая из автономного АРМ, не имеющего подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, а «оперативной» – изменения структуры АС, состава штатных средств в процессе эксплуатации АС. В соответствии с алгоритмом все новые признаки появляются сначала в «оперативной» подсистеме, проходят там проверку, после чего – передаются в «консервативную». Под проверкой следует понимать определение перечня актуальных угроз, характерных для вновь вводимых штатных средств, и определение категорий нарушителей, способных влиять на эти штатные средства. Необходимые данные выявляются при изменении структуры АС, отнесении вновь вводимых штатных средств к уровням воздействия нарушителей. На сегодня алгоритм находится на этапе тестирования.

ЛИТЕРАТУРА

1. Стефаров А.П. Модель нарушителя прав доступа в автоматизированной системе / А.П. Стефаров, В.Г. Жуков, М.Н. Жукова / Программные продукты и системы. 2012. №2. С. 51–54.

КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ «ИНФОРМАТИКА»

Е.Р. Тухбатуллин, студент 5-го курса, А.А. Конев, доцент
г. Томск, ТУСУР, каф. КИБЭВС, pancher86@mail.ru

Лабораторная работа – это практическое занятие, которое проводится с группой студентов, и целью такой работы является расширение возможностей использования теоретических знаний для решения практических задач.

Комплекс лабораторных работ по информатике создается для студентов первого курса, специальностей 090303 «информационная безопасность автоматизированных систем», и 090305 «информационно-аналитические системы безопасности». В соответствии с федеральными государственными образовательными стандартами высшего профессионального образования по направлению подготовки (специальности) 090303 и 090305 подготовка специалиста предусматривает изучение математического и естественнонаучного цикла, в который входит дисциплина «Информатика». Проектируемые результаты освоения математического и естественнонаучного цикла по дисциплине «Информатика», включают следующие требования. Студенты, прошедшие обучение по указанным выше специальностям, должны знать основные понятия информатики; формы и способы представления данных в персональном компьютере; состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; классификацию современных компьютерных систем; типовые структуры и принципы организации компьютерных сетей. Согласно рассмотренным стандартам студенты должны уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска и т.п.); пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет; применять персональные компьютеры для обработки различных видов информации. А также студенты должны владеть следующими навыками: навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов и т.п.); навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией и т.п.); навыками поиска и обмена информацией в глобальной сети Интернет.

В разрабатываемом комплексе лабораторных работ будут рассмотрены такие вопросы, как: работа с офисными приложениями,

включая текстовый процессор, электронные таблицы, презентации; работа с сетевыми средствами поиска и обмена информацией; работа с виртуальными операционными системами (ОС); основы работы в операционных системах семейства Windows и Linux как в графическом интерфейсе, так и в командной строке; восстановление данных операционных систем после сбоев; использование типовых средств обеспечения информационной безопасности.

В перечень ПО, которое планируется использовать в данных лабораторных работах, входят: ОС Windows 7 и Ubuntu 10.10, VirtualBox, MS Office 2010, антивирусы Avira, Eset Smart Security, веб-браузеры Internet Explorer и Mozilla Firefox, do-Pdf, 7-zip.

В результате работы были рассмотрены федеральные государственные образовательные стандарты высшего профессионального образования по специальностям 090303 и 090305, выявлены требования по дисциплине «Информатика» для данных специальностей, составлены перечень лабораторных работ и содержание предложенных работ, т.е. вопросы, которые необходимо проработать при составлении лабораторных работ, а также программное обеспечение, которое необходимо использовать при проведении лабораторных работ.

ЛИТЕРАТУРА

1. Портал «Российское образование» // Федеральный государственный образовательный стандарт высшего профессионального образования по специальности 090303 «информационная безопасность автоматизированных систем» [Электронный ресурс]. URL: http://www.edu.ru/db/cgi-bin/portal/spe/spe_new_list.plx?substr=090303&s t =all&qual=0 (дата обращения: 16.01.12).

2. Портал «Российское образование» // Федеральный государственный образовательный стандарт высшего профессионального образования по специальности 090305 «Информационно-аналитические системы безопасности» [Электронный ресурс]. URL: http://www.edu.ru/db/cgi-bin/portal/spe/spe_new_list.plx?substr=090305&st=all&qual=0 (дата обращения 16.01.12)

3. Трифонова Н.А., Прозорова С.С. Лабораторный практикум «Office для студента». Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2004. С. 20–48.

ТЕСТ НА СЛЕДУЮЩИЙ БИТ

Р.Р. Вильданов*, *студент 5-го курса; В.В. Маркин*, *инженер;
Р.В. Мещеряков*, *доцент*, *к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, ФВС, rivir@keva.su

Генераторы псевдослучайных последовательностей (ПСП) являются важнейшими элементами любой системы защиты, надежность

последней в значительной степени определяется именно свойствами используемых генераторов.

Качественные ПСП, являясь по своей сути детерминированными, обладают тем не менее практически всеми свойствами реализаций истинно случайных процессов и успешно заменяют их, так как случайные последовательности чрезвычайно сложно формировать.

Тестирование псевдослучайных последовательностей – совокупность методов определения меры близости заданной псевдослучайной последовательности к случайной. В качестве такой меры обычно выступает наличие равномерного распределения, большого периода, равной частоты появления одинаковых подстрок и т. п.

В настоящее время существуют несколько наборов тестов для анализа статистической безопасности генераторов ПСП – это графические тесты, тесты Дональда Кнута, Diehard, Dieharder, NIST STS, TestU01, Crypt-X, ENT и др.

Эндрю Яо доказал в 1982 г. что генератор, прошедший «тест на следующий бит», пройдет и любые другие статистические тесты на случайность, выполнимые за полиномиальное время [1]. Тест на следующий бит – тест, служащий для проверки генераторов псевдослучайных чисел на криптостойкость.

Распределение D ($D = G(X)$) – последовательность, создаваемая генератором, проходит тест на предсказание следующего бита, если для любого полиномиального алгоритма A и любого p верно:

$$\Pr_{t\in D}[A(t_1,...,t_p)=t_{p+1}]<\frac{1}{2}+v(|t|),$$

где $v(|\ t\ |)$ – обозначение функции, убывающей быстрее, чем обратный полином степени t.

Например, пусть кто-то написал полиномиальный алгоритм, который предсказывает следующий бит. Тогда возьмем последовательности, созданные генератором G, с вероятностями a, b, c, d, ... Затем берем p бит из одной последовательности и загружаем в другую. Если алгоритм угадывает следующий бит, то получаем выигрыш, равный вероятности последовательности. Если общий выигрыш ($\Pr_{t\in D}[A(t_1,...,t_p)=t_{p+1}]$) не слишком больше 1/2, то генератор G псевдослучаен.

На данный момент существуют по крайней мере два алгоритма, реализующих данный тест: алгоритм Садегияна–Махаери и «практический тест на следующий бит» (PNB, авторы Лавасани и Эглидос).

Алгоритм Садегияна–Махаери использует преимущество древовидной структуры, способной сохранить всю информацию о подпоследовательностях в общей последовательности. Алгоритм вычисления

m-битных последовательностей может быть представлен в виде двоичного дерева с взвешенными ребрами. В данном дереве каждый лист на глубине l хранит информацию о том, сколько раз встретилась данная l-битная последовательность. Так как дерево является взвешенным, то его каждому его ребру приписывается отношение количества, записанного в дочернем листе, к количеству, записанному в родительском. Для достаточно большой случайной последовательности предполагается, что числа, соответствующие рёбрам, будут примерно равны 1/2.

Алгоритм Садегияна-Махаери не дает ясного и точного критерия для определения случайности последовательности. Вместо этого создатели алгоритма предполагают возможность сделать некоторые выводы о общем поведении последовательности. Когда алгоритм успешно предсказывает (l+1) бит, то считается, что наступила локальная детерминированность.

«Практический тест на следующий бит» – основывается на алгоритме Садегияна-Махаери с некоторыми изменениями. Тест определяет отклонение в статистике появления следующего бита для подпоследовательности. Если же такое отклонение имеется – тест пытается использовать его для предсказания следующего бита. Последовательность считается неслучайной, если она содержит слишком много подпоследовательностей, чей последний бит предсказуем. Практический тест показывает более разумные результаты в сравнении с оригинальным тестом Садегияна-Махаери.

Тестирование последовательностей с использованием PNB показало [4], что данный тест является наиболее «сильным» из «сильнейших» тестов, используемых в пакете статистических тестов NIST STS.

ЛИТЕРАТУРА

1. Yao A.C. Abstract-Theory and application of trapdoor functions // Proc. 23rd IEEE Annual Symposium on Foundations of Computer Science (FOCS 1982), 1982. P. 80–91.

2. Goldwasser S., Bellare M. Lecture Notes on Cryptography [Электронный ресурс]. Режим доступа: http://cseweb.ucsd.edu/~mihir/papers/gb.pdf (дата обращения: 27.03.2012).

3. Sadeghiyan B., Mohajeri J. A New Universal Test for Bit Strings // ACISP'96 LNCS Series. Springer Verlag, 1996. P. 311–319.

4. Lavasani A., Eghlidos T. Practical Next Bit Test for Evaluating Pseudorandom Sequences [Электронный ресурс]. Режим доступа: http://www.scientiairanica.com/PDF/Articles/00001073/ eghlidos.pdf (дата обращения: 28.03.2012).

ИСПОЛЬЗОВАНИЕ TeX-РЕДАКТОРА ДЛЯ ОПИСАНИЯ МОДЕЛЕЙ БЕЗОПАСНОСТИ

Д.В. Волков, студент 4-го курса; Д.В. Кручинин, аспирант
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, kdv@keva.tusur.ru

Модель безопасности – система, функционирующая в соответствии со строго определенным набором формализованных правил и реализующая какую-либо политику безопасности.

