ТУСУР

НАУЧНАЯ СЕССИЯ ТУСУР–2013

МАТЕРИАЛЫ ВСЕРОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ СТУДЕНТОВ, АСПИРАНТОВ И МОЛОДЫХ УЧЕНЫХ
15–17 мая 2013 г. (В пяти частях)

Часть 4

г. Томск

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

НАУЧНАЯ СЕССИЯ ТУСУР–2013

Материалы

Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2013»

15–17 мая 2013 г., г. Томск

В пяти частях

Часть 4

В-Спектр
2013

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

Н 34 **Научная сессия ТУСУР–2013:** Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 15–17 мая 2013 г. – Томск: В-Спектр, 2013: В 5 частях. – Ч. 4. – 266 с.

ISBN 978-5-91191-283-3
ISBN 978-5-91191-287-1 (Ч. 4)

Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых посвящены различным аспектам разработки, исследования и практического применения радиотехнических, телевизионных и телекоммуникационных систем и устройств, сетей электро- и радиосвязи, вопросам проектирования и технологии радиоэлектронных средств, аудиовизуальной техники, бытовой радиоэлектронной аппаратуры, а также автоматизированых систем управления и проектирования. Рассматриваются проблемы электроники СВЧ- и акустооптоэлектроники, нанофотоники, физической, плазменной, квантовой, промышленной электроники, радиотехники, информационно-измерительных приборов и устройств, распределенных информационных технологий, вычислительного интеллекта, автоматизации технологических процессов, в частности в системах управления и проектирования, информационной безопасности и защиты информации. Представлены статьи по математическому моделированию в технике, экономике и менеджменте, антикризисному управлению, 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 978-5-91191-283-3
ISBN 978-5-91191-287-1 (Ч. 4)

Всероссийская научно-техническая конференция студентов и молодых ученых «Научная сессия ТУСУР–2013»

15–17 мая 2013 г.

ПРОГРАММНЫЙ КОМИТЕТ

- *Шурыгин Ю.А.* – сопредседатель 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, д.ист.н., профессор;
- *Давыдова Е.М.*, зам. зав. каф. КИБЭВС по УР, доцент каф. КИБЭВС, к.т.н.;
- *Дмитриев В.М.*, зав. каф. МОТЦ, д.т.н., профессор;
- *Еханин С.Г.*, проф. каф. КУДР, д.ф.-м.н., доцент;
- *Ехлаков Ю.П.*, проректор по информатизации и управлению ТУСУРа, зав. каф. АОИ, д.т.н., профессор;
- *Зариковская Н.В.*, доцент каф. ФЭ, к.ф.-м.н.;
- *Карташев А.Г.*, проф. каф. РЭТЭМ, д.б.н.;
- *Катаев М.Ю.*, проф. каф. АСУ, д.т.н.;
- *Коцубинский В.П.*, зам. зав. каф. КСУП, доцент каф. КСУП, к.т.н.;
- *Лощилов А.Г.*, с.н.с. СКБ «Смена» ТУСУРа, к.т.н.;
- *Лукин В.П.*, директор отд. распространения волн Ин-та оптики атмосферы СО РАН, почетный член Американского оптического общества, д.ф.-м.н., профессор, г. Томск;
- *Малюк А.А.*, декан фак-та информационной безопасности МИФИ, к.т.н., г. Москва;
- *Малютин Н.Д.*, начальник НУ ТУСУРа, директор НОЦ «Нанотехнологии», д.т.н., профессор;
- *Мещеряков Р.В.*, зам. начальника НУ, проф. каф. КИБЭВС, д.т.н., доцент;
- *Мицель А.А.*, проф., зам. зав. каф. АСУ, д.т.н.;

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

СЕКЦИИ КОНФЕРЕНЦИИ

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

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

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

Секция 4. Проектирование биомедицинских электронных и наноэлектронных средств. Председатель секции – Еханин Сергей

Георгиевич, проф. каф. КУДР, д.ф.-м.н., доцент; зам. председателя – Романовский Михаил Николаевич, доцент каф. КУДР, к.т.н.

Секция 5. Проектирование измерительной аппаратуры. Председатель секции – Лощилов Антон Геннадьевич, с.н.с. СКБ «Смена», к.т.н.; зам. председателя – Бомбизов Александр Александрович, м.н.с. СКБ «Смена».

Секция 6. Проектирование и эксплуатация радиоэлектронных средств. Председатель секции – Шостак Аркадий Степанович, проф. каф. КИПР, д.т.н.; зам. председателя – Озёркин Денис Витальевич, декан РКФ, доцент каф. КИПР, к.т.н.

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

Секция 8. Оптические информационные технологии, нанофотоника и оптоэлектроника. Председатель секции – Шарангович Сергей Николаевич, проф., зав. каф. СВЧиКР, к.ф.-м.н.; зам. председателя – Буримов Николай Иванович, зав. УНЛ каф. ЭП НИЧ, к.т.н.

Секция 9. Инфокоммуникационные технологии и системы широкополосного беспроводного доступа. Председатель секции – Ворошилин Евгений Павлович, зав. каф. ТОР, к.т.н.; зам. председателя – Гельцер Андрей Александрович, ст. преподаватель каф. ТОР, к.т.н.

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

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

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

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

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

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

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

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

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

Секция 17. Автоматизация технологических процессов. Председатель секции – Давыдова Елена Михайловна, доцент, зам. зав. каф. КИБЭВС по УР, к.т.н.; зам. председателя – Зыков Дмитрий Дмитриевич, доцент каф. КИБЭВС, к.т.н.

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

Секция 19. Математическое моделирование в технике, экономике и менеджменте. Председатель секции – Мицель Артур Александрович, проф. каф. АСУ, д.т.н.; зам. председателя – Зариковская Наталья Вячеславовна, доцент каф. 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 – Миргородский Семен Константинович, м.н.с. каф. ФЭ.

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

Подсекция 23.1. Актуальные проблемы социальной работы в современном обществе. Председатель секции – Грик Николай Антонович, зав. каф. ИСР, д.и.н., проф.; зам. председателя – Казакевич Людмила Ивановна, доцент каф. ИСР, к.и.н.

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

Секция 24. Инновационные проекты, студенческие идеи и проекты. Председатель секции – Уваров Александр Фавстович, проректор по инновационному развитию и международной деятельности ТУСУРа, к.э.н.; зам. председателя – Чекчеева Наталья Валерьевна, зам. директора Института инноватики, к.э.н.

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

Секция 26. Современные информационные технологии. Открытия. Творчество. Проекты. Председатель секции – Федорова Наталия Андреевна, начальник учебно-методического управления НОУ «Открытый молодежный университет»; зам. председателя – Смолонская Марина Александровна, заместитель начальника учебно-методического управления НОУ «Открытый молодежный университет».

Секция 27. Правовые проблемы современной России. Председатель секции – Соколовская Наталья Сергеевна, доцент каф. уголовного права, к.ю.н.

Адрес Оргкомитета:

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

1-й том – 1–7-я секции;
2-й том – 8–14-я, 25, 26-я секции;
3-й том – 15, 19–22-я секции;
4-й том – 16–18-я секции;
5-й том – 23, 24, 27-я секции.

СЕКЦИЯ 16

ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ

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

МЕТОДЫ И СИСТЕМЫ ВЫБОРА НАИЛУЧШЕГО ОБЪЕКТА

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

Широко распространенной проблемой для человека является проблема выбора наилучшего объекта. Таким объектом может быть товар или услуга. Как правило, покупатель сравнивает характеристики рассматриваемых товаров по ряду важных для него аспектов, стремясь выбрать лучшую альтернативу. Но в реальности редко встречается объект, превосходящий другие по всем характеристикам. Чем сложнее задача выбора и чем серьезнее последствия выбора, тем больше возрастает необходимость прибегнуть к помощи специальных методов и алгоритмов, которые смогут помочь человеку в сравнении товаров.

Методы решения задачи. Задачи выбора наилучшей альтернативы из некоторого множества допустимых вариантов встречаются во всех без исключения областях знаний, отличаются большим разнообразием и решаются различными методами в зависимости от типа информации [1]:

- методы на основе количественных характеристик – многокритериальная теория полезности (Р.Л. Кини, Х. Райфа), эвристические методы;
- методы на основе качественных характеристик, которые сразу же переводятся в количественный вид – метод анализа иерархий (Т. Саати), методы теории нечетких множеств (Л.А. Заде), методы теории полезности (В. Парето);
- методы на основе количественных характеристик, использующие несколько индикаторов при сравнении альтернатив – методы сравнительного превосходства (Б. Рой).
- методы на основе качественных характеристик без перехода к количественному виду – методы вербального анализа решений (О.И. Ларичев).

На практике часто встречаются слабоструктурированные задачи, которые содержат как количественные, так и качественные оценки альтернатив, причем качественные преобладают. Поэтому необходимо использовать методы, позволяющие осуществлять выбор решений из множества альтернатив, где критерии имеют различные типы шкал измерения в условиях неопределенности.

Среди перечисленных методов наибольшей универсальностью и теоретической обоснованностью обладают методы теории полезности, методы теории нечетких множеств и метод анализа иерархий [2].

Однако не существует полностью универсальных подходов искусственного интеллекта для решения подобного класса задач. Рассмотрим существующие разработки решения данной задачи.

Системы выбора. Существуют интернет-каталоги с возможностью отбора товаров по производителю и цене [3]. Такие каталоги незначительно сужают круг поиска, а описания товаров требуют дополнительного анализа.

Существуют сайты с возможностью подбора товаров на основе нескольких параметров, характеризующих потребности заказчика [4]. Количество параметров зависит от предметной области и варьируется от 3 до 15. На основе этих параметров определяются подходящие товары посредством *sql*-запроса к таблице базы данных. Зачастую подходящих товаров может либо вообще не оказаться, либо их количество будет исчисляться десятками, анализировать которые приходится самостоятельно. Также есть ресурсы [5], упрощающие ручной анализ, предоставляющие сервисы для сравнения товаров в виде сводной таблицы характеристик.

Рассмотренные системы не могут быть использованы в процессе решения задачи выбора наилучшего товара в силу следующих причин:

- системы созданы применительно к узкой предметной области;
- являются коммерческими разработками, не предназначенными для стороннего использования;
- отсутствуют методы и алгоритмы выбора наилучшего товара.

Предлагаемые алгоритмы и методы выбора программных продуктов на примере «1С:Предприятие 8».

Предлагается рассмотреть задачу выбора программных продуктов (ПП), где проблема выбора в последнее время становится актуальной. Наиболее ярко эта проблема выражена среди ПП системы «1С:Предприятие 8».

Выявление данных и знаний осуществляется путем сбора экспертной информации, поэтому автоматизация процесса выбора осуществляется с помощью построения экспертной системы [6]. В системе

присутствует модуль анализа функциональных возможностей программных продуктов, предназначенный для выбора наилучшего ПП из набора альтернатив (до 10). Алгоритм выбора основывается на теории нечетких множеств и представлен следующими этапами [7]:

- формирование частных оценок характеристик ПП и установление шкал измерения для них;
- нормирование частных оценок характеристик с использованием обобщенной функции желательности Харрингтона. Приведение к единой универсальной шкале;
- расчет интегральной оценки на основе системы нечеткого вывода.