Все математические модели безопасности компьютерных систем классифицируются по пяти основным видам:

1) модели систем дискреционного разграничения доступа;
2) модели систем мандатного разграничения доступа;
3) модели безопасности информационных потоков;
4) модели ролевого разграничения доступа;
5) субъектно-ориентированная модель изолированной программной среды.

Описание моделей безопасности проводят порой с использованием сложного математического аппарата. А для набора математических текстов предпочтительно использовать TeX-редактор.

TeX – это издательская система, предназначенная для набора научно-технических текстов высокого полиграфического качества, разработанная американским профессором информатики Дональдом Кнутом в целях создания компьютерной типографии.

В отличие от обыкновенных текстовых процессоров и систем компьютерной вёрстки, построенных по принципу WYSIWYG (What You See Is What You Get), в TeX'е пользователь лишь задает текст и его структуру, а TeX самостоятельно на основе выбранного пользователем шаблона форматирует документ, заменяя при этом дизайнера и верстальщика.

TeX можно использовать для всех видов текста, начиная с короткого письма и заканчивая многотомными книгами, причём изначально TeX создавался для более длинных текстов и научных работ. Многие большие научные издательства используют его для книгопечатания или книжного набора. Особую силу имеют как формульный набор, так и окно шрифта.

Список некоторых возможностей, предлагаемых стандартными макросами:

1) алгоритмы расстановки переносов, определения междусловных пробелов, балансировки текста в абзацах;
2) автоматическая генерация содержания, списка иллюстраций, таблиц и т.д.;

3) механизм работы с перекрёстными ссылками на формулы, таблицы, иллюстрации, их номер или страницу;

4) механизм цитирования библиографических источников, работы с библиографическими картотеками;

5) размещение иллюстраций (иллюстрации, таблицы и подписи к ним автоматически размещаются на странице и нумеруются);

6) оформление математических формул, возможность набирать многострочные формулы, большой выбор математических символов;

7) оформление графов, схем, диаграмм, синтаксических графов;

8) оформление алгоритмов, исходных текстов программ (которые могут включаться в текст непосредственно из своих файлов) с синтаксической подсветкой;

9) разбивка документа на отдельные части (тематические карты).

Краткий перечень TeX'овских достоинств:

1) никакая другая из существующих в настоящее время издательских систем не может сравниться с TeX'ом в полиграфическом качестве текстов с математическими формулами;

2) система TeX реализована на всех современных компьютерных платформах, и все эти реализации действительно работают одинаково;

3) благодаря этому TeX стал международным языком для обмена математическими и физическими статьями: набрав свою статью в TeX'е, математик может послать ее по электронной почте своему коллеге, даже если отправитель работает под Windows, а получатель – с UNIX'ом или, допустим, на Макинтоше;

4) в Интернете существуют обширные архивы препринтов, в которые каждый может послать (и из которых каждый может получить) статью; все эти статьи набраны опять-таки в TeX'е;

5) наконец, основные реализации TeX'а для всех платформ распространяются бесплатно.

Разумеется, у TeX'а есть и недостатки. Главный из них – в том, что с помощью TeX'а тяжело (хотя в принципе и возможно) готовить тексты со сложным расположением материала на странице (наподобие рекламных буклетов). Но такие приложения практически не встречаются в научно-технической литературе.

ЛИТЕРАТУРА

1. Девянин П. Н.. Модели безопасности компьютерных систем. М., 2005.
2. Львовский С.М. Набор и вёрстка в системе LaTeX // 2003. 3-е изд.
3. Воронцов К.В. LaTeX2 в примерах. М., 2005.
4. Электронный ресурс: http://www.itsec.ru/articles2/Inf_security/models/

АНАЛИЗ БЕЗОПАСНОСТИ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Д.К. Воротников, студент 3-го курса факультета МРМ
г. Новосибирск, СибГУТИ, vorotnikovdk@yandex.ru

В настоящий момент в IT-индустрии происходят крайне важные и значимые изменения. В рабочей деятельности и повседневной жизни увеличивается доля мобильных устройств в общем количестве используемых устройств. Мобильная техника становится все более и более популярной и со временем вполне способна встать на один уровень со стационарной [1].

Системы дистанционного банковского обслуживания (далее – ДБО) используются уже более десяти лет. Онлайн-банкинг предоставляется всеми крупными банками, и ежедневно им пользуется огромное число пользователей по всему миру. Поэтому системы ДБО являются основной целью киберпреступников. Киберпреступность – очень важный фактор, сдерживающий развитие финансовых сервисов, и поэтому системы защиты ДБО постоянно эволюционируют, и одним из наиболее эффективных методов стало использование двухфакторной аутентификации. А в связи с увеличением доступности мобильных устройств и постоянным расширением их возможностей они часто используются в системах двухфакторной аутентификации.

Главной целью киберпреступников является совершение несанкционированной транзакции. Механизмы аутентификации призваны защитить счета от несанкционированного доступа. Безопасная аутентификация современных систем ДБО может включать в себя элементы однофактороной аутентификации:

- проверку пары логин/пароль;
- использование контрольных вопросов;
- запрос дополнительной личной информации о владельце,

а также двухфакторной:

- данные о компьютере владельца;
- SSL сертификаты;
- смарт-карты;
- биометрические данные владельца;
- одноразовые пароли (OTP), получаемые с помощью:
  - карты переменных кодов;
  - генератора OTP (например, DigiPass);
  - OTP, получаемых на мобильный телефон по sms [2].

Наиболее устойчивыми перед атаками злоумышленников являются одноразовые пароли. Элементы двухфакторной аутентификации, связанные с компьютером, уязвимы перед вредоносным программным обеспечением (троянами-формграбберами), а однофакторной аутентификации – дополнительно перед фишингом и брутфорсом. Самым же удобным и понятным для пользователя является использование одноразовых паролей, получаемых в sms-сообщениях.

Атака на мобильные устройства получила название «Man-in-the-Mobile» (MitMo, «Человек в мобильном»). Основной функционал троянов, реализующих эту атаку, – это кража sms-сообщений с одноразовыми паролями систем ДБО и отправка их злоумышленнику. Из-за необходимости одновременного заражения и компьютера, и мобильного устройства трояны работают «в паре», сначала поражается компьютер пользователя, потом – мобильное устройство.

При рассмотрении двух троянских программ ZeuS-in-the-Mobile и SpyEye-in-the-Mobile становится видно, что они обе попадают в устройство благодаря заражению компьютера пользователя и методов социальной инженерии. Обе программы имеют версии для наиболее популярных мобильных платформ: Symbian, Android, Windows Mobile и Blackberry. Основной их функционал – пересылка sms-сообщений на номер злоумышленника или на веб-сервер. Основным недостатком, несомненно, является отсутствие эффективного метода заражения мобильного устройства. Другой важный изъян – минимальное сокрытие и простота удаления трояна. Кроме этого, можно выделить отсутствие возможности выбора номеров для пересылки и смены командного центра у SpitMo и Android-версии ZitMo [3, 4].

Для разработки более действенной концепции противодействия была предпринята попытка предвосхитить развитие событий в среде вирусописателей. Для повышения эффективности атак киберпреступникам необходимо обеспечить:

- кросплатформенность;
- эффективное распространение (поиск и эксплуатация уязвимостей «нулевого» дня);
- возможность выбора sms: все или только с определенных номеров;
- синтаксический анализ поступающих sms;
- сокрытие трояна в системе (использование rootkit-технологий [5]);
- сокрытие или удаление указанных sms;
- блокировку или перенаправление звонков с указанных номеров (на случай контрольного звонка);
- несколько вариантов отправки данных;
- возможность смены C&C;

• шифрование исполняемого файла трояна, конфигурационных файлов, передаваемых данных.

Для противодействия MitMo-атакам можно использовать различные методы. Самым старым и самым распространенным является метод сигнатурного анализа – определения вредоносных программ на основе совпадения с сигнатурами в базе антивируса. Связано это с начальной стадией развития троянов для мобильных платформ. Противодействие еще не детектирующимся вирусам обеспечивается проактивной защитой: эвристическим анализом файлов, анализом sms и http трафика, а также контролем доступа к звонкам, сообщениям и отправке данных по сети с целью выявления аномалий и блокировки нежелательной активности.

Эти методы нашли широкое применение в антивирусных программах для стационарных устройств. Но, к сожалению, подавляющее большинство современных антивирусов для мобильных платформ не использует данные методы, насколько возможно судить из описаний, доступных на сайтах производителей, а также trial-версий. Акцент в большей степени делается на защиту персональных данных владельца МУ, в том числе в случае потери или кражи устройства.

Кроме того, дополнительную защиту критичным данным, то есть одноразовым паролям, можно обеспечить, используя технику синтаксического анализа. Необходимо определять sms сообщения, содержащие важные данные по номерам или по ключевым словам, и выдавать пользователю предупреждение, если какое-либо из приложений пытается получить доступ к таким sms.

Безопасность любой системы должна обеспечиваться комплексно. Самая продуманная и функциональная антивирусная программа не способна защитить от атак, направленных на человека, – социальной инженерии. Поэтому важным этапом обеспечения безопасности должна явиться образовательная и воспитательная работа с пользователями систем дистанционного банковского обслуживания.

Мобильные устройства являются удобными и функциональными. Данная сфера в IT-индустрии развивается наиболее стремительно. В скором времени благодаря развитию техники и технологий мобильные устройства по своим техническим характеристикам догонят стационарные устройства, что можно отметить как тренд. Это приведет к частичному, а для некоторых – полному переходу сервисов на мобильные платформы. Затронет это и банковские системы. Соответственно подобное развитие должны будут пережить антивирусные программы и комплексы для обеспечения противодействия новым типам угроз. В перспективе никакой разницы в функционале программ для ПК и МУ не будет.

ЛИТЕРАТУРА

1. Группа компаний «Связной». Краткий обзор рынка смартфонов в России по итогам 3-го квартала 2011 г. [Электронный ресурс]. ГК «Связной», 2011. Режим доступа : http://www.svyaznoy.ru/info/press-centre/?ID=1435216, свободный. Загл. с экрана.

2. Шевченко А. Атаки на банковские системы [Электронный ресурс] // No bunkum. Журнал номер один о технологиях информационной безопасности. 2011. 12 ноября (№ 3). «NO BUNKUM», 2011. Режим доступа: http://nobunkum.ru/issue003/banker-attacks/, свободный. Загл. с экрана.

3. Масленников Д. ZeuS-in-the-Mobile – факты и догадки [Электронный ресурс] // Securelist – Всё об интернет-безопасности. 2009. 12 ноября. «Лаборатория Касперского». 1997–2011. Режим доступа: http://www.securelist.com/ru/analysis/208050718/ZeuS_in_the_Mobile_fakty_i_dogadki, свободный. Загл. с экрана.

4. Heyman A. First SpyEye Attack on Android Mobile Platform now in the Wild [Electronic resource] // Trusteer.com. 2011. Trusteer, 2011. Режим доступа: http://www.trusteer.com/blog/first-spyeye-attack-android-mobile-platform-now-wild. Загл. с экрана.

5. Papathanasiou C. This is not the droid you're looking for... [Electronic resource] / C. Papathanasiou, N.J. Percoc // A Whitepaper for DEF CON 18. 2011. Trustwave, 2011. Режим доступа: http://www.defcon.org/images/defcon-18/dc-18-presentations/Trustwave-Spiderlabs/DEFCON-18-Trustwave-Spiderlabs-Android-Rootkit-WP.pdf. Загл. с экрана.

ПРОЕКТИРОВАНИЕ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ТЕСТИРОВАНИЯ МОДУЛЯ АУТЕНТИФИКАЦИИ БАЗ ДАННЫХ MYSQL

Р.А. Воронкин, доцент каф. защиты информации;
А.А. Ягодкин, студент
г. Ставрополь, ФГБОУ ВПО «Северо-Кавказский государственный технический университет», zik@ncstu.ru

Социальные и экономические изменения в последние годы создали условия для широкого внедрения в России новейших информационных технологий, создания и использования перспективных информационных, телекоммуникационных систем связи и обработки информации баз данных как в государственном, так и в негосударственном секторах экономики.

В российском сегменте рынка большой процент составляют СУБД с открытым кодом. В период 2008–2010 гг. был 2,5-кратный рост применения в России СУБД с открытым кодом, в 2011 году доля использующих их компаний продолжила рост. Можно предположить, что на фоне финансового кризиса рост интереса к открытому ПО и в российском, и в мировом корпоративном сегменте будет усиливаться.

Учитывая прогресс Интернета России в последние годы, рост открытых баз данных с 25 до 63% закономерен.

Одним из ключевых игроков на российском рынке является СУБД MySQL от компании Oracle. MySQL – СУБД с открытым исходным кодом и без должной поддержки крайне уязвима. Одной из основных уязвимостей является ее модуль аутентификации. Для нахождения проблем с целью их устранения была разработана распределенная система тестирования.

Основные особенности программы тестирования:

– два режима работы – самостоятельной, или программы, входящей в состав распределенной системы;

– удобство пользования, клиент-серверные технологии в разы уменьшают занимаемое программой пространство;

– журнал событий – предназначен для фиксации действий пользователя и выявления уязвимых мест в целевом модуле авторизации;

– подключаемые словари позволяют увеличивать глубину проверки модуля аутентификации;

– распределение процесса тестирования позволяет сократить время работы программы и получения результатов;

– простой и эффективный способ аутентификации, основанный на логин-пароле, контроль логин-пароля проводится на удаленном сервере системы;

– исполняемый файл программы обфусцирован для противодействия анализу и модификации программы при декомпиляции.

Статическая модель программы тестирования представлена диаграммой классов на рис. 1.

Программа осуществляет свою работу в двух режимах:

1. Режим автономной работы. В случае выбора режима автономной работы пользователь может проверить лишь единичную комбинацию авторизационных данных, после тестирования происходит фиксация события в локальном журнале или возврат к выбору.

2. Режим работы с подключаемыми словарями. В случае режима работы со словарями пользователю необходимо ввести комбинацию логин-пароль, зарегистрированную в системе. Устанавливается подключение к серверу системы, программа производит запрос для проверки соответствия указанных логина и пароля. Если введенные логин и пароль неверны, то пользователю выводится сообщение об ошибке и производится возврат к выбору режима.

В случае правильности логин-пароля, на основе словарей отрабатываются подключения к целевой базе данных. Если целевой сервер сообщает о выполненном успешном подключении или ошибке, собы-

тие фиксируется в журнале системы и журнале пользователя программы. Если за время работы программы подключение не будет установлено, то программа закончит работу с предложенными ей параметрами.

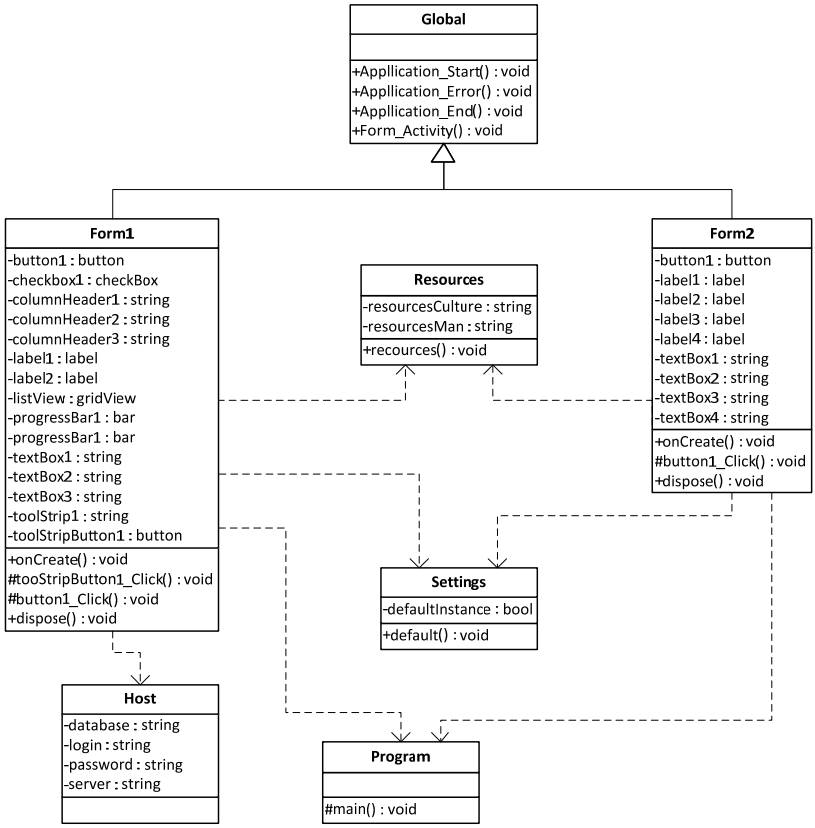


Рис. 1. Диаграмма классов программы тестирования

Режим работы со словарями допускает работу одного пользователя с несколькими программами одновременно.

Таким образом, использование данной программы позволит предотвратить утечку конфиденциальной информации, хранимой в базах MySQL, поможет разработчику оценить устойчивость модуля аутентификации баз данных при проведении распределенных атак и провести анализ адекватности используемых в нем методов защиты на этапе построения.

ЛИТЕРАТУРА

1. Нейгел К., Ивьен Б., Глинн Д., Уотсон К., Скиннер М. C# 4.0 и платформа .NET 4 для профессионалов. М.: Вильямс, 2011. 1440 с.

2. Алферов А.П. Основы теории баз данных : учеб. пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин и др. 2-е изд., испр. и доп. М.: Гелиос-АРВ, 2002. 480 с.

3. Хомоненко А.Д. Базы данных: учеб. для вузов / А.Д. Хомоненко, В.М. Цыганков, М.Г. Мальцев. СПб.: КОРОНА, 2004. 736 с.

МЕТОДИКИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.С. Яценко*, *аспирант

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

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

На фоне всеобщей информатизации и осознания необходимости осуществления информационной безопасности приходит осознание необходимости проведения аудита информационной безопасности [1] в организации для поддержания систем защиты в актуальном состоянии [2].

Существуют различные методики аудита информационной безопасности, использующие различные подходы и предоставляющие разные возможности аудиторам. Далее приводятся этапы проведения процедуры аудита информационной безопасности, их классификация по используемому подходу с его описанием и возможностями.

Процедура проведения аудита информационной безопасности делится на 4 этапа [3]:

1) подготовительный этап, на котором происходит заключение договоров, определение границ аудита и определение ответственных лиц;

2) определение информационных источников – происходит согласование источников, из которых будет браться информация для аудита, формат общения аудиторов с персоналом и руководителями организации;

3) сбор данных – производится сбор данных из источников, определенных на предыдущем этапе, собеседования с персоналом, проведение тестирований и т.д.;

4) анализ данных и выработка рекомендации – производится анализ собранной информации и выносятся рекомендации по устранению найденных несоответствий и узких мест, по изменению конфигурации средств защиты или использованию других. Вся эта информация закрепляется в итоговом отчете.

Существующие методики аудита, исходя из используемого подхода, можно разделить на 3 типа:

1) методики, основанные на проверке соответствия стандартам информационной безопасности;
2) методики, основанные на оценке рисков;
3) методики активного аудита.