Сравнение систем по интегральной оценке необходимо проводить по области их применения, по возможности максимально суживая ее. Это позволит сравнивать между собой однотипные программы с высокой точностью.

Заключение. Проведен анализ методик и систем выбора и оценена возможность их применения в условиях рассматриваемой задачи.

Предлагаемый подход выбора программных продуктов предназначен для работы со слабоструктурированными данными, которые содержат как количественные, так и качественные оценки.

Предложенный алгоритм носит достаточно универсальный характер.

ЛИТЕРАТУРА

1. Ларичев О.И. Свойства методов принятия решений в многокритериальных задачах индивидуального выбора // Автоматика и телемеханика. 2002. № 2. С. 146–158.

2. Янгуразова Н.Р. Принятие решений в многокритериальной задаче на основе экспертной системы: Дис. … к.т.н. Уфа, 2007.

3. Интернет-супермаркет программного обеспечения [Электронный ресурс]. Режим доступа к сайту: http://softkey.ru

4. Отраслевые и специализированные решения 1С [Электронный ресурс]. Режим доступа к сайту: http://solutions.1c.ru

5. Интернет-магазин бытовой электроники [Электронный ресурс]. Режим доступа к сайту: http://dtd.ru

6. Адуева Т.В., Ахаев А.В., Ходашинский И.А. Продукционная система выбора программных продуктов системы «1С:Предприятие 8» // Бизнес-информатика. 2012. №1(19). С. 55–61.

7. Ахаев А.В. WEB-ориентированная экспертная система выбора программных продуктов // Наука. Технологии. Инновации: матер. Всерос. науч. конф. студентов, аспирантов и молодых ученых: Новосибирск, 29 нояб. 2 декаб. 2012 г. Новосибирск: Изд-во НГТУ, 2012. Ч. 3. С. 263–266.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ НЕЧЕТКИХ СИСТЕМ НА ОСНОВЕ АЛГОРИТМА СВЕТЛЯЧКОВ

М.А. Ананев, студент
Научный руководитель И.А. Ходашинский, проф., д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, makernew@mail.ru
Проект ГПО КИБЭВС-1211 – «Нечеткие системы»

Нечеткие системы применяются в таких проблемных областях, как автоматическое управление, прогнозирование, распознавание образов, принятие решений. Они встроены в огромное количество промышленных изделий, начиная с роботов и систем управления электропоездами и заканчивая такими потребительскими товарами, как фото- и видеокамеры, кондиционеры, стиральные машины и др. Преимуществами нечетких систем являются невысокая стоимость разработки, гибкость, интуитивно понятная логика функционирования.

Основная концепция нечеткого моделирования заключается в использовании степени принадлежности, которая является эффективным средством описания поведения плохо формализованных объектов, систем и процессов. Нечеткое моделирование возможно на основе таблицы наблюдений, а также с использованием априорного знания и опыта.

Важной проблемой, решаемой в процессе построения нечеткой системы, является идентификация параметров нечетких лингвистических правил. Решение данной задачи осложняется высокой размерностью, неполнотой и неточностью экспериментальных данных. Актуальной является задача повышения точности вывода нечеткой системы на реальных данных [1].

Алгоритм. Рассматривается популяционный алгоритм оптимизации – «Алгоритм светлячков». Его суть построена на основе модели передвижения светлячков в пространстве.

Каждый светлячок является решением. Качество решения улучшается путем передвижения светлячков в сторону более ярких светлячков с учётом коэффициентов поглощения среды и взаимной привлекательности светлячков. Количество решений при каждой итерации не изменяется.

Приводится описание пошагового алгоритма.

Общие положения для описания популяционных алгоритмов.

В качестве вектора для оптимизации выступают антецеденты нечеткой системы. Вектор представлен в виде массива X_i, i принимает значения от 1 до $\sum_{j=1}^{L} kO_j$, где L – количество входных переменных не-

четкой системы; k – количество переменных, описывающих каждый терм; O – количество термов для j-й переменной.

Оптимизация параметров нечеткой системы алгоритмом светлячков

Шаг 1. Инициализация.

Задается количество итераций N и максимальное количество векторов S. Задаются параметры γ – коэффициент поглощения среды; β_0 – взаимная привлекательность светлячков, находящихся в 1 точке пространства. Генерируются начальные векторы $X_i(\overline{i=1,S})$ и высчитывается для них среднеквадратичная ошибка и фитнесс-функция $\varphi(X_i)$ на основе ошибки.

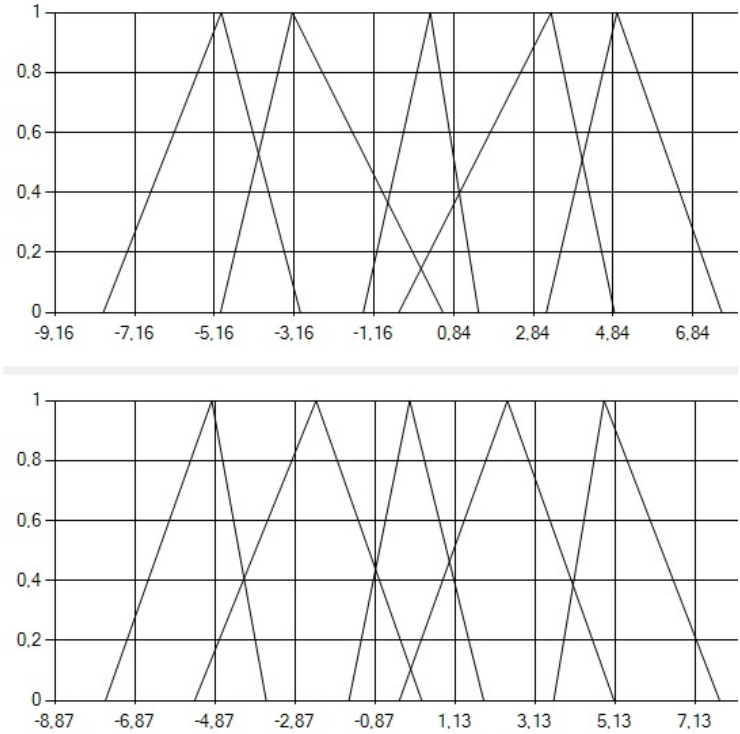


Рис. 1. Итоговое расположение функций принадлежности после настройки алгоритмом светлячков

Шаг 2. Если $\varphi(X_j) \le \varphi(X_i)$, то

$$X_j = X_i + B(r_{i,j}) * (X_j - X_i) + a,$$

где $B(r_{i,j}) = \frac{\beta_0}{1+\gamma r_{i,j}^2}$ – привлекательность светлячков, a – параметр рандомизации, $a = [\overline{-1,1}]$, $r_{i,j} = |X_j - X_i|$ – расстояние между светлячками.

Шаг 3. Для каждого вектора вычисляется фитнес-функция. Если текущая итерация меньше N, то переходим к шагу 2 [2].

Эксперимент. Данный алгоритм применен для построения нечеткого аппроксиматора. Эксперимент проводился для настройки относительно функции произведения синусов с двумя входами. В качестве параметров используется: количество итераций N=5000, максимальное количество векторов S=30, параметры β_0 =0,8 – взаимная привлекательность светлячков и γ=0,8 – коэффициент поглощения среды.

После выполнения настройки были получены следующие результаты: среднеквадратичная ошибка равна 0,00203, абсолютная ошибка равна 0,03843. Вид полученного расположения функций принадлежности переменных x и y представлен на рис. 1.

В работе алгоритм описан математически, а также приведены графики зависимости значения среднеквадратичной ошибки от изменяемых параметров алгоритма.

ЛИТЕРАТУРА

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

2. Yang X.-S. Firefly Algorithm, Stochastic Test Functions and Design Optimization // International Journal of Bio-Inspired Computation. 2010. № 2. P. 78–84.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ НЕЧЕТКИХ СИСТЕМ НА ОСНОВЕ ПОПУЛЯЦИОННОГО СОРНЯКОВОГО АЛГОРИТМА

А.Е. Анфилофьев, студент

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

г. Томск, ТУСУР, каф. КИБЭВС, yowwi00@gmail.ru

Проект ГПО КИБЭВС-1211 – «Нечеткие системы»

При моделировании сложных систем часто сталкиваются с ситуациями, в которых нет полного описания изучаемого объекта. Решением такой проблемы может стать нечеткое моделирование. При описании объекта, заданного в виде таблицы наблюдений, и отсутствии его математической модели в моделировании и идентификации парамет-

ров исследуемых систем используются методы аппроксимации, среди которых особое место занимают нечеткие аппроксиматоры.

Для построения аппроксиматора необходима идентификация структуры и параметров, то есть определение числа нечетких правил и количество функций принадлежности, на которые разбиты входные и выходные переменные, а также определение неизвестных параметров антецедентов и консеквентов нечетких правил путем оптимизации работы нечеткой системы по заданному критерию. Для оптимизации используются хорошо изученные классические методы, основанные на производных, и метаэвристические, которые менее точны, но эффективнее первых при решении нелинейных, многокритериальных задач оптимизации с ограничениями.

Алгоритм. Рассматривается популяционный сорняковый алгоритм оптимизации. Его суть построена на основе модели способа распространения сорняков на ограниченной территории.

Каждый сорняк является решением. Качество решения (приспособленность сорняка к выживанию) улучшается путем порождения каждым сорняком новых, в зависимости от своей приспособленности. Количество решений остается фиксированным в каждом поколении.

В качестве вектора для оптимизации выступают антецеденты нечеткой системы. Вектор представлен в виде массива X_i, i принимает значения от 1 до $\sum_{j=1}^{L} kO_j$, где L – количество входных переменных нечеткой системы; k – количество переменных, описывающих каждый терм; O_j – количество термов для j-й переменной.

Ниже приведен сорняковый алгоритм оптимизации нечеткой системы.

Шаг 1. Инициализация.

Задается количество итераций N, и максимальное количество векторов, которое может быть сохранено после каждой итерации S. Задаются параметры $n_{\min}$ и $n_{\max}$, которые соответствуют минимальному и максимальному количеству дочерних векторов, которые может породить родительский вектор на каждой итерации. Задается параметр нормального распределения σ. Генерируется начальный вектор X^0 и высчитывается для него среднеквадратичная ошибка и фитнес-функция φ^0 на основе ошибки.

Шаг 2. Для каждого вектора X^S (S принимает значения от 1 до текущего количества векторов) определяется n^S – количество векторов, которое может породить данный вектор.

$$n^s = \frac{n_{max} - n_{min}}{\varphi^{best} - \varphi^{worst}} \varphi^s + \frac{\varphi^{best} n_{min} - \varphi^{worst} n_{max}}{\varphi^{best} - \varphi^{worst}},$$

где φ^{best}, φ^{worst} – лучшее и худшее значение фитнес-функции соответственно.