Алгоритм оценки защищенности методик аудита первого типа состоит в проверке действующих в организации процессов и подходов на соответствие требованиям стандарта. В результате такого аудита выносятся рекомендации по приведению объекта аудита в соответствие стандарту. Ярким примером таких методик аудита является аудит на основе стандарта ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства защиты информации. Системы менеджмента информационной безопасности. Требования». Данный стандарт содержит ряд требований к системам менеджмента информационной безопасности, документации, управлению ресурсами и внутреннему аудиту [4].

Алгоритм оценки защищенности, методик аудита информационной безопасности второго типа состоит в оценке рисков с использованием экспертного подхода. В процессе такого аудита эксперты производят идентификацию и оценку рисков, влияющих на состояние информационной безопасности организации. Также происходит оценка уязвимостей, через которые данные угрозы могут быть осуществлены. После этого выносятся рекомендации, основанные на данных анализа и возможных путях решения. Риски должны быть приняты, минимизированы, перенесены или отвергнуты (т.е. организация должна отказаться от деятельности, из-за которой возникают данные риски). Исходя из принятых решений составляется комплекс мероприятий (мер), который должен привести риски к приемлемому уровню. После реализации комплекса мероприятий должен быть проведен анализ остаточных рисков [5]. В пример методики второго типа можно привести методику, реализованную в программном комплексе ГРИФ, разработанную компанией Digital Security.

Алгоритм оценки защищенности методик аудита третьего типа состоит в проведении тестирования на проникновение компьютерных сетей организации и их компонентов. По ходу проведения оценки, специалистами с использованием автоматизированных средств или вручную проводится поиск уязвимостей сети, которые можно использовать для получения доступа к ресурсам сети, или дополнительной информации об используемом программном обеспечении, средств защиты, сетевом оборудовании и архитектуры сети. Помимо тестирования компонентов сети, используют методы социальной инженерии для

получения важной информации от сотрудников организации, что порой тоже является очень результативным. Собранная информация анализируются и проводится попытка проникновения, для оценки опасности найденных уязвимостей. На основании результатов проверки составляется список уязвимостей с указанием уровня опасности, а также выносятся рекомендации по изменению действующих политик безопасности, используемых конфигураций средств защиты информации и используемого программного обеспечения для ликвидации найденных уязвимостей, представляющих реальную опасность [6, 7]. Пример такой методики приведен в стандарте NIST SP800-115 «Technical Guide to Information Security. Testing and Assessment».

Перечисленные типы методик аудита информационной безопасности давно себя зарекомендовали и используются международными аудиторами. Они дают возможность оценить текущее состояние информационной безопасности и выбрать соответствующие меры защиты информации, но, к сожалению, не содержат инструментов, позволяющих прогнозировать изменения состояния информационной безопасности на основе информации о текущем состоянии системы защиты. Хотя в последнее время появились методики аудита информационной безопасности, использующие математический аппарат для прогнозирования состояния информационной безопасности [8, 9], но данная область все равно требует дальнейшего изучения и развития.

ЛИТЕРАТУРА

1. ГОСТ Р 50922–2006 «Защита информации. Термины и определения».

2. Курило А.П. Аудит информационной безопасности. М.: БДЦ-пресс, 2006. 304 с.

3. СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы РФ. Аудит информационной безопасности».

4. ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства защиты информации. Системы менеджмента информационной безопасности. Требования».

5. ISO/IEC 27005 «Information technology – Security techniques – Information security risk management».

6. NIST SP800-115 «Technical Guide to Information Security. Testing and Assessment».

7. Open Source Security Testing Methodology Manual (OSSTMM).

8. Политов М.С. Экспериментально-аналитический метод оценки и прогнозирования уровня защищенности информационных систем на основе модели временных рядов. Дис. … канд. тех. наук: 05.13.19 / Уфимский государственный авиационно-технический университет, 2010. 145 с.

9. Ерохин С.С. Методика аудита информационной безопасности объектов электронной коммерции. Дис. … канд. тех. наук: 05.13.19/ Том. гос. ун-т систем управления и радиоэлектроники, 2010. 128 с.

РАЗРАБОТКА ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

А.В. Южаков, студент 4-го курса
Научный руководитель Ю.М. Филимонов, доцент
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, artem.tghcd@gmail.com

Роль случайных чисел велика при генерации ключей, в протоколах аутентификации, в схемах цифровых подписей, а также в некоторых алгоритмах шифрования. При таком применении безопасность значительно зависит от качества источника случайности. Из-за большого количества ограничений таким источником чаще всего может стать лишь аппаратный генератор случайных чисел.

Имеющиеся на рынке устройства не всегда пригодны для конечного потребителя. Основной причиной для этого являются завышенные цены на такие разработки. Не следует исключать и возможные слабые стороны таких генераторов, которые были допущены по недосмотру или намеренно.

При использовании аналоговых приборов полученный оцифрованный шум часто имеет низкую энтропию и/или плохие статистические параметры выходного потока. Пост-обработка вывода для улучшения статистических параметров создает риск сокрытия некоторых возможных дефектов генератора. Причем эта ошибка может остаться незамеченной даже при прохождении стандартных статистических тестов [1].

В последнее время интерес исследователей и разработчиков все больше привлекает генерация случайных чисел с помощью логических элементов, которые могут быть созданы в том же технологическом цикле, что и остальные элементы генератора, а также не требует оцифровки.

В настоящей работе рассматривается создание генератора случайных чисел на основе логических элементов. На рис. 1 рассматривается упрощенная схема данного генератора [1].

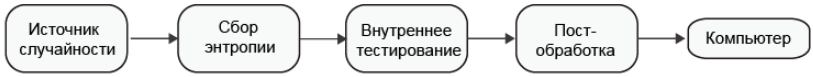
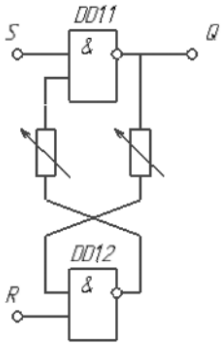


Рис. 1. Общая структура аппаратного генератора случайных чисел

В данном генераторе источником энтропии является метастабильное состояние логического элемента – триггера. При подаче на оба входа триггера (обозначены как *S* и *R* на рис. 2) активных уровней и последующем их снятии, состояние выхода будет неопределенным (выход *Q*), т.е. оно будет определяться тем элементом, который пере-

ключится позже. Регулировка задержки до граничного уровня и исключение внешних воздействий может позволить получить сигнал, случайность которого обусловлена переходными процессами в триггере.



В данной работе регулировка задержки была проведена при помощи переменных резисторов, однако выяснилось, что из-за слишком грубой настройки (номинал резистора составлял 550 Ом), не удается достичь граничного уровня.

Рис. 2. Схема триггера с потенциометрами

В дальнейшем планируется применить в разработке микропроцессор. Микропроцессор со встроенным USB-контроллером играет сразу 3 роли: реализует связь между компьютером и устройством посредством USB-интерфейса, выполняет постобработку и встроенные статистические тесты, а также регулирует величину задержки с помощью цифроаналогового преобразователя. Тесты необходимы для оповещения о дисфункции, причиной которой мог стать сбой, наведение помех или атака злоумышленника. Пост-обработка осуществляет приведение потока к необходимому распределению или уменьшает смещение и корреляцию, в случае необходимости.

Подстройку граничной задержки возможно реализовать при помощи цифроаналогового преобразователя, задавая уровень опорного напряжения в несколько милливольт. Таким образом, можно достичь значительно большей точности, чем при применении потенциометров.

Преимущества разрабатываемого генератора:

– произвольное тактирование (в пределах возможностей используемой элементной базы);

– простота;

– дешевизна.

Проект ГПО КИБЭВС-0907 – «Аппаратный генератор случайных чисел».

ЛИТЕРАТУРА

1. True Random Number Generators in Configurable Logic Devices: 2009. [Электронный ресурс]: The Montpellier Laboratory of Informatics, Robotics, and Micro-electronics, 2009. URL: http://www.lirmm.fr/~w3mic/ANR/PDF/D2.pdf

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА И АНАЛИЗА РИСКОВ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

А.Е. Заболотникова, студентка 5-го курса каф. ИСТМ
г. Красноярск, СФУ, ИКИТ, anastasenokn@mail.ru

В связи с глобальной информатизацией современного общества широкое распространение получили системы электронного документооборота (СЭД). Обеспечение минимального уровня защиты документооборота достигается с помощью выполнения требований и рекомендаций нормативно-методических документов. Системы анализа угроз и рисков позволяют оценить возможные угрозы системы и выбрать наиболее подходящие меры по их снижению или устранению, что обеспечивает стабильность функционирования СЭД.

Целью работы является создание автоматизированной системы, производящей анализ рисков, и получение адекватных оценок защищенности СЭД.

Результатом работы автоматизированной системы является отчет, в котором отражены анализ рисков информационной безопасности СЭД и показатели эффективности внедрения комплекса мероприятий контрмер.

Описание модели СЭД. Анализ рисков информационной безопасности осуществляется с помощью построения модели СЭД. Авторами предлагается использовать концепцию модели на основе композитного документооборота, представленную в работе [1]. Главным преимуществом такой модели являются: простота реализации, возможность адаптации к любому типу организации и возможность модификации модели в процессе ее построения.

Для построения критериев эффективности в модели композитного документооборота информационная система отображается взаимодействием компонентов трех множеств [2]:

- множество участников;
- множество действий участников;
- множество состояний документов.

Для описания множества участников необходимо составить список всех сотрудников, пользователей системы электронного документооборота. Для описания множества состояний необходимо составить подробный список документов и список производимых действий с документами участниками системы документооборота. Все документы разделяются на категории ценности информации и составляются в соответствующий список по убыванию ценности информации, содержа-

щейся в документе. Основным критерием при определении особой ценности документа является содержание документа.

Таким образом, входными данными для автоматизированной системы является следующая информация о СЭД:

- перечень ресурсов с ценной информацией;
- физические связи ресурсов друг с другом;
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации;
- группы пользователей, имеющих доступ к ценной информации, и их права доступа;
- средства защиты информации.

Исходя из введенных данных, строится модель СЭД, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Расчет рисков для угроз информационной безопасности СЭД. Риск реализации угрозы информационной безопасности для каждого вида информации рассчитывается по трем основным угрозам: конфиденциальность, целостность и доступность. Информационные риски системы документооборота рассчитывается по формуле (1):

$$R = P^*C, \quad (1)$$

где R – информационный риск; P – вероятность реализации угрозы; C – ценность документа (ущерб от реализации угрозы).

Задание контрмер. Выбор защитных мер для понижения риска осуществляется в соответствии с ГОСТ Р ИСО/МЭК ТО 13335-4–2007 и ГОСТ Р ИСО 15489-1–2007.

Получение оценки снижения рисков основывается на предположении, что вероятность успешной атаки на укрепленную систему задается соотношением (2):

$$Pnew = Pold^*(«Старое_время» / «Новое_время»), \quad (2)$$

где Pold – вероятность успешной атаки в базовой (старой) конфигурации; «Старое_время» – ожидаемое время успешной атаки с минимальной длительностью в базовой (старой) конфигурации; «Новое_время» – ожидаемое время успешной атаки с минимальной длительностью в укрепленной (новой) конфигурации.

Алгоритм работы автоматизированной системы. На первом этапе осуществляется ввод исходных данных в систему:

- список ценных информационных ресурсов с указанием ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по трем видам угроз:

- список пользователей информационных ресурсов с указанием прав их доступа;
- перечень средств защиты информации на ресурсах.

На втором этапе формируется модель СЭД с точки зрения информационной безопасности. Далее пользователь имеет возможность задавать контрмеры из перечня имеющихся.

В результате работы алгоритма программа представляет отчет, содержащий данные об:

- инвентаризации и значениях риска для каждого ценного ресурса;
- остаточных рисках;
- эффективности выбранных контрмер.

Автоматизированная система предусматривает возможность отслеживания изменений возможных рисков СЭД во времени и отображение динамики в наглядной форме. Также предусмотрена возможность пополнения баз данных угроз и защитных контрмер, что усиливает эффективность работы данной системы.

ЛИТЕРАТУРА

1. Круковский М.Ю. Концепция построения моделей композитного документооборота // Математичні машини і системи. 2004. № 2. С. 149–163.

2. Круковский М.Ю. Методология построения композитных систем документооборота // Математичні машини і системи. 2004. № 1. С. 101–114.

3. Данилов А.Д. Ценность информации и технологии «электронного правительства» / Технологии информационного общества. Интернет и современное общество: Тр. VIII Всерос. объедин. конф. Санкт-Петербург, 8–11 ноября 2005 г. СПб.: Филологический факультет СПбГУ, 2005. С. 136–140.

4. Золотарев В.В., Данилова Е.А. Управление информационной безопасностью: учеб. пособие: В 3 ч. Ч. 1. Анализ информационных рисков / Сиб. гос. аэрокосмич. ун-т. Красноярск, 2010. 144 с.

МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Э.Р. Заитова, М.А. Швецова, Е.Г. Шубникова, студентки 4-го курса
Научный руководитель Г.А. Праскурин, ст. преподаватель каф. КИБЭВС
г. Томск, ТУСУР, каф. РЗИ, zugzwangname@gmail.com

Для обеспечения информационной безопасности в автоматизированных системах управления, построения эффективной системы защиты информации недостаточно выявить каналы утечки информации, проанализировать возможные угрозы, последствия их реализации и оценить потери. Нужно еще хорошо представлять облик нарушителя.

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций по ошибке, незнанию или осознанно, использующее для этого различные возможности, методы и средства.

Одной из важнейших составляющих вероятного сценария осуществления противоправных действий по доступу к информации является модель нарушителя. Наличие такой модели нарушителя безопасности, которая постоянно корректируется на основе получения новых знаний о возможностях нарушителя и изменениях в системе защиты, на основе анализа причин произошедших нарушений, позволит повлиять на сами эти причины, а также точнее определить требования к системе обеспечения информационной безопасности от данного вида нарушений [1].

Основные подходы к созданию модели нарушителя описаны в нормативно-правовых документах ФСТЭК и ФСБ, таких как: РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и т.д. [2].

При создании модели нарушителя информационной безопасности хорошим дополнением может стать использование форензики – науки, позволяющей точнее оценить, какие преступления в области компьютерных сетей может совершить злоумышленник, а также составить полную картину о средствах, использованных им.

Модель нарушителя определяет:

- категории (типы) нарушителей, которые могут воздействовать на объект;
- цели;
- используемые методы и средства; последовательность действий нарушителей.

Исходя из вышеперечисленных документов, для создания модели нарушителя необходимо определить:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);

• ограничения и предположения о характере возможных действий нарушителей.

Для каждого конкретного случая создается собственная модель, и определяется вероятность применения той, или иной атаки, причем в отдельных случаях возникает необходимость моделирования нескольких сценариев действий нарушителя.

Проект ГПО КИБЭВС-1003 – «Анализ защищенности сети».

ЛИТЕРАТУРА

1. Модель нарушителя информационной безопасности // AVOIDANCE.RU: Статьи об информационной безопасности. URL: http://avoidance.ru/ articles/narushiteli-informacionnoj-bezopasnosti/58-model-narushitelja.html (дата обращения: 01.03.12).

2. РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

СФЕРЫ ПРИМЕНЕНИЯ АТРИБУТНЫХ СЕРТИФИКАТОВ

Н.С. Михайлов, аспирант; А.О. Заяц, студент

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, pancher86@mail.ru

Сертификат открытого ключа, сертификат ключа проверки электронной подписи (согласно ст. 2 Федерального закона от 06.04.2011 «Об электронной подписи» № 63-ФЗ) [1] – цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа.

Большинство сертификатов открытых ключей подписи имеют срок действия один или два года. Сертификаты могут использоваться для аутентификации пользователей, и информация, идентифицирующая субъекта, может учитываться при принятии решения об управлении доступом. Но иногда авторизация имеет меньший срок действия, чем сертификат открытого ключа. Использование дополнительной информации о субъекте в качестве авторизации, указывается в дополнениях сертификата открытого ключа, но это не является выходом по двум причинам. Во-первых, подобный сертификат должен аннулироваться при любых изменениях данных о субъекте. Во-вторых, удостоверяющий центр (УЦ), выпускающий данный сертификат, не имеет полномочия подписывать эту информацию, а должен связываться с источником информации о правах доступа конкретного пользователя.

Для решения данных проблем вводится понятие атрибутного сертификата. Он связывает атрибуты прав доступа с владельцем сертификата. Атрибутный сертификат не содержит открытого ключа, поэтому

его используют вместе с сертификатом открытого ключа. Аутентификация субъекта осуществляется при помощи сертификата открытого ключа, а связывание атрибутов с данным субъектом – посредством атрибутного сертификата. Поэтому сертификат открытого ключа называют – «электронным паспортом», связывающим субъект и открытый ключ, а АС – «электронным пропуском», т.е. это источник дополнительной информации об идентифицированном ранее субъекте.

Атрибутный сертификат имеет такой же формат, как сертификат открытого ключа, но другие функциональные возможности. Для наглядного представления структура АС изображена в таблице.

Структура атрибутного сертификата

Версия (v.1 или v.2)
Владелец сертификата
Имя издателя
Идентификатор алгоритма подписи
Серийный номер
Период действия(не ранее/не позднее)
Атрибуты
Уникальный идентификатор изделия
Дополнения

Владелец атрибутного сертификата характеризуется подобно субъекту сертификата открытого ключа подписи, но может быть задан по имени, издателю и серийному номеру сертификата открытого ключа либо при помощи хэш-кода сертификата или открытого ключа. Атрибуты описывают информацию о полномочиях владельца атрибутного сертификата. Как и сертификат открытого ключа подписи, атрибутный сертификат может содержать дополнения. Наряду с имеющимися в системе сервисами аутентификации, атрибутные сертификаты обеспечивают защищенную передачу информации о полномочиях их владельцев.

По предварительному анализу некоторых видов деловой активности можно явно выделить приложения использования такого рода «удостоверяющего свидетельства»:

− бизнес-процессы, в которых исходящие (входящие) документы имеют свойство разрешения на что-либо. Например, в задачах фитосанитарного контроля импортное карантинное разрешение (ИКР) в полной мере может быть в электронном виде представлено средствами «удостоверяющего свидетельства». В этом случае решаются требования и сложной вложенной структуры самого документа, и метаданных ИКР, с указанием периода его действительности, а также возможности у Россельхознадзора отозвать конкретный ИКР с автоматическим выводом его из действительного оборота, например в случаях выявления заболевания в отдельном регионе поставки и т.п. [2];

− различного рода выписки из реестров, кадастров и т.п., например выписка из реестра юридических лиц. Действует в течение 6 месяцев, но с переводом ее формы в электронный вид с учетом свойств

«удостоверяющего свидетельства» выписка может приобрести новые качества – при изменении записи в реестре юридических лиц она может быть досрочно отозвана, что безусловно повысит степень доверия и актуальности выписки, уменьшит число обращений за выписками, а также будет способствовать уменьшению различных мошеннических действий с данной информацией;

– в системах, аналогичных интернет-банкингу. Аутентификация пользователя и действительность платежного поручения определяется криптографическими свойствами ЭЦП и защищенного соединения на ключах, сертификат которого выдан во внешнем по отношению к банковской системе УЦ (возможно даже в рамках государственных программ), а фактическая информация о счете пользователя оформляется в виде криптографически связанного с сертификатом открытого ключа атрибутного сертификата или сертификатов в случае управления пользователем несколькими счетами. Такая конструкция позволяет банковской системе оперативно управлять вплоть до блокирования счетами пользователя, не вмешиваясь в механизмы идентификации субъекта, которые в общем виде могут быть внешними по отношению к банковской системе;

– электронная лицензия на программное обеспечение или иную информацию, причем в таком варианте использования автоматически решается задача контроля целостности и неизменности программного обеспечения или иной информации;

– в системах, где «удостоверяющее свидетельство» – электронный документ, определяет правила допуска к конкретной информации в соответствии с определенным регламентом. В этом случае разносятся процедуры идентификации субъекта и назначения конкретных (возможно, временных или отзываемых) полномочий по доступу к информации, что может определяться только владельцем информации. Данное приложение особенно актуально в условиях централизованной идентификации субъектов информационного обмена, например в рамках программ, аналогичных программе «Социальная карта»;

– для обмена сведениями о физических и юридических лицах с уполномоченными органами (кредитными организациями, государственными агентствами, ведомствами, министерствами), например для приема различных заявлений от физических лиц (дистанционным способом), а также в банковской деятельности на территории РФ.