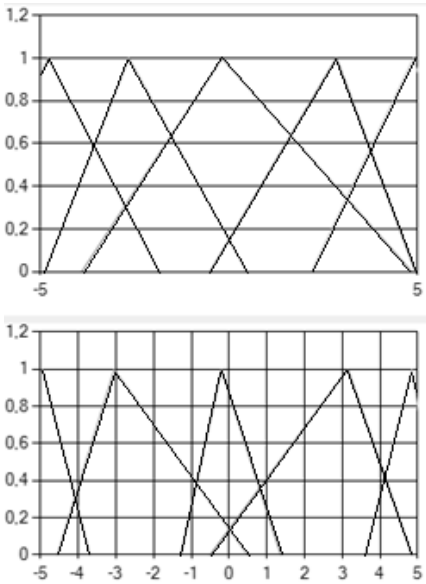
Шаг 3. Для каждого вектора X^S создается n^S новых векторов по правилам:

$$X_i^{s,j} = X_i^s + \sigma_N \sqrt{-2\ln(a)}\cos(b), \quad j = \overline{(1, n^s)} \text{ и } \sigma_N = \sigma((N - N')/N),$$

где N' – номер текущей итерации; *a, b* – случайные числа [0, 1]; X_i^S – компонента вектора X^S.

Шаг 4. Все векторы, включая родительские и дочерние, упорядочиваются по убыванию ошибки. Если количество векторов превышает *S,* популяция уменьшается до *S.* Если текущая итерация меньше *N*, то переходим к шагу 2 [2].

Эксперимент. Данный алгоритм применен для построения нечеткого аппроксиматора (рис. 1). Эксперимент проводился для настройки относительно функции произведения синусов с двумя входами. В качестве параметров используются: количество итераций N=100, максимальное количество векторов S = 20 , параметры $n_{\min} = 1$ и $n_{\max} = 5$, параметр нормального распределения $\sigma = 0{,}5$.



После выполнения настройки были получены следующие результаты: среднеквадратичная ошибка равна 0,00144, абсолютная ошибка равна 0,03656. Вид полученного расположения функций принадлежности переменных *x* и *y* представлен на рис. 1.

Рис. 1. Итоговое расположение функций принадлежности после настройки сорняковым алгоритмом

В работе алгоритм описан математически, а также приведены графики зависимости значения среднеквадратичной ошибки от изменяемых параметров алгоритма.

ЛИТЕРАТУРА

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

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

УМЕНЬШЕНИЕ РАЗМЕРНОСТИ БАЗЫ ПРАВИЛ НЕЧЕТКОГО КЛАССИФИКАТОРА

А.В. Боровков, аспирант каф. КИБЭВС

г. Томск, ТУСУР, ФВС, xander27b@gmail.com

Одной из основных проблем при работе с нечеткими системами является быстрый рост базы правил при росте количества переменных, при использовании всех возможных комбинаций термов. Для 8 переменных при 5 термах на каждой объем базы правил составит 5^8=390625 правил, состоящих из 8 пар переменная – терм каждое.

При генерации набора правил из всех возможных комбинаций термов могут появиться нечеткие правила, под критерии которых не подпадает ни одна точка из наблюдений. Для таких правил результатом конъюнкции посылок будет 0, и их можно удалить, не изменив результат классификации. Рассмотрим результат работы алгоритма на данных из библиотеки KEEL – «iris», «bupa», «glass». Из каждого набора было составлено 5 выборок (табл. 1).

Таблица 1

Результаты экспериментов по очистке таблицы правил

Параметр	iris	bupa	glass
Количество переменных	4	6	9
Количество термов на переменную	5	5	3
Начальное количество правил	625	15625	19683
Среднее количество правил после очистки	203,2	1719,2	3128,4
Отношение количества после очистки количеству до	0,325	0,11	0,159

Нередко требуется обработать данные, в которых не очевидны зависимости между переменными и классом объекта. Поэтому перед настройкой классификатора стоит изучить возможность исключения переменных. Сразу можно исключить переменные, линейно связанные между собой. Такие переменные можно определить по коэффициенту

корреляции, близкому по модулю к 1. При исключении переменных с относительно высоким коэффициентом корреляции (например, 0,75), можно получить отрицательное влияние на точность классификации.

Далее можно изучить возможность исключения других переменных без ущерба для качества классификации. Рассмотрим по шагам способ эмпирического определения влияния переменной на результат классификации. Зафиксируем $\Delta error_{max}$ – максимальное увеличение ошибки, на которое мы согласны для упрощения системы. Выполним настройку классификатора. Ошибку классификации после этой настройки обозначим за $error_0$, затем будем исключать переменные по одной из систем и повторять инициализацию и настройку. Сохраним в отдельное множество все переменные, исключение которых увеличило ошибку не более чем на $\Delta error_{max}$, и будем искать максимально мощное подмножество этого множества такое, что исключение из системы все переменных, принадлежащих этому множеству, увеличит ошибку не более чем на $\Delta error_{max}$. В случае если мы имеем несколько таких подмножеств, мощности которых равны (и больше мощностей других подмножеств), тогда выберем то увеличение ошибки, исключение которого из системы минимально.

После удаления переменных в базе правил появятся правила с одинаковыми антецедентами. Можно объединить группы таких правил в единые правила, заменив антецедент на наиболее часто встречающийся в группе.

Рассмотрим результат работы этого алгоритма на классических данных – «iris». Вся выборка была разбита на 5 пар из обучающей и тестовой выборки. На каждой из переменных изначально было определенно по 5 термов. В качестве метода настройки был использован генетический алгоритм, запущенный на 100 итераций. Затем выбранная система дополнительно обучалась еще 100 итерациями. В качестве эталона была выбрана система, содержащая все переменные и обученная на 200 итерациях генетического алгоритма. При работе был использован алгоритм удаления переменных, были также удалены правила, которым не соответствовали наблюдения (табл. 2).

По результатам эксперимента видно, что использование меньшего количества переменных увеличивает ошибку, причем после дополнительных 100 итераций обучения генетическим алгоритмом разрыв в ошибке может превышать $\Delta error_{max}$, тем не менее разрыв остается довольно незначительным (в пределах 5%) и размерность системы сильно сокращается. К примеру, при проведении этого эксперимента были выделены переменные, наличие или отсутствие которых обеспечивало наибольшее изменение в точности классификации, на основании того, какие переменные чаще всего исключались.

Таблица 2

Результаты эксперимента по исключению переменных

Параметр	Без удаления	Удаление $\Delta error_{max} = 1\%$	Удаление $\Delta error_{max} = 2\%$
Среднее кол-во переменных	4	1,72	1,12
СКО кол-ва переменных	0	0,78	0,32
Среднее кол-во правил	203,2	17,12	5,8
СКО кол-ва правил	8,35	19,08	3,49
Средняя ошибка на обучающей	1,9%	5,8%	5,3%
СКО ошибки на обучающей	0,7%	2%	2%
Средняя ошибка на тестовой	5,1%	9,5%	8,6%
СКО ошибки на тестовой	5,1%	5%	5%

Таблица 3

Частота использования переменных при уменьшении размерности

Переменная	% использования при $\Delta error_{max} = 2\%$	% использования при $\Delta error_{max} = 2\%$
SepalLength	16	4
SepalWidth	8	0
PetalLength	100	76
PetalWidth	48	32

Из табл. 3 видно, что система вполне может обходиться без переменных SepalLength и SepalWidth, но удаление PetalLength и PetalWidth сильно ухудшают точность классификации. На тех же данных был проведен отдельный эксперимент, где для классификации использовалась только одна переменная PetalLength. Классификатор настроен 100 итерациями генетического алгоритма, и средняя ошибка классификации для них составила 10,1% как для тестовой, так и для обучающей выборки.

ПРОЕКТИРОВАНИЕ НЕЙРОННОЙ СЕТИ ДЛЯ МОДЕЛИ ЦЕНТРОБЕЖНОГО НАСОСА

В.А. Чурилов, студент, Е.О. Иванов, аспирант

г. Томск, ТУСУР, каф. АОИ, chvuircitloorv@gmail.com

Проект ГПО АОИ-1301

Рассматривается моделирование многослойной нейронной сети, обучающейся по методу обратного распространения ошибки, с помощью унифицированного языка моделирования UML. Целью данной задачи является получение гибкой структуры, сохраняющей оптимальное быстродействие.

Проектирование нейронной сети с использованием языка UML. В настоящее время при создании сложных программных систем

широко используется принцип объектно-ориентированного программирования, в котором поведение системы определяется взаимодействием объектов. При этом гибкость этого поведения зависит от того, насколько качественно спроектированы объекты (классы) и связи между ними, а также от правильности распределения ответственности (поведения) между объектами.

Базовым классом нейронной сети будет класс (рис. 1), описывающий линейный нейрон и состоящий из обычных для линейного нейрона атрибутов, таких как вектор весов, количество входов, указание, использовать ли пороговый вход и его вес, вспомогательные поля, предназначенные для хранения текущего состояния входов и выходов нейрона (для увеличения производительности). В класс линейного нейрона добавлены методы, инициализирующие его переменные и задающие начальные значения весов случайным образом в определенном диапазоне.

Рис. 1. UML-диаграмма классов для различных нейронов

Зависимости, описывающие работу насоса, являются нелинейными, поэтому необходимо расширить линейный нейрон до нелинейного. Выход линейного нейрона является входом нелинейной функции активации. Следует отметить следующий важный момент: вид функции активации не задается в самом нелинейном нейроне, вместо этого операции вычисления выхода функции активации (и, как следствие, её производной в точке) делегируются на абстрактный класс функции активации.

В роли функции активации были реализованы часто используемые на практике функции, такие как биполярная сигмоидальная функция и функция гиперболического тангенса [1]. Такая схема организации позволяет использовать любую функцию активации, не оказывая влияния на остальную структуру объектов модели сети, и применять

оптимальный вариант вычисления значения ее производной на основе выхода нейрона или кэшированного значения индуцированного локального поля.

Объединим нейроны в слои, а слои – в многослойную нейронную сеть (рис. 2). Такая организация позволит составлять сеть из произвольного набора слоев с линейными и нелинейными нейронами и различными функциями активации.

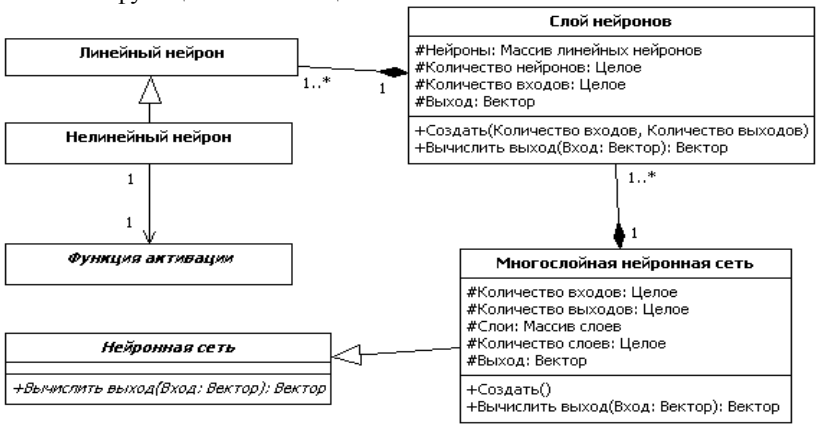


Рис. 2. UML-диаграмма классов многослойной сети

Составив нейронную сеть, введем абстрактный класс учителя, который будет являться реализацией идеи обучения с учителем: предъявление примеров сети и вычисление сигнала ошибки. Как правило, обучение нейронной сети – это длительный процесс, поэтому добавим возможность взаимодействия учителя с внешним миром.

Общение будем осуществлять с помощью сигналов, позволяющих прервать процесс обучения или узнать причину его останова. Определим нового учителя, адаптирующего свободные параметры нейронной сети в соответствии с алгоритмом обратного распространения ошибки (рис. 3).

Для алгоритма обратного распространения ошибки можно использовать последовательный и пакетный режимы обучения, также возможны различные вариации и улучшения, например изменение порядка представления примеров, использование схемы акцентирования. Поэтому представляется целесообразным делегирование потенциально изменяемой части общего алгоритма в отдельный класс (учитель эпохи). Наиболее простым (в терминах реализации) и довольно распространенным является режим предъявления обучающих данных случайным образом (случайный учитель эпохи) на каждой эпохе обуче-

ния. Для предотвращения возникновения явления переобучения сети введен класс, реализующий многократную перекрестную проверку (кроссвалидация) путем разбиения обучающего множества на *K* подмножеств, каждое из которых поочередно используется для тестирования сети [2].

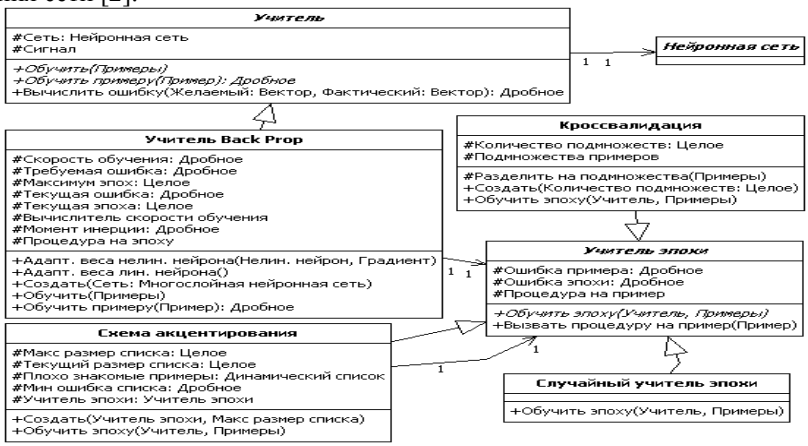


Рис. 3. UML-диаграмма учителя

Заключение. Спроектированная в виде набора диаграмм классов языка UML-модель многослойной нейронной сети, обучающейся по алгоритму обратного распространения ошибки, позволяет достичь высокой гибкости в построении необходимой нейронной сети.

ЛИТЕРАТУРА

1. LeCun Y., Bottou L., Orr G.B., Müller K.-R. Efficient BackProp // Neural Networks: tricks of the trade. Berlin: Springer, 1998. С. 9–50.

2. Zhang P. Model selection via multifold cross validation // The Annals of Statistics. 1993. Vol. 21, №1. С. 299–313.

НЕЙРОСЕТЕВОЕ ЧАСТОТНОЕ УПРАВЛЕНИЕ НАСОСОМ

А.А. Даниленко, М.Б. Байдин, студенты

Руководитель Е.О. Иванов, аспирант

г. Томск, ТУСУР, каф. АОИ, danilenkoprogaleksandr@gmail.com, the_scrubs_fan@mail.ru

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

Для того чтобы алгоритмы управления могли применяться на практике, они должны быть достаточно простыми для реализации и

понимания, должны обладать способностью к обучению, гибкостью, устойчивостью, нелинейностью. В последнее время для целей управления все чаще стали применяться нейронные сети [1].

Нейронным управлением называется применение полностью определенных нейронных сетей для выработки действительных управляющих сигналов [1].

Основные причины применения нейронных сетей в задачах управления [1]:

– нейронные сети могут обучаться любым функциям; способность нейронных сетей к самообучению избавляет от необходимости использовать сложный математический аппарат;

– нейронная сеть может реализовать нелинейное отображение;

– нейроконтроллеры пригодны для управления в условиях существенных неопределенностей;

– высокая степень параллельности нейронных сетей.

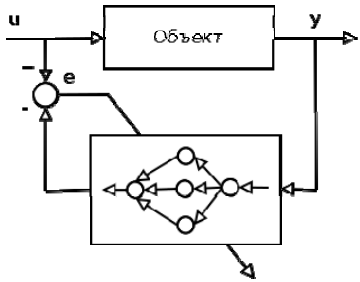


Рис. 1. Архитектура прямого инверсного управления

Для управления насосом была выбрана наиболее простая (но достаточная для рассматриваемого случая) архитектура обобщенного обучения (рис. 1): сеть обучается автономно с использованием образцов, полученных по характеристикам разомкнутого или замкнутого объекта управления. Обученная таким образом сеть настраивается на работу в качестве контроллера для объекта управления, подобно обычной системе управления с обратной связью.

В качестве объекта управления выступает насос, напорная характеристика которого есть функция $H(Q, n)$. Выходным значением нейроконтроллера (управляющим сигналом для объекта управления) будет значение частоты оборотов электродвигателя насоса n для того, чтобы удовлетворить требованиям пользователей в напоре H и подаче Q. Таким образом, последовательная схема нейронного управления будет иметь вид, представленный на рис. 2.

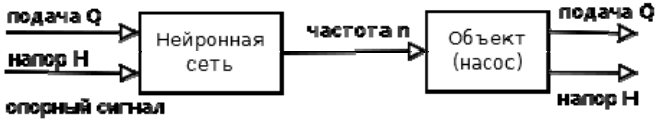


Рис. 2. Последовательная схема нейронного управления насосом

Для получения обучающего множества значения напора и подачи предполагается снимать с приборов, установленных на насосе (манометр и расходомер).

В процессе эксплуатации нейроконтроллера требуемое значение подачи будет получаться из системы верхнего уровня (прогноз), требуемое значение напора должно соответствовать требованиям пользователей водозабора. Такт времени управления – 1 ч.

В качестве нейронной сети контроллера была выбрана многослойная сеть прямого распространения 2-18-1 с обучением по алгоритму прямого распространения.

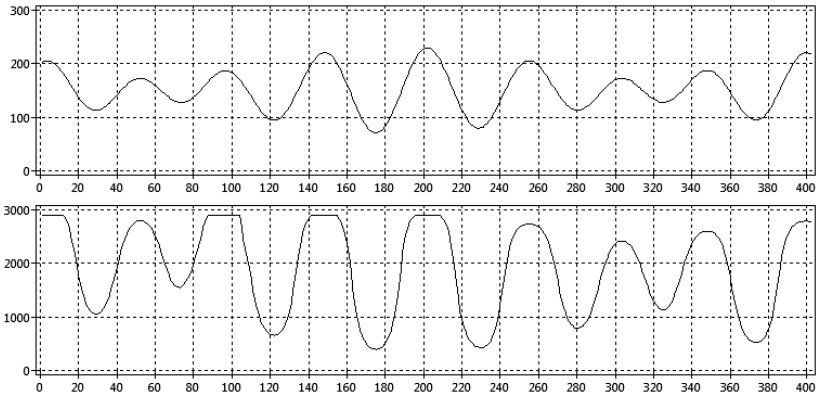


Рис. 3. Работа нейроконтроллера

На рис. 3 представлено моделирование работы нейроконтроллера. Верхний график представляет собой зависимость подачи (или потребления) Q от времени. Требуемый напор H задается пользователем и остается постоянным в пределах времени моделирования. Нижний график задает управляющий сигнал нейроконтроллера, т.е. частоту оборотов n двигателя, которую нужно развить для того, чтобы насос выдал требуемое значение Q и H. Как видим, нейроконтроллер имеет адекватный отклик, а также ограничивает величину управляющего сигнала максимальным значением частоты 2900 об/мин. Также предполагается функционирование насоса в пределах рабочих зон, указанных в его паспорте.

ЛИТЕРАТУРА

1. Сигеру Омату, Марзуки Халид, Рубия Юсоф. Нейроуправление и его приложения. М.: Радиотехника, 2000.

РЕШЕНИЕ ЗАДАЧ АППРОКСИМАЦИИ ФУНКЦИЙ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ, НАСТРАИВАЕМЫХ ГЕНЕТИЧЕСКИМ АЛГОРИТМОМ

Д.В. Федотов, студент каф. системного анализа и исследования операций

г. Красноярск, Сибирский государственный аэрокосмический университет им. акад. М.Ф. Решетнева, fedotov.dm.v@gmail.com

Целью исследования являлась реализация нейронной сети прямой проходимости, тестирование качества аппроксимации в зависимости от структуры сети, коэффициента скорости обучения и настроек генетического алгоритма (ГА) на тестовых задачах и анализ полученных результатов. Использовались следующие параметры сети: на выходном слое и в скрытых слоях активационной функцией нейрона является сигмоида. Алгоритмы обучения сети – обратное распространение ошибки [1]. Настройка весов нейронной сети происходила с помощью ГА. На обучающую и тестовую выборки были наложены помехи с нулевым математическим ожиданием и конечной дисперсией. Все значения ошибок представлены в процентах несоответствия полученных и исходных значений функций, усредненных по выборке.

Для получения результатов были использованы следующие настройки и параметры:

1) на каждых настройках проводилось 100 запусков нейронной сети;
2) каждое множество весов обучалось в течение 1000 эр;
3) алгоритм обучения – обратного распространения ошибки;
4) объем обучающей и тестовой выборок – 100 точек;
5) ошибка по всем запускам усреднялась;
6) тестовая функция: cos(x) на интервале [–2, 6].

Для исследования вопроса влияния структуры сети на качество аппроксимации были сделаны тесты нейронной сети без настройки начальных весов с помощью ГА. Наилучшие результаты были получены при использовании структуры 3×7 (3 скрытых слоя, по 7 нейронов на каждом). Были проведены исследования структур, позволяющих достичь очень точного приближения (по 30 нейронов на слое), однако такие структуры не показали лучших результатов. Для исследования влияния коэффициента скорости обучения на качество аппроксимации были проведены тесты с использованием трех значений коэффициента (0,5; 1; 1,5). Коэффициент скорости обучения позволяет определить меру влияния ошибки приближения на предыдущем шаге. Наилучший результат был получен при значении коэффициента, равном 1 (ошибка 7%, при 0,5 – 9%, при 1,5–15%). Особое внимание следует уделить

влиянию ГА на качество аппроксимации. Для этого было проведено исследование влияниея настроек ГА на точность приближения. Используемая структура сети: 3×7. В качестве оптимизационной функции ГА использует ошибку приближения нейронной сети при подстановке полученных весов без дополнительного обучения. На этом этапе были сняты начальные ошибки приближения, помещенные в табл. 1, после чего было продолжено обучение сети с помощью алгоритма обратного распространения ошибки. Результаты представлены в табл. 2.