ЛИТЕРАТУРА

1. Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2. Сервер атрибутных сертификатов (AA) [Электронный ресурс]. URL: http://www.top-cross.ru/Pki/aa.html (дата обращения: 20.02.2012).

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ РАБОТЫ С ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСЬЮ И ОБЕСПЕЧЕНИЯ ШИФРОВАНИЯ ДАННЫХ

И.П. Зелинский, студент 5-го курса каф. ИСТМ
Научный руководитель Л.А. Лапина, доцент каф. ИСТМ
г. Красноярск, СФУ, ИКИТ, Joseph_Z@mail.ru

Среди всего спектра методов защиты данных от несанкционированного доступа особое место занимают криптографические методы. В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения.

На сегодняшний момент существует огромное количество программных продуктов криптографической защиты информации, но многие из них, за явным исключением, обладают рядом минусов, одним из которых является отсутствие обучающего модуля для обычных пользователей. Пользователь обычно не имеет ни малейшего представления о методах шифрования данных и о том, как правильно использовать тот или иной метод. В связи с этой проблемой было решено разработать такой программный продукт, который не просто может быть использован в качестве криптографической защиты информации, но и сможет обучить пользователей основам защиты данных, а также наглядно показать работу основных методов защиты, что называется изнутри.

Таким образом, разработанный программный продукт представляет собой программу для реализации в прикладном программном обеспечении функций криптографической защиты информации – применения электронной цифровой подписи (ЭЦП) и шифрования с так называемым HELP-приложением. Такой программный продукт может применяться практически в любых системах различного уровня и назначения, нуждающихся в использовании средств ЭЦП и шифрования, кроме того, может использоваться и непосредственно пользователем MS Windows для подписи и шифрования файлов в проводнике MS Windows. Программа написана на высокоуровневом языке программирования C++ с использованием интерфейса MicrosoftCryptoAPI, который является основой средств защиты Microsoft Internet Security Framework. Он позволяет создавать приложения, использующие криптографические методы, и обеспечивает базовые функции защиты для безопасных каналов и подписи кода.

Программа работает в трех режимах:

1) обучение основам криптографической защиты информации с возможностью наглядного представления в виде схем, изображений и обучающих FLASH-роликов;

2) пошаговый режим работы с краткими объяснениями на каждом шаге работы с возможностью видеть, что происходит на каждом этапе шифрования или использования ЭЦП;

3) обычный режим (режим профи), используемый непосредственно для применения ЭЦП и шифрования в форсированном режиме.

Основные функции, реализованные в программе:

- формирование и проверка корректности ЭЦП;
- подпись и шифрование;
- расшифрование и проверка корректности ЭЦП;
- управление сертификатами и ключами пользователя;
- управление криптопровайдерами.

Программа обеспечивает возможность использования криптопровайдеров, входящих в состав Windows. Все они отличаются друг от друга своими типами, которые определяются набором параметров, включающим:

- алгоритм обмена сессионным (симметричным) ключом;
- алгоритм вычисления цифровой подписи;
- формат цифровой подписи;
- схема генерирования сессионного ключа по хешу;
- длина ключа.

Обучающий модуль разработан в виде HELP-приложения, с помощью языка разметки гипертекста HTML и языка программирования JavaScript. Особое внимание в обучающем модуле уделяется проблеме использования ЭЦП в системах электронного документооборота и юридически значимого электронного документооборота, в прикладных системах персонального использования. В HELP-приложение для изучения и ознакомления с ЭЦП вынесены следующие разделы:

- общие положения;
- история создания;
- сферы применения;
- функционирование ЭЦП;
- виды ЭЦП;
- средства работы с ЭЦП;
- атаки на ЭЦП.

В разделе «Общие положения» включены законодательные аспекты обеспечения правовых условий использования электронной цифровой подписи в электронных документах, описаны действующие федеральные законы об использовании ЭЦП, рассмотрены основные понятия и определения. В разделе «Функционирование ЭЦП» представлены FLASH-ролики и схемы функционирования ЭЦП, ее создания и проверки.

Разработанный программный комплекс предназначен в первую очередь для студентов специальности «информационные системы и технологии», изучающих дисциплину «Информационная безопасность и защита информации». Также программный продукт будет полезен специалистам, работающим с электронным документооборотом, и всем желающим получить, обновить или восполнить знания в направлении криптографической защиты информации, ЭЦП, шифрования. В программе реализованы функции управления сертификатами, криптопровайдерами, реализована работа с ЭЦП и шифрованием, а значит, программа будет полезна всем пользователям, которые хотят защитить личные файлы в проводнике MS Windows.

ЛИТЕРАТУРА

1. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

2. Жданов О.Н. Методы и средства криптографической защиты информации: учеб. пособие / О.Н. Жданов, В.В. Золотарев / Сиб. гос. аэрокосмич. ун-т. Красноярск, 2008. 256 с.

СОДЕРЖАНИЕ

СЕКЦИЯ 15

ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ

*Председатель – **Ходашинский И.А.**, профессор каф. КИБЭВС, д.т.н., зам. председателя – **Лавыгина А.В.**, ст. преп. каф. АОИ, к.т.н.*

Ахаев А.В.
СТРУКТУРА ПРОДУКЦИОННОЙ СИСТЕМЫ ВЫБОРА ПРОГРАММНЫХ ПРОДУКТОВ СИСТЕМЫ «1С:ПРЕДПРИЯТИЕ 8» 9

Батурина Е.В.
ПЛАНИРОВАНИЕ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ РОБОТОМ-МАНИПУЛЯТОРОМ.....12

Белоногов И.Ю.
ХАОТИЧЕСКИЙ И КВАНТОВЫЙ АЛГОРИТМ РОЯЩИХСЯ ЧАСТИЦ ДЛЯ НАСТРОЙКИ ПАРАМЕТРОВ НЕЧЁТКИХ СИСТЕМ 14

Дель В.А.
ЯДРО АВТОМАТИЗИРОВАННОЙ ТЕСТИРУЮЩЕЙ СИСТЕМЫ.....18

Елистратов С.А., Чичерин А.А., Косенко М.А.
СИСТЕМА РАСПОЗНАВАНИЯ ГЛАСНЫХ ЗВУКОВ В РЕЧЕВЫХ СИГНАЛАХ.....21

Евсютин О.О.
ПРИЛОЖЕНИЯ ТЕОРИИ КЛЕТОЧНЫХ АВТОМАТОВ В ОБРАБОТКЕ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ 23

Гаращенко И.Н., Шмакова А.К., Кудаев Н.Ю., Зубаиров Т.Р., Катков С.А., Сесова Е.О., Пушкарев М.Ю.
РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ ТРАНСПОРТНЫМ РОБОТОМ (НА ПРИМЕРЕ LEGO-РОБОТА).....25

Горбунов И.В.
ЭФФЕКТ ПЕРЕОБУЧЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ МОДИФИЦИРОВАННОГО АЛГОРИТМА ПЧЕЛИНОЙ КОЛОНИИ ДЛЯ НЕЧЕТКОГО АППРОКСИМАТОРА 28

Ламожапов Ч.А., Волков С.А., Гурьев Р.А., Харин М.А.
ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СРЕДСТВ АНАЛИЗА ДАННЫХ В ВЕБ-ПРОЕКТЕ 32

Гусакова Е.Н., Ходашинский И.А.
АЛГОРИТМЫ И ПРОГРАММНЫЕ СРЕДСТВА ВЫДЕЛЕНИЯ ИНФОРМАТИВНЫХ ПРИЗНАКОВ В ЗАДАЧАХ КЛАССИФИКАЦИИ 35

Качалов А.Н.
НЕЧЕТКИЙ РЕГУЛЯТОР КАК СРЕДСТВО УПРАВЛЕНИЯ КОМПЕНСИРУЮЩИМИ УСТРОЙСТВАМИ В АКТИВНО-АДАПТИВНОЙ СЕТИ.....37

Ханефт А.А.
ТЕСТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА RUBY ON RAILS.....39

Кривцов И.А.
ПРИМЕНЕНИЕ МЕТОДА ЦВЕТОВЫХ ГИСТОГРАММ ДЛЯ КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ С ЦЕНТРАЛЬНЫМ ПОЗИЦИОНИРОВАНИЕМ ОБЪЕКТА 41
Семенов К.А., Утешева А.Е., Погуда А.А.
РЕШЕНИЕ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ В НЕЙРОСЕТЕВОМ БАЗИСЕ 44
Серебренникова О.А.
ПРОЕКТИРОВАНИЕ WEB-САЙТА «СИБИРСКОГО МЕДИЦИНСКОГО ЖУРНАЛА» 46
Синьков Д.С.
АЛГОРИТМ APRIORI. ЗАДАЧА ГЕНЕРАЦИИ АССОЦИАТИВНЫХ ПРАВИЛ ДЛЯ ПРОДВИЖЕНИЯ ТОВАРОВ В ИНТЕРНЕТ-МАГАЗИНЕ 49
Соловьёв В.А.
СТРУКТУРА СИСТЕМЫ АВТОНОМНОГО ТЕСТИРОВАНИЯ ПРОГРАММ 51
Ямшанов А.В.
АВТОМАТИЧЕСКИЙ СБОР, ОБРАБОТКА И РУБРИКАЦИЯ НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ 53
Земцов Н.Н., Корниенко И.С.
МНОГОКРИТЕРИАЛЬНАЯ ОПТИМИЗАЦИЯ, ПОСТРОЕНИЕ ПАРЕТО-ФРОНТА 56