Таблица 1

Ошибка приближения после получения начальных весов

Селекция	Скрещивание	Мутация	Ошибка
Пропорциональная	Одноточечное	Средняя	12,17
	Двухточечное	Слабая	12,15
Ранговая	Одноточечное	Средняя	11,59
	Двухточечное	Слабая	11,41
Турнирная (размер турнира = 2)	Одноточечное	Средняя	10,14
	Равномерное	Средняя	10,17
	Равномерное по всей популяции	Средняя	9,04
	Равномерное	Сильная	9,99
	Равномерное по всей популяции	Сильная	9,92

Таблица 2

Влияние начальных весов, отобранных ГА на ошибку

Настройки ГА	Случайные веса		Веса, отобранные ГА		$\lvert E_{ГА} - E_{случ} \rvert$	
	Обуч.	Тест.	Обуч.	Тест.	Обуч.	Тест.
П-О-Ср	8,27	8,57	7,12	7,56	1,15	1,01
П-Д-Сл			5,77	6	2,5	2,57
Р-О-Ср			6,04	6,55	2,23	2,02
Р-Д-Сл			6,89	7,22	1,38	1,35
Т2-О-Ср			5,73	6,06	2,54	2,51
Т2-Р-Ср			5,91	6,41	2,36	2,16
Т2-Р-Си			6,69	6,93	1,58	1,64
Т2-Рп-Ср			7,16	7,81	1,11	0,76
Т2-Рп-Си			7,14	7,66	1,13	0,91

Обозначения настоек ГА, представленные в табл. 2: первая буква – тип селекции (П – пропорциональная, Р – ранговая, Т2 – турнирная с размером турнира – 2 индивида); вторая буква – тип скрещивания (О – одноточечное, Д – двухточечное, Р – равномерное, Рп – равномерное по всей популяции); третья буква – тип мутации (Сл – слабая, Ср – средняя, Си – сильная). $E_{ГА}$ и $E_{случ}$ – ошибки, полученные при использовании весов после ГА и без него (случайным выбором в заданном интервале) соответственно.

Анализируя полученные результаты, можно отметить, что структура 3×7 показала наилучший результат, т.к. обеспечивала достаточную гибкость нейронной сети. В то же время данная структура не допускала переобучения, как получилось со структурой 3×30, которая, показав меньшую ошибку на обучающей выборке, дала большую ошибку на тестовой из-за помех, наложенных на выборки. Значение коэффициента обучения, равное 1, оказалось лучше благодаря тому, что при небольших значениях сеть медленно корректирует веса в сторону точного приближения и не успевает обучиться, при больших – есть вероятность «проскочить» лучшие значения весов. Таким образом, значение, равное 1, оказалось серединой, не позволяющей допускать эти случаи. Относительно применения ГА для настройки начальных весов можно сказать, что при любых настройках результат улучшается. Целесообразно использовать среднюю мутацию и одноточечное или равномерное скрещивание. Однако при сравнении табл. 1 и 2 видно, что выбор лучших начальных весов не гарантирует наименьшую ошибку после обучения сети.

ЛИТЕРАТУРА

1. Хайкин С. Нейронные сети: полный курс. 2-е изд., испр.: Пер. с англ. М.: ООО «И.Д. Вильямс», 2006. 1104 с.

ОЦЕНКА ЭФФЕКТИВНОСТИ ГЕНЕРАЦИИ БАЗ ПРАВИЛ НЕЧЕТКОГО АППРОКСИМАТОРА МОДИФИКАЦИЯМИ АЛГОРИТМА С-СРЕДНИЕ ДЛЯ ЗАДАЧИ ПАРЕТО ОПТИМИЗАЦИИ

И.В. Горбунов, аспирант

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

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

Популярность и практичность нечетких систем основана на их способности выражать сложные и недостаточно понятые связи между данными с помощью нечетких правил [1]. При этом к нечеткой системе, построенной на основе реальных данных, выдвигаются два основных требования: 1) система должна точно воспроизводить данные из анализируемой таблицы наблюдений; 2) эксперт должен понимать смысл каждого правила в контексте данного приложения. Таким образом, построение нечетких систем требует решения задачи многокритериальной оптимизации [2].

В данной работе рассматривается метод построения нечетких аппроксиматоров типа Синглтон, которые являются оптимальными от-

носительно двух критериев: точности и сложности. Сложность в данной работе оценивается суммой числа правил и числа термов нечеткой системы.

Задача оптимизации разделена на два этапа: этап генерации и этап оптимизации. На этапе генерации будут ся модификации алгоритмов нечеткой кластеризации для построения базы правил: нечеткий с-средний (FCM) [3], алгоритм Густавсона–Кесселя (Gustafson–Kessel) [4], алгоритм Гата–Гевы (Gath–Geva) [5]. Этап оптимизации производится методом наименьших квадратов [6].

После формирования кластеров каждым из оригинальных методов кластеризации кластеры проецировались на каждую из осей входных параметров в виде термов с функций принадлежности Гаусса следующим алгоритмом. Алгоритм формирования баз правил из нечетких кластеров:

Вход: Таблица наблюдений $\{\mathbf{x}_p, t_p\}$, матрица центров кластеров **v**, матрица разбиения **u**, экспоненциальный вес m.

Выход: **θ** – база правил аппроксиматора.

S – матрица дисперсий элементов таблицы наблюдения относительно центров векторов по каждому из входных параметров. Матрица содержит строк по количеству кластеров c, столбцов по количеству входых параметров l.

Шаг 1. Расчет размеров проекции кластера для определения параметров функции принадлежности:

$$S_{ij} = \frac{\sum_{k=1}^{n} (\mathbf{u}_{ki})^m \cdot (x_{kj} - v_{ij})^2}{\sum_{k=1}^{n} (\mathbf{u}_{ki})^m}.$$

Шаг 2. Построение функций принадлежности A_{iq}, соответствующих каждому лингвистическому терму; A_{ij}=Gauss($\mathbf{v}_{ij}$, $\sqrt{\mathbf{S}_{ij}}$).

Шаг 3. Заполнение нечеткой базы знаний правилами вида

R_i: **ЕСЛИ** $x_1=A_{i1}$ **И** $x_2=A_{i2}$ **И** $x_3=A_{i3}$ **И** … **И** $x_n=A_{in}$,

ТО r_i = *метод_ближайшего_соседа* ($\{\mathbf{x}_p, t_p\}$, R_i), описывающими каждый кластер.

Эксперимент. Для проведения эксперимента таблицу наблюдений разбивают на q равных по размеру, не пересекающихся блоков согласно методу *контроля по q-блокам* (*q-fold CV*) [7].

Эксперимент проводился на уже разделённых на части наборах данных из репозитория KEEL [8]. Для всех наборов q=10. Методы кластеризации использовались со значением экспоненциального веса m=2.

Для наглядности результаты представлены графически на рис. 1–3 для DEE, Diabets, Ele-2 соответственно.

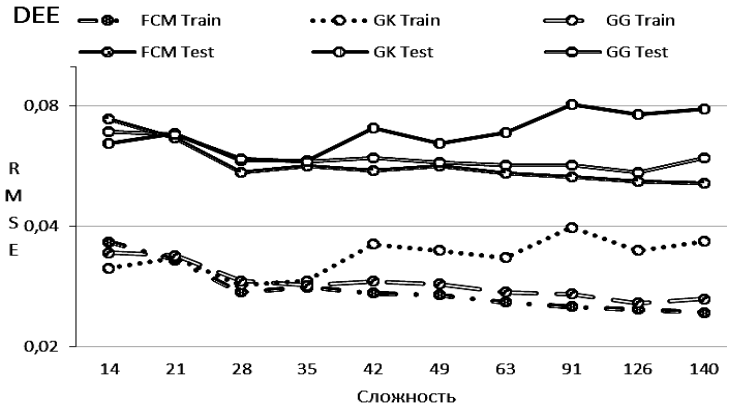


Рис. 1. Результаты на наборе DEE

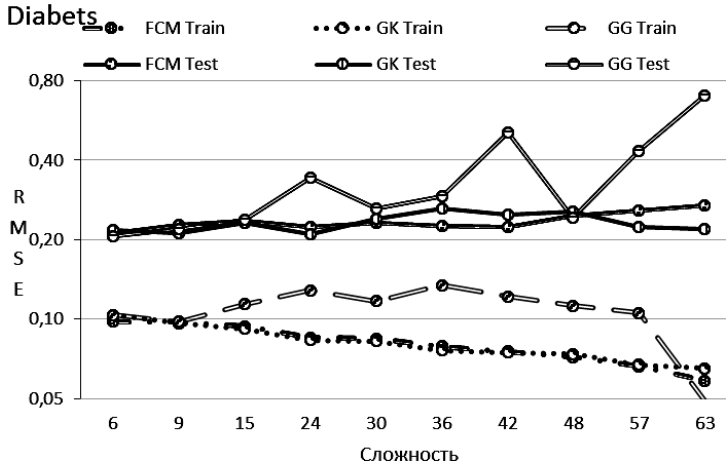


Рис. 2. Результаты на наборе Diabets

Анализ полученных результатов. Условно графики можно разделить на три области. Область малой, средней и высокой базы сгенерированной базы правил. На малой сложности при двух построенных кластерах лидер безусловен, наиболее точные результаты показывает алгоритм Густавсона–Кесселя, остальные алгоритмы показывают переменный результат. На средней области ошибки уменьшаются как на тестовых, так и на обучающих данных и соединяются в близких мало различимых значениях.

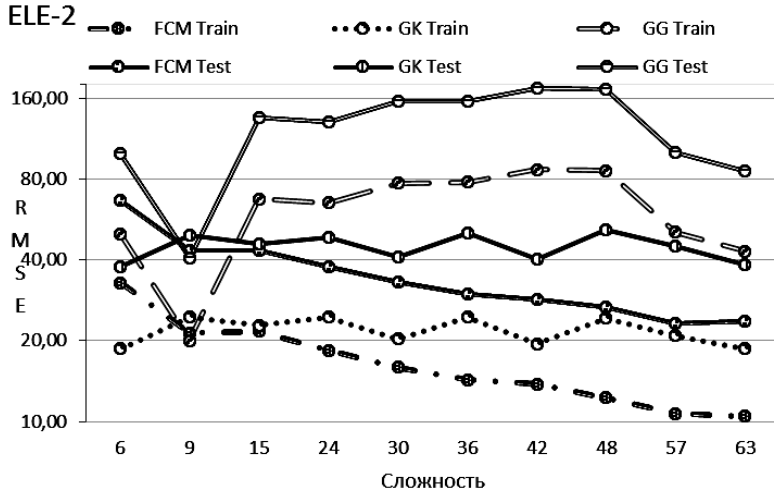


Рис. 3. Результаты на наборе Ele-2

В области высокой сложности не у всех алгоритмов происходит улучшение. Алгоритм Гата–Гевы показывает ухудшение в данной области на наборах Ele-2 и Diabets, а на наборе DEE ухудшение показывает алгоритм Густавсона–Кесселя, при этом по совокупности всех наборов лучший в данной области показывает результат метод нечеткого с-среднего. Таким образом, можно с учетом допущений и ограниченности по количеству проверенных тестов рекомендовать использовать для генерации Парето оптимальных баз правил с малой сложностью алгоритм Густавсона–Кесселя, для баз правил с высокой сложностью – метод нечеткого с-среднего.

ЛИТЕРАТУРА

1. Gonzalez J., Rojas I., Pomares H. etc. Improving the accuracy while preserving the interpretability of fuzzy function approximators by means of multiobjective evolutionary algorithms // Intern. Journ. Approximate Reasoning. 2007. Vol. 44, № 1. P. 32–44.

2. Fazzolari M., Alcala R., Nojima, Y. etc. A Review of the Application of Multiobjective Evolutionary Fuzzy Systems: Current Status and Further Directions // IEEE Trans. Fuzzy Systems. 2013. Vol. 21, № 1. P. 45–65.

3. Bezdek J. Pattern Recognition with Fuzzy Objec-tive Function. N.Y.: Plenum Press, 1981.

4. Gustafson D.E., Kessel W.C. Fuzzy clustering with a fuzzy covariance matrix // IEEE CDC. San Diego, CA, USA. 1979. P. 761–766.

5. Gath I., Geva A.B. Unsupervised optimal fuzzy clustering // IEEE Transactions on Pattern Analysis and Machine Intelligence. 1989. № 11(7). P. 773–781.

6. Ходашинский И.А. Идентификация нечетких систем на базе алгоритма имитации отжига и методов, основанных на производных // Информационные технологии. 2012. №3. С. 14–20.

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

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

ФОРМИРОВАНИЕ ИНФОРМАТИВНОГО ПРИЗНАКОВОГО ПРОСТРАНСТВА С ПОМОЩЬЮ АЛГОРИТМА МУРАВЬИНОЙ КОЛОНИИ

Е.Н. Гусакова, аспирант

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

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, rouxrenard@list.ru

Во многих научно-технических областях в основе решения прикладных задач лежит классификация объектов. Одной из задач, решаемых при классификации, является задача формирования информативного признакового пространства, работа с которым не только упрощала бы задачу классификации, но и гарантировала бы ее высокое качество.

Областью, в которой снижение размерности пространства признаков особенно актуально, является обнаружение сетевых атак: каждое сетевое соединение может быть описано большим количеством информационно неравнозначных характеристик. При этом уточнение ценности каждого отдельного признака в результирующем наборе и выяснение оптимального количества информативных признаков – задача отдельного исследования (feature selection).

В качестве тестового набора данных часто используются данные KDD Cup 1999 [1]. Основными преимуществами этого набора данных является большое количество классов объектов (23), большое количество признаков (41), большое количество записей (5 млн).

Многие исследователи рассматривают задачу селекции признаков как задачу оптимизации [2–4]: при этом максимизируется (или минимизируется) функция, зависящая от процента ошибок, получаемого при обучении модели на итоговом наборе признаков. Решение задачи классификации в данном случае может решаться множеством способов, в частности различного вида эволюционными алгоритмами: классическим, генетическим, алгоритмом бактерий, алгоритмом муравьиной колонии и т.д.

В данной работе рассматривается способ отбора информативных признаков методом муравьиной колонии. Алгоритм муравьиной колонии представляет собой итеративный метод случайного поиска, основанный на моделировании поведения агентов (муравьев) в процессе решения ими оптимизационных задач [5, 6]. В случае решения задачи отбора информативных признаков необходимо представить ее в виде, пригодном для использования метода муравьиной колонии. В частности, набор признаков может быть представлен в виде графа, в котором каждый узел – это признак.

В начале работы алгоритма каждый муравей из колонии устанавливается в какую-то начальную точку (признак). Каждый следующий узел (признак) выбирается методом рулетки в зависимости от количества феромона на ребре, соединяющем текущее положение муравья и предполагаемый следующий узел. При этом вероятность выбора каждой точки вычисляется следующим образом:

$$P_{ij}^{k} = \frac{\tau_{ij}^{\alpha}}{\sum_{j=0}^{n} \tau_{ij}^{\alpha}}. \qquad (1)$$

Количество феромона на каждой итерации рассчитывалось по формуле

$$\tau_{ij} = (1-\rho)\tau_{ij} - \Delta\tau_{ij}, \qquad (2)$$

где $\Delta\tau_{ij} = Q / e_k$; e_k – процент ошибок классификатора.

Муравей останавливается тогда, когда пройдено необходимое количество признаков. Испарение феромона происходит на каждом шаге. На каждой итерации выбирается набор признаков (путь муравья) с минимальной ошибкой. Алгоритм завершается тогда, когда пройдено требуемое количество итераций либо когда минимальная ошибка становится больше (или остается неизменной).

Таким образом, количество феромона на каждой грани обратно пропорционально проценту ошибок, полученному при классификации объектов по этому признаку.

В данном подходе предполагается, что существует какой-то оптимальный набор признаков, на котором классификаторы дают минимальный процент ошибок. Следовательно, на гранях, соединяющих признаки из этого набора, будет максимальное количество феромона. На гранях же, соединяющих неинформативные признаки, феромона должно быть минимальное количество.

До начала работы алгоритма из начального набора данных были удалены атаки, по которым нет достаточного количества данных (количество записей меньше 100).

В качестве классификаторов использовались метод ближайших соседей и наивный байесовский классификатор. Результаты, полученные при использовании двух разных классификаторов, во многом совпадают друг с другом.

Всего было проведено 10 экспериментов (по 5 экспериментов для каждого классификатора). Эксперименты отличались конечной длиной пути муравья: расчеты проводились для 20, 15, 10, 8 и 6 точек (признаков) соответственно. Каждый эксперимент включал 10 итераций. Начальное количество признаков – 38. На каждом шаге процент испарения феромона составляет 10%. Начальное количество феромона – 0,5.

Для каждого классификатора минимальный процент ошибок был получен на наборе из 15 признаков. Изменение процента ошибок с каждой итерацией представлено на рис. 1.

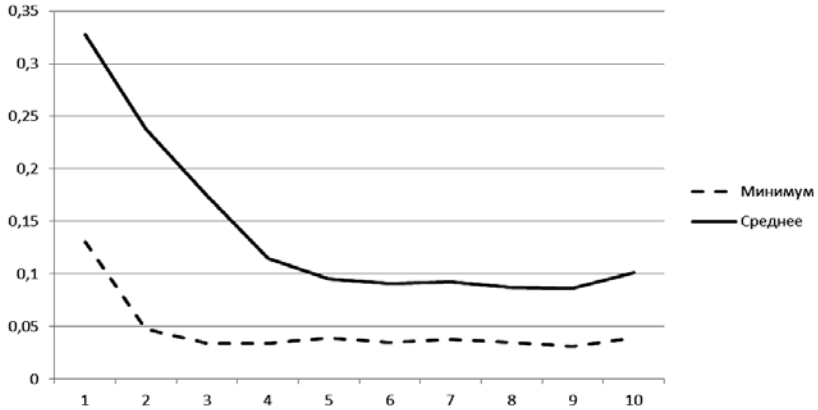


Рис. 1. График зависимости процента ошибок от номера итерации (выбор 15 признаков из 38)

Процент ошибок на лучших наборах признаков колеблется от 1,4 до 1,7%. На основе результатов 10 экспериментов были выбраны наиболее удачные наборы признаков – наборы, при использовании которых процент ошибок был минимален. А затем для каждого признака было подсчитано число наборов (из списка наиболее удачных), в которых он встречается. В результате можно сделать вывод об информативности признаков, а также групп признаков. Так, например, признаки 30 (dst_host_diff_srv_rate) и 31 (dst_host_same_src_port_rate) всегда присутствуют вместе во всех самых успешных наборах признаков. Признак 29(dst_host_same_srv_rate) встречается в тех же наборах, но не встречается в самых удачных наборах из малого количества признаков (6–8). Признаки 6 (hot), 8 (logged_in) и 18 (count_) также часто встречаются вместе. Информативность данных признаков подтверждается и

другими исследователями [7–8]. Признаки, не встречающиеся ни в одном из самых успешных наборов, могут быть признаны неинформативными (9 (num_compromised), 19 (srv_count) и 37 (num_outbound_cmds)), что подтверждается и другими работами [7, 8]. Признак 19 (srv_count) в некоторых работах, например в [7], указывается как информативный для атак, которые в данной работе вообще не рассматривались ввиду малого количества записей по ним (buffer_overflow – всего 30 записей, Loadmodule – 9 и Rootkit – 10 записей).

Таким образом, алгоритм муравьиной колонии показывает неплохие результаты при выборе информативных признаков. В дальнейшем планируется исследовать алгоритм с целью выявления оптимальных его параметров. Кроме того, планируется модифицировать алгоритм таким образом, чтобы длина оптимального набора признаков получалась в результате работы алгоритма, а не задавалась заранее. Возможно совмещение алгоритма муравьиной колонии с другими классификаторами и нечеткими методами.

ЛИТЕРАТУРА

1. KDD Cup 1999 Data [Электронный ресурс]. URL: http://kdd.ics.uci.edu/databases/ kddcup99

2. Олейник А.А., Субботин С.А. Мультиагентный метод с непрямой связью между агентами для выделения информативных признаков // Штучний інтелект. 2009. № 4. С. 75–82.

3. Van G.. Dijck M., Van Hulle M. Wevers Genetic Algorithm for Feature Subset Selection with Exploitation of Feature Correlations from Continuous Wavelet Transform: a real-case Application // International Journal of Computational Intelligence,. 2004.

4. Kim Y., Nick Street W., Menczer F. Feature Selection in Data Mining // Data mining, 2003. P. 80–105.

5. Dorigo M. Optimization, Learning and Natural Algorithms. Politecnico di Milano, Italy, 1992.

6. Dorigo M. The Ant System: Optimization by a colony of cooperating agents // IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics. 1996. Vol. 26, №1. P. 1–13.

7. Adetunmbi A. Olusola, Adeola S. Oladele and Daramola O. Abosede. Analysis of KDD ’99 Intrusion Detection Dataset for Selection of Relevance Features // Proceedings of the World Congress on Engineering and Computer Science 2010. Vol. 1.

8. Shailendra Singh, Sanjay Silakari. An ensemble approach for feature selection of Cyber Attack Dataset // International Journal of Computer Science and Information Security. 2009. Vol. 6, №2. P. 297–302.

МНОЖЕСТВО НЕЧЕТКИХ СИСТЕМ ДЛЯ ВЫБОРА ОПТИМАЛЬНОГО НАПРАВЛЕНИЯ ПАСА В КИБЕРФУТБОЛЬНОЙ СТРАТЕГИИ РОБОТОВ

А.Н. Качалов, аспирант каф. УИ
Научный руководитель И.А. Ходашинский, проф. каф. КИБЭВС., д.т.н.
г. Томск, ТУСУР, alexey.kachalov@yandex.ru

Киберфутбол – это футбол роботов, которые представляют собой электромеханические изделия на двух колесах. Роботы-кубики ездят по специальному игровому полю, управляемые компьютером через радиоканал. Собирает игровую обстановку специализированная видеокамера, подвешенная над полем. Данные от камеры попадают в компьютер, где обрабатываются для распознавания объектов на поле, и затем «игровая обстановка» в виде координат всех роботов и мяча передается программам-стратегиям. Именно программа-стратегия реализует алгоритм команды, принимает решение о движении каждого робота [1].

Перед тем как осуществить пас, необходимо знать, какому из роботов наиболее удобно будет произвести этот пас и в какую точку на поле пас должен быть направлен. Удобность совершения паса можно охарактеризовать через время, необходимое для подъезда в точку, где окажется мяч, и как точно сам робот успеет оказаться в этой же точке. Возможные варианты точки, куда направляется пас, формируются в первую очередь по запросу других роботов, но выбор, если есть еще 4 дружественных робота, как минимум из 4 вариантов паса, должен быть под влиянием величины перспективности самого паса т.е. насколько мяч будет перемещаться ближе и под прямым углом к воротам противника, а также в зону, максимально не занятую противником, и осуществимости паса, т.е. шанса, что мяч не будет перехвачен ни одним из противников во время его передвижения до точки назначения.

Для решения данной задачи путем описания нечеткой логикой, необходимо в первую очередь выделить оценки факторов исполнительности, осуществимости и перспективности на разных нечетких системах, а итоговую оценку оптимальности паса производить уже в другой нечеткой системе на основе результатов значений трех базовых нечетких систем.

Возможность исполнения заданного паса в первую очередь базируется на точном знании необходимого времени перемещения робота в точку исполнения паса. На рис. 1 представлен пример расположения роботов и мяча перед исполнением паса. Для вычисления времени RunawayTime, измеряемого в тактах симулятора, нечеткая система принимает на вход переменные «Расстояние до точки удара по мячу

RB» (3 терма), «Длина перпендикуляра между роботом и прямой направления паса RH» (3 терма), «Угол Angle между прямой перемещения робота Velocity и прямой RA между координатой робота и точкой начала прямой разгона перед пасом» (2 терма), «Текущая скорость робота Velocity» (2 терма).

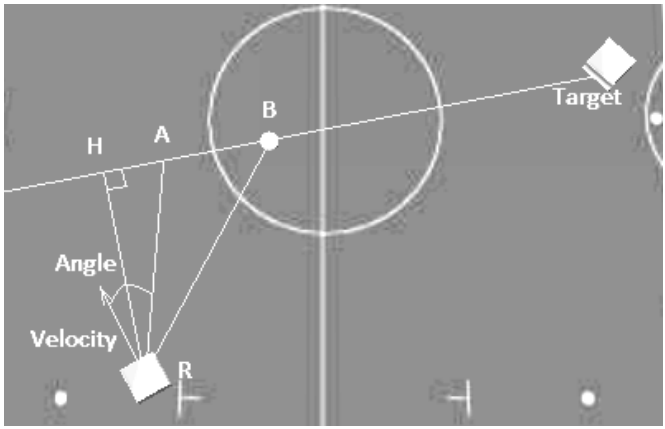


Рис. 1. Положения роботов и мяча перед исполнением паса

Пример правила нечеткой системы типа синглтон с вышеописанным порядком описания переменных представлен ниже:

IF RB = Far AND RH = Average AND Velocity = Low AND Angel = Ang90 THAN RunawayTime = 130.

Оценка перспективности паса Hopefull выполняется нечеткой системой, которая на вход принимает «Расстояние GoalDistance от точки принятия паса до центра ворот» (3 терма) и «Угол GoalAngle между перпендикуляром ворот и прямой, соединяющей центр ворот и точки принятия паса» (3 терма).

Пример правила нечеткой системы типа синглтон с вышеописанным порядком описания переменных представлен ниже:

IF GoalDistance = Close AND GoalAngle = ANG0 THEN Hopefull = 100.

Оценка осуществимости Drawback паса показана на рис. 2, данная нечеткая система принимает на вход переменные «Наименьшее расстояние Distance между роботом и отрезком паса» (4 терма), а также «Угол Angel между наименьшим расстоянием и вектором собственного передвижения» (4 терма).

Пример правила нечеткой системы типа синглтон с вышеописанным порядком описания переменных представлен ниже:

IF Distance = Average AND Angel = ANG60 THEN Drawback = 35.

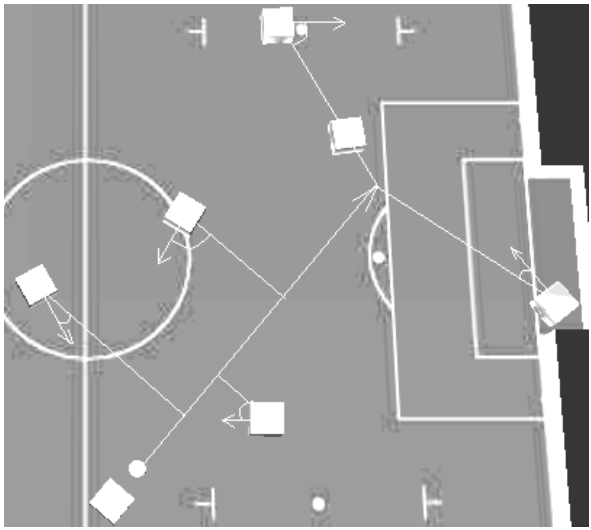


Рис. 2. Положения роботов-соперников относительно траектории паса

Оценка оптимальности паса Optimality выполняется нечеткой системой на основе переменных SumDrawback «Интегральная осуществимость паса» (2 терма), Hopefull «Перспективность паса» (2 терма), RunawayTime «Время перемещения робота к точке удара по мячу для исполнения паса» (3 терма), TimeDifference «Разница времен перемещения робота к точке удара по мячу и перемещения мяча в точку удара» (4 терма).

Пример правила нечеткой системы типа синглтон с вышеописанным порядком описания переменных представлен ниже:

IF SumDrawback = High AND Hopefull = High
AND RunawayTime = Optimal AND TimeDifference = Small
THEN Optimality = 75.

Дальнейшим шагом в работе ожидается обучение нечеткой системы определения , необходимого для перемещения в точку исполнения паса на объективных данных симулятора методом наименьших квадратов.

ЛИТЕРАТУРА

1. Что такое киберфутбол // [Социальная сеть фанатов России]. URL: http://rusfan.ru/posts/117036

ВОЗМОЖНОСТИ УПРАВЛЕНИЯ РОБОТОМ LEGO MINDSTORMS NXT С ПОМОЩЬЮ ЗВУКОВОГО ДАТЧИКА

Ю.О. Лобода, доцент каф. КИБЭВС, магистрант ОКЮ,
В.В. Филатов, студент ФВС
г. Томск, ТУСУР, yulloboda@gmail.com

Целью данной работы является изучение датчика звука в конструкторе LEGO Mindstorms NXT. Изучению подлежит модель функционального блока, у которого еще неизвестны входные и выходные параметры.

Звуковыми (или акустическими) волнами называются распространяющиеся в среде упругие волны, обладающие частотами в пределах 16–20000 Гц. Волны с частотами меньше 16 Гц называются инфразвуковыми, а с частотами более 20000 Гц – ультразвуковыми, и в общем случае слуховым аппаратом человека не воспринимаются [1]. Поскольку звуковой датчик предназначен для реагирования на человеческую речь, нам особенно важна его работа в диапазоне частот от 80 до 1500 Гц, однако датчик может воспринимать и другие диапазоны частот.

Датчик звука является электроакустическим прибором, который преобразовывает звуковые колебания в электрический ток, изменяющийся линейно со звуковой волной. В основу работы микрофона положен принцип действия звуковых колебаний на тонкую мембрану. Колебания внутренней мембраны микрофона порождают электрические колебания. Напряжение, возникающее в процессе работы датчика, подается на интерфейс для сбора данных [2].

Звуковой датчик, используемый в конструкторе LEGO Mindstorms NXT, может работать в двух режимах: dB и dBA. На рис. 1 представлены сравнительные характеристики датчика при работе в разных режимах [3].

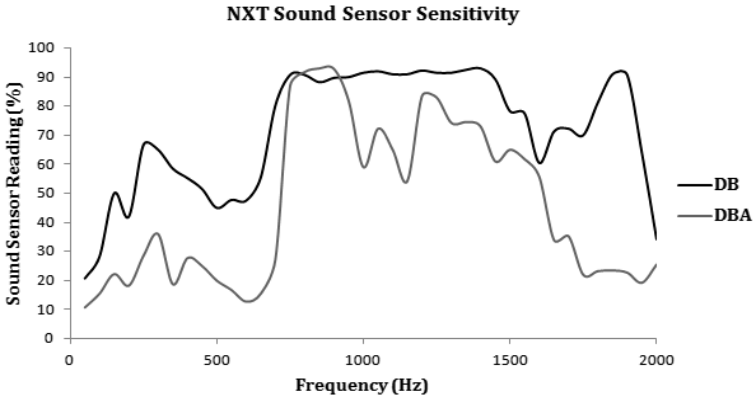


Рис. 1. Сравнительные характеристики работы звукового датчика в режимах dB и dBA [3]

Из рис. 1. видно, что в режиме dB самым равномерным и «гладким» диапазоном частот является 800–1400 Гц, который позволяет захватить большее количество воспринимаемых человеческому уху звуков.

Следующий рис. 2 демонстрирует детектирование датчиком звуковых импульсов, генерируемых другим роботом NXT, запрограммированным издавать звук фиксированной частоты, равной 1100 Гц [3].

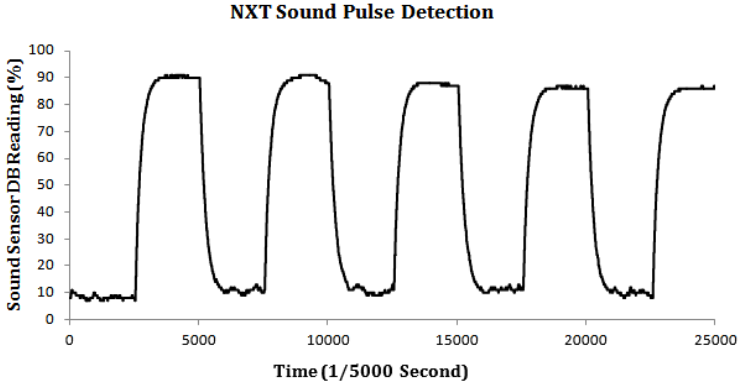


Рис. 2. Детектирование звуковых импульсов, издаваемых другим роботом NXT на частоте 1100 Гц [3]

Исходя из теоремы Котельникова [4], для того чтобы восстановить исходный аналоговый сигнал со сколь угодной точностью по своим дискретным отсчетам взятым с частотой f, необходимо, чтобы выполнялось условие

$$f > 2f_c,$$

где f_c – максимальная частота, которой ограничен спектр реального сигнала [4].

Таким образом, анализируя график, приведенный на рис. 2, видим, что звуковой датчик неспособен различать колебания разных частот в спектре сигнала, но это не мешает датчику реагировать на амплитуду сигнала. Этот эксперимент показал, что датчик легко может обнаруживать звуковые импульсы, когда они громче, чем окружающий шум [3].

Эксперименты с измерением зависимости чувствительности от расстояния показали, что датчик способен детектировать амплитуду звукового сигнала лишь на расстоянии не более 0,7 м.