СЕКЦИЯ 17
АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

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

Афиркина Т.А.
АВТОМАТИЗАЦИЯ УЧЕТА РАБОЧЕГО ВРЕМЕНИ СОТРУДНИКОВ ТОМСКОГО ЦЕНТРА ОВД 59
Андрианова А.В., Паргачёв И.А.
РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО УСТРОЙСТВА ДЛЯ НАПЫЛЕНИЯ ПРОСВЕТЛЯЮЩИХ ПОКРЫТИЙ 61
Архипов Я.В.
ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА И КОНТРОЛЯ ТРАНСПОРТНЫХ СРЕДСТВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ СЛУЖБЫ «ГОСТЕХНАДЗОР» ХМАО–ЮГРЫ 64
Долгушин В.Е.
УСТАНОВКА МИКРОКЛИМАТА ДОМАШНИХ РАСТЕНИЙ 65
Евсютин О.О.
КРИТЕРИЙ ВЫБОРА БАЗИСОВ ДЕКОРРЕЛИРУЮЩИХ ПРЕОБРАЗОВАНИЙ, ПОЛУЧАЕМЫХ ИЗ СОСТОЯНИЙ РАЗВИТИЯ КЛЕТОЧНОГО АВТОМАТА 67

Езангина Т.А.
ПАРАМЕТРИЧЕСКИЙ СИНТЕЗ РЕГУЛЯТОРА ЛИНЕЙНОЙ ИНТЕРВАЛЬНОЙ СИСТЕМЫ НА ОСНОВЕ НЕЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ 70
Исхаков С.Ю.
МЕТОДИКА ПОСТРОЕНИЯ МОДЕЛЕЙ СЕТЕВЫХ УСТРОЙСТВ 72
Исхаков С.Ю., Исхаков А.Ю., Козыренко Н.С., Шумская А.О.
МОДЕЛИРОВАНИЕ ОБЪЕКТОВ В СИСТЕМЕ МОНИТОРИНГА ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ 75
Иванов Е.О.
МОДЕЛЬ ВОДОЗАБОРА ПОДЗЕМНЫХ ВОД ДЛЯ ЭНЕРГОЭФФЕКТИВНОГО УПРАВЛЕНИЯ НАСОСНЫМИ СТАНЦИЯМИ 77
Копытин А.А., Козлов М.С.
ПРЕИМУЩЕСТВА ОСНАЩЕНИЯ АВТОРЕМОНТНЫХ ПРЕДПРИЯТИЙ СПЕЦИАЛИЗИРОВАННЫМ РАЗБОРОЧНО-СБОРОЧНЫМ ОБОРУДОВАНИЕМ 80
Козлов М.С., Копытин А.А.
ПРОБЛЕМЫ ШИНОМОНТАЖНЫХ ПРЕДПРИЯТИЙ ЛЕГКОВОГО АВТОТРАНСПОРТА КРАСНОДАРСКОГО КРАЯ 83
Козловский К.А., Егоров В.Б., Сусиков А.Н.
СИСТЕМА ТЕСТИРОВАНИЯ ЗНАНИЙ СТУДЕНТОВ 86
Латровкин В.В.
СИТУАЦИОННЫЙ ЦЕНТР УПРАВЛЕНИЯ ЭНЕРГОЭФФЕКТИВНОСТЬЮ 87
Леонов А.Е., Иванов А.Д.
КОНФЕРЕНЦ-СВЯЗЬ. КОНГРЕСС-СИСТЕМЫ, СИНХРОННЫЙ ПЕРЕВОД И СИСТЕМЫ ВИЗУАЛИЗАЦИИ 89
Медведева А.Н.
ПРОГРАММА МОДЕЛИРОВАНИЯ ПРИБОРОВ МИКРОЭЛЕКТРОНИКИ 92
Мытько В.В.
РОЛЬ ПОДЪЕМНО-ОСМОТРОВОГО ОБОРУДОВАНИЯ ПРИ ОБСЛУЖИВАНИИ ГРУЗОВЫХ АВТОМОБИЛЕЙ 94
Николаев В.В., Копытин А.А.
ЭЛЕКТРОДУГОВАЯ НАПЛАВКА ШЕЕК ВАЛОВ ПОРОШКОВОЙ ПРОВОЛОКОЙ 96
Нукин А.Ж.
МАТЕМАТИЧЕСКОЕ И АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЭНЕРГОЭФФЕКТИВНОЙ РАБОТЫ ВОДОГРЕЙНОЙ КОТЕЛЬНОЙ. 99
Оплачко Е.О.
СТАТИСТИЧЕСКИЕ ОЦЕНКИ БЛИЗОСТИ ТЕКСТОВЫХ ДОКУМЕНТОВ 101
Пехов О.В.
УСТРОЙСТВО ТЕСТИРОВАНИЯ ПАМЯТИ 104
Полонец Б.П., Шабалин Г.А.
АНАЛИЗ И ВЫБОР КОНСТРУКЦИЙ БАЛАНСИРОВОЧНЫХ СТЕНДОВ ДЛЯ ШИНОМОНТАЖНЫХ РАБОТ 109

Поляков А.А., Межевалов А.А., Ковалев А.А.
ПРИЛОЖЕНИЕ ДЛЯ МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМ ДЛЯ ВЗАИМОДЕЙСТВИЯ С WEB-РЕСУРСАМИ 112
Романова И.Е.
ДЕДУКТИВНОЕ УСТРОЙСТВО «ПОЗНАЮ МИР» 115
Шабалин Г.А., Полонец Б.П.
АНАЛИЗ КОНСТРУКТИВНЫХ ВОЗМОЖНОСТЕЙ ПЛАТФОРМЕННЫХ СТАПЕЛЕЙ, ПРЕДСТАВЛЕННЫХ НА РОССИЙСКОМ РЫНКЕ 117
Шиляев И.И.
УСТРОЙСТВО УПРАВЛЕНИЯ ПРОМЫШЛЕННЫМ РОБОТОМ 121
Шмитько Е.В.
СОВРЕМЕННЫЕ МЕТОДЫ ПРОЕКТИРОВАНИЯ ЦИФРОВЫХ СХЕМ 123
Тарасов М.С.
УСТРОЙСТВО СБОРА ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ 125
Усов Е.Е., Коваленко П.Н.
ЯЗЫК VHDL. СИНТЕЗ ЭЛЕКТРОННЫХ СРЕДСТВ 127
Воротников В.А.
КОМПЛЕКСНАЯ СИСТЕМА СИГНАЛИЗАЦИИ И ВИДЕОНАБЛЮДЕНИЯ 128
Жернаков К.М.
СИСТЕМА ПЕРЕДАЧИ ДАННЫХ ПО ЭЛЕКТРОСЕТИ ДЛЯ ЭЛЕКТРОПРИВОДОВ 130
Шишкин И.Н.
АВТОМАТИЗАЦИЯ РАСПРЕДЕЛЕННОГО ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА НА ПРИМЕРЕ АВТОМАТИЗАЦИИ РАБОТЫ ТАКСОПАРКА 132

СЕКЦИЯ 18

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель – **Шелупанов А.А.**, проректор по НР ТУСУРа, зав. каф. КИБЭВС, профессор, д.т.н.;*
*зам. председателя – **Мещеряков Р.В.**, зам. начальника НУ, зам. зав. каф. КИБЭВС по НР, доцент, к.т.н.*

Алчебаева М.В., Рожков А.В.
ПЕРИОДИЧЕСКИЕ АТ-ГРУППЫ НАД АБЕЛЕВЫМИ И НЕАБЕЛЕВЫМИ ГРУППАМИ В ВОПРОСАХ ЗАЩИТЫ ИНФОРМАЦИИ 135
Алейнов Ю.В.
МОДЕЛИРОВАНИЕ СЕТИ ДЛЯ ИЗУЧЕНИЯ СПОСОБОВ КОМБИНИРОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И СИСТЕМ HONEYPOT 137