Заключение. Ограничения, установленные в ходе экспериментов, позволяют судить о предназначении датчика для того, чтобы продемонстрировать принципиальные возможности по работе со звуком. Чтобы обрабатывать в реальном времени звуковой сигнал, необходимы вычислительные мощности, которых недостаточно в микроконтролле-

ре конструктора Lego Mindstorms NXT. Робот может регистрировать лишь амплитуду сигнала в процентном соотношении от 0 до 100%, т.е. производить измерения в условных единицах.

ЛИТЕРАТУРА

1. Трофимова Т.И. Курс физики: учеб. пособие для студ. 19-е Изд., стер. М.: Изд. центр «Академия», 2012. 560 с.

2. Технические средства обучения // [Сайт о технических средствах обучения]. URL: http://новаяшкола.рф/uchebno-laboratornoe-oborudovanie/datchiki-dlya-shkoly/datchiki-po-fizike/datchik-zvuka (11.03.2013).

3. NXT Sound System // [University of Hawaii, Departament of Information and Computer Sciences]. URL: http://www.jade-cheng.com/uh/projects/nxt-sound/ (11.03.2013).

4. Википедия – свободная энциклопедия // [Авторские энциклопедические статьи]. URL: http://ru.wikipedia.org/wiki/Теорема_Котельникова (11.03.2013).

ОЦЕНКА ИНФОРМАТИВНОСТИ ПРИЗНАКОВ СЕТЕВЫХ АТАК

М.А. Мельников, А.В. Мальцев

Научные руководители: Е.Ю. Костюченко, доцент, к.т.н., Е.М. Давыдова, доцент, к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, gpo.neural.network@gmail.com

Проект ГПО КИБЭВС-1005 – «Анализ сетевого трафика на основе нейронных сетей»

Целью данной работы является выявление наиболее информативных признаков сетевых вторжений различными методами. В качестве исходных данных использовалась база данных, созданная университетом MIT в 1999 г. Специально подготовленная программа в течение 7 недель накапливала данные о сетевых соединениях по различным параметрам. 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 около 100 байт.

Атаки разделяются на четыре основных категории:

− DOS: отказ в обслуживании, например syn-flood;

− R2L: неавторизованный доступ от удаленной машины, например подбор пароля;

− U2R: неавторизованный доступ к привилегиям локального суперпользователя (root), например различные атаки на переполнение буфера;

− пробы: обследования и другие пробы, например сканирование портов.

Изначально данные были собраны в текстовый файл, где каждая строка представляет собой вектор из 41 значения-признака. Однако признаки далеко не равнозначны, поэтому очень важной задачей является поиск и отбор признаков, *достаточно информативных* для распознавания.

Решающим критерием информативности признаков в задачах классификации является, конечно, процент ошибок. Чем информативнее признак, тем выше процент ошибок при его отсутствии в итоговом наборе признаков. Однако даже если распределения генеральной совокупности известны, вычисление процента ошибок связано с очень большими затратами машинного времени. Данная работа была проделана ранее, мы же дадим математическую оценку признакам, что позволит сравнить полученный результат с уже имеющимся и выделить наиболее оптимальное подпространство признаков.

Для этого воспользуемся информационным подходом, согласно которому информация признака рассматривается как достоверное различие между классами образов в пространстве признаков. Оценку информативности можно дать несколькими методами: накопления частот, Шеннона, Кульбака.

Метод накопленных частот. Сущность этого метода состоит в том, что если имеются 2 выборки признака x, принадлежащие 2 различным классам, то по обеим выборкам в одних координатных осях строят эмпирические распределения признака x и подсчитывают накопленные частоты (сумму частот от начального до текущего интервала распределения). Оценкой информативности служит модуль максимальной разности накопленных частот.

Метод Шеннона. Предлагает оценивать информативность как средневзвешенное количество информации, приходящееся на различные градации признака. Под информацией в теории информации понимают величину устраненной энтропии.

Метод Кульбака. Предлагает в качестве оценки информативности меру расхождения между двумя классами, которая называется дивергенцией.

На данный момент успешно реализованы методы накопленных частот и метод Шеннона. Полученные результаты оценки информативности приведены на рис. 1.

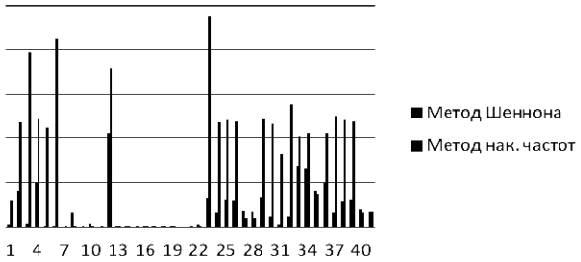


Рис. 1. Сравнительные оценки информативности признаков

Значения информативности для метода Шеннона лежат в интервале [0; 1]. Значения же для метода накопленных частот напрямую зависят от рассматриваемой выборки и для наглядного представления были пронормированы по ее размеру. В дальнейшем благодаря полученным и уже ранее имевшимся данным будет проведена минимизация признакового пространства, что позволит оптимизировать работу имеющейся нейронной сети

ЛИТЕРАТУРА

1. База данных атак, составленная университетом. MIT, 1999. http://kdd.ics.uci.edu/databases/kddcup99/

2. Список признаков http://kdd.ics.uci.edu/databases/kddcup99/task.html

3. Дашутина Е.В., Меркулова Е.В. Проектирование СКС-диагностики сердечно-сосудистых заболеваний // Інформаційні управляючі системи та комп'ютерний моніторинг (ІУС КМ-2012)–2012: матер. ІІ міжнар. наук.-техн. конф. студентів, аспірантів та молодих вчених. Донецьк: ДонНТУ, 2012. С. 285–288.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ НЕЧЕТКИХ СИСТЕМ НА ОСНОВЕ ПОПУЛЯЦИОННОГО АЛГОРИТМА «КУКУШКИН ПОИСК»

Д.Ю. Минина, студентка

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

г. Томск, ТУСУР, каф. КИБЭВС, pound_2007@mail.ru

Проект ГПО КИБЭВС-1211 – «Нечеткие системы»

Моделирование сложных систем осложняется проблемой неточного или неполного описания изучаемого объекта. Одним из решений такой проблемы является нечеткое моделирование. В тех случаях, когда описание объекта задано в виде таблицы наблюдений и отсутствует математическая модель данного объекта, в компьютерном модели-

ровании и идентификации параметров исследуемых систем используются методы аппроксимации, среди которых особое место занимают нечеткие аппроксиматоры.

Для построения аппроксиматора необходима идентификация структуры и параметров. Идентификация структуры включает определение числа нечетких правил и количество функций принадлежности, на которые разбиты входные и выходные переменные. Идентификация параметров включает определение неизвестных параметров антецедентов и консеквентов нечетких правил путем оптимизации работы нечеткой системы по заданному критерию. Для оптимизации используются хорошо изученные классические методы, у которых есть свои недостатки, и метаэвристические, которые менее точны, но зачастую эффективнее первых при решении нелинейных, многокритериальных задач оптимизации с ограничениями.

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

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

Приводится описание пошагового алгоритма.

Шаг 1. Инициализация исходной популяции.

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

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

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

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

Задается количество итераций для работы алгоритма в качестве критерия остановки.

Шаг 2. Генерация нового решения на основе полетов Леви.

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

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

Шаг 3. Оценка качества решения.

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

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

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

Выбирается заранее заданное количество «худших» решений (с наибольшим значением среднеквадратичной ошибки), для каждого из которых генерируется случайное число. Если оно оказывается больше заранее заданного, то гнездо удаляется (удаляется вектор решения).

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

Шаг 5. Итерации продолжаются заданное количество раз.

Эксперимент. Данный алгоритм применен для построения нечеткого аппроксиматора (рис. 1). Эксперимент проводился для аппроксимации функции произведения синусов с двумя входами. Удалось добиться уменьшения среднеквадратичной ошибки относительно равномерно распределенных по области определения функций принадлежности, взятых за начальное значение, более чем в два раза.

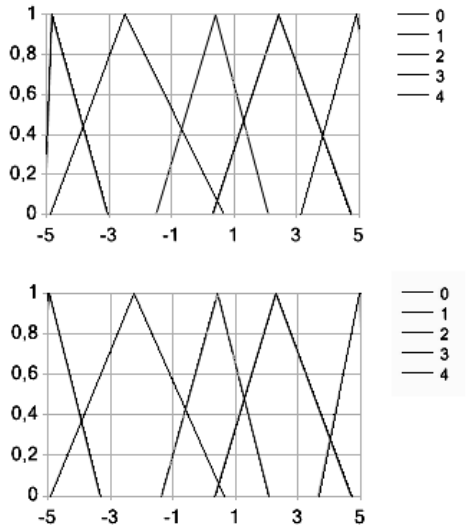


Рис. 1. Итоговое расположение функций принадлежности после настройки алгоритмом «кукушкин поиск»

В работе алгоритм описан математически, а также приведены графики зависимости значения среднеквадратичной ошибки от изменяемых параметров алгоритма.

ЛИТЕРАТУРА

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

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

АЛГОРИТМЫ И ПРОГРАММНЫЕ СРЕДСТВА ПОСТРОЕНИЯ НЕЧЕТКИХ КЛАССИФИКАТОРОВ НА ОСНОВЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА

С.А. Рубанов, студент

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

г. Томск, ТУСУР, каф. КИБЭВС, mescalito86@gmail.com

Под классификацией подразумевают процесс отнесения объектов исследования к некоторым классам в зависимости от каких-либо характерных признаков данного класса. Характерные признаки выявляются путем обнаружения закономерных связей межу элементами таблицы, на основании которой будет проводиться классификация.

Классификация используется во многих областях современной жизни, начиная от определения заболевания на основании каких-либо анализов и заканчивая обнаружением атак на сервер, основываясь на параметрах запроса.

Нечеткий классификатор. Существует множество алгоритмов и методов, на основании которых может быть построен классификатор. В данной работе был разработан и реализован нечеткий классификатор (НК), т.е. классификатор, основанный на нечеткой логике, а алгоритмом настройки данного классификатора был выбран генетический алгоритм.

Обработка лингвистической информации в нечеткой системе происходит при помощи базы правил. Каждое правило состоит из двух частей: условной и заключительной. Антецедент или условная часть (IF-часть) содержит утверждение относительно значений входных переменных, в консеквенте или заключительной части (THEN-части) указывается значение, которое принимает выходная переменная [1].

Для нечеткого классификатора *i*-е правило представлено следующим образом:

$$IF\ x_1 = A_{1i}\ AND\ x_2 = A_{2i}\ AND\ \ldots\ AND\ x_n = A_{ni}\ THEN\ class = c_j,$$

где c_j – идентификатор j-го класса.

Нечеткая классификация описывается функцией $f: R^n \to [0,1]^m$, которая относит классифицируемый объект к каждому классу с определенной степенью принадлежности, вычисленной следующим образом: $\beta_j(x) = \sum_{R_{ij}} \prod_{k=1}^{n} A_{ki}(x_k)$, j=1, 2, … , m.

Выходом классификатора является класс, определяемый следующим образом: $class = c_{j^*}$, где $j^* = \