Ананев М.А., Цыбань Е.В., Штыгайло С.В., Якимук А.Ю., Сопов М.А.
ШАБЛОНЫ СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ 139
Воронкин Р.А., Бабкин В.Ю.
ПРОЕКТИРОВАНИЕ ПРОГРАММЫ БЕЗОПАСНОГО ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА УСТРОЙСТВАХ ПОД УПРАВЛЕНИЕМ ANDROID 142
Баринов А.Е.
СИСТЕМАТИЗАЦИЯ ПАРАМЕТРОВ СИСТЕМНЫХ СОБЫТИЙ С ЦЕЛЬЮ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 145
Бут Г.А.
ТРЕБОВАНИЯ ПО ПЕРСОНАЛЬНЫМ ДАННЫМ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ 146
Чимитдоржиева Е.Ц.
ИССЛЕДОВАНИЕ МОДЕЛЕЙ УГРОЗ ПРИ ПОМОЩИ МАТЕМАТИЧЕСКИХ МЕТОДОВ 149
Чижов Н.В.
КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ ДЛЯ ОПЕРАЦИОННЫХ СИСТЕМ, ОСНОВАННЫХ НА ЯДРЕ LINUX 151
Дремин А.С.
ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ КОММЕРЧЕСКОЙ ТАЙНЫ 153
Дударев А.И.
СРЕДСТВА И МЕТОДЫ АНАЛИЗА ПРОГРАММ И ПРОДИВОДЕЙСТВИЕ ЕМУ 156
Ефремкин А.В.
АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ ОРГАНИЗАЦИИ НА ПРИМЕРЕ «РОСГОССТРАХ БАНКА». ТЕХНИЧЕСКИЕ СРЕДСТВА 158
Ерофеева И.И.
РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ КОНКУРЕНТНОГО РАННЕГО ПРЕДУПРЕЖДЕНИЯ ДЛЯ ПРЕДПРИЯТИЯ 161
Феденко В.А.
МОДЕЛИ И АЛГОРИТМЫ ПОЛУЧЕНИЯ ВЕРОЯТНОСТНЫХ ОЦЕНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 164
Ганюшкин И.Г.
ИССЛЕДОВАНИЕ ПРЕВЕНТИВНЫХ МЕР ДЛЯ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 167
Ибрагимов Р.Ю.
АНАЛИЗ ПОДХОДОВ К ПОСТРОЕНИЮ МОДЕЛЕЙ УГРОЗ ИНФОРМАЦИННОЙ БЕЗОПАСНОСТИ 169
Исхаков А.Ю.
МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ И МОНИТОРИНГА ТРАФИКА НА КОММУТАТОРАХ CISCO SYSTEMS 172

Иванчук И.Я., Конев А.А.
ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА 174
Харченко С.С.
ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ КОДЕ 175
Корсюк А.О., Сопов М.А.
ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ФУНКЦИОНИРОВАНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 178
Ковтун А.С.
ПРОБЛЕМАТИКА СОВРЕМЕННЫХ СИСТЕМ МОНИТОРИНГА 180
Козлов В.М.
АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ ОРГАНИЗАЦИИ НА ПРИМЕРЕ «РОСГОССТРАХ БАНКА». ПРОГРАММНЫЕ СРЕДСТВА 181
Козыренко Н.С., Михайлов Н.С.
АКТУАЛЬНОСТЬ ПЕРЕХОДА К ЭЛЕКТРОННОМУ ДОКУМЕНТООБОРОТУ 184
Кручинин Д.В.
ПРИМЕНЕНИЕ ТЕСТОВ НА ПРОСТОТУ В ЗАЩИТЕ ИНФОРМАЦИИ 187
Кураленко А.И.
ПРОЦЕСС АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ 189
Кузьменко А.Н.
ВНЕДРЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА ЗАЩИТЫ «SPECTOR 360» 191
Лукьянов А.С., Авсентьев А.О.
ОЦЕНКА ЭФФЕКТИВНОСТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МЕТОДОВ ТЕОРИИ ГРАФОВ 193
Лыбина А.С., Пьянкова М.Ю., Толстокулакова Е.М.
АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ОТНОШЕНИЯМИ С КЛИЕНТАМИ В СЕТЕВОМ МАРКЕТИНГЕ 195
Макаров И.Е.
РАЗРАБОТКА СИСТЕМЫ КЛАССИФИКАЦИИ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ 200
Нечаев К.А., Зыков Д.Д.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕРВИС-ОРИЕНТИРОВАННОЙ АРХИТЕКТУРЫ (SOA) 201
Остапчук Т.В., Сопов М.А.
БЕЗОПАСНОСТЬ СИСТЕМ ПЛАТЕЖЕЙ VISA, MASTERCARD 204
Петриченко Р.В.
СЕГМЕНТАЦИЯ РЕЧЕВОГО СИГНАЛА 206
Рошкован К.С., Поляков Д.В., Рубанов С.А., Наханов В.И., Мещеряков Р.В.
РЕЧЕВОЙ ПОЛИГРАФ 208
Попова Е.В.
МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ 210

Рахманенко И.А.
ИНТЕГРАЦИЯ РЕЧЕВОГО КОРПУСА И ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ИССЛЕДОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ 211
Рихтер Д.Ю.
ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ОТ УТЕЧЕК 213
Рогожин А.А.
РАЗРАБОТКА МЕТОДИКИ ПОСТРОЕНИЯ ОПТИМАЛЬНОЙ НАДЕЖНОЙ СТРУКТУРЫ ПОДСИСТЕМЫ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ 215
Рошкован К.С., Сопов М.А.
ШАБЛОНЫ СЕРТИФИКАТОВ ОТКРЫТЫХ КЛЮЧЕЙ 218
Рожков С.А., Рожков А.В.
МАТЕМАТИЧЕСКИЕ МОДЕЛИ ЗАЩИЩЕННЫХ ПРОТОКОЛОВ В ТЕРМИНАЛЬНЫХ СИСТЕМАХ И ТОНКИХ КЛИЕНТАХ 220
Саблин М.С., Миронова В.Г.
РАЗРАБОТКА МОДЕЛИ НАРУШИТЕЛЯ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ 225
Салиева Л.Р.
РЕЧЕВЫЕ ТЕХНОЛОГИИ В ОБУЧЕНИИ СТУДЕНТОВ – НОСИТЕЛЕЙ РУССКОГО ЯЗЫКА ПРОИЗНОШЕНИЮ НА ИНОСТРАННОМ ЯЗЫКЕ 229
Шадрин А.А.
ЗАЩИТА .NET ПРИЛОЖЕНИЙ 230
Шефф Б.В., Миронова В.Г.
ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ КАДРОВОГО ДЕЛОПРОИЗВОДСТВА 231
Шильненков В.Е., Мещеряков Р.В.
ПРОЕКТИРОВАНИЕ АВТОНОМНОГО УСТРОЙСТВА ДЛЯ ПОДКЛЮЧЕНИЯ К UTP 236
Шишкин И.Н.
РАЗГРАНИЧЕНИЕ ДОСТУПА В INTERNET С ИСПОЛЬЗОВАНИЕМ VPN И NPS. 238
Шишкин В.В., Кирсанов С.В.
ОЦЕНКА ЗАЩИЩЁННОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ И ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ АСУ ТП ГАЗОВОЙ ОТРАСЛИ 240
Шитов И.С.
ЗАЩИЩЕННЫЙ УДАЛЕННЫЙ ДОСТУП К ЛАБОРАТОРНОМУ СЕТЕВОМУ ОБОРУДОВАНИЮ 242
Шудрак М.О., Лубкин И.А.
МЕТОДИКА ДЕКОМПИЛЯЦИИ БИНАРНОГО КОДА И ЕЕ ПРИМЕНЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 245
Шумская А.О.
АНАЛИЗ ПОДХОДОВ К РЕАЛИЗАЦИИ ОБНАРУЖЕНИЯ СЕТЕВОГО ВТОРЖЕНИЯ 250

Заитова Э.Р., Швецова М.А., Шубникова Е.Г.
РАЗРАБОТКА МЕТОДИКИ АНАЛИЗА ЗАЩИЩЕННОСТИ СЕТИ 252
Сметанин А.А.
ФОРМАЛИЗАЦИЯ ПРОЦЕДУРЫ ВЫБОРА СОТРУДНИКА 255
Новохрестов А.К., Минина Д.Ю., Сологуб И.А.
СТРУКТУРА И ФУНКЦИИ АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ..... 257
Созинова И.С., Черепанов С.Е.
АНАЛИЗ МЕТОДОВ ПОИСКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ КОДЕ 259
Стефаров А.П.
О РЕШЕНИИ ЗАДАЧИ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ И КЛАССИФИКАЦИИ НАРУШИТЕЛЯ ПРАВ ДОСТУПА В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ..... 262
Тухбатуллин Е.Р., Конев А.А.
КОМПЛЕКС ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ «ИНФОРМАТИКА» 265
Вильданов Р.Р., Маркин В.В., Мещеряков Р.В.
ТЕСТ НА СЛЕДУЮЩИЙ БИТ 266
Волков Д.В., Кручинин Д.В.
ИСПОЛЬЗОВАНИЕ TeX-РЕДАКТОРА ДЛЯ ОПИСАНИЯ МОДЕЛЕЙ БЕЗОПАСНОСТИ 269
Воротников Д.К.
АНАЛИЗ БЕЗОПАСНОСТИ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ 271
Воронкин Р.А., Ягодкин А.А.
ПРОЕКТИРОВАНИЕ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ТЕСТИРОВАНИЯ МОДУЛЯ АУТЕНТИФИКАЦИИ БАЗ ДАННЫХ MYSQL 274
Яценко А.С.
МЕТОДИКИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ..... 277
Южаков А.В.
РАЗРАБОТКА ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ 280
Заболотникова А.Е.
АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА И АНАЛИЗА РИСКОВ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА..... 282
Заитова Э.Р., Швецова М.А., Шубникова Е.Г.
МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 284
Михайлов Н.С., Заяц А.О.
СФЕРЫ ПРИМЕНЕНИЯ АТРИБУТНЫХ СЕРТИФИКАТОВ 86
Зелинский И.П.
ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ РАБОТЫ С ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСЬЮ И ОБЕСПЕЧЕНИЯ ШИФРОВАНИЯ ДАННЫХ..... 289

Научное издание

Материалы
Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2012», посвященной 50-летию ТУСУРа

16–18 мая 2012 г., г. Томск

В пяти частях

Часть 3

Корректор – **В.Г. Лихачева**
Верстка **В.М. Бочкаревой**

Издательство «В-Спектр».
Сдано на верстку 01.04.2012. Подписано к печати 25.04.2012.
Формат 60×84 1/16. Печать трафаретная. Печ. л. 18,75.
Тираж 500 экз. Заказ 18.

Тираж отпечатан в издательстве «В-Спектр».
ИНН/КПП 7017129340/701701001, ОГРН 1057002637768
634055, г. Томск, пр. Академический, 13-24, т. 49-09-91.
E-mail: bvm@sibmail.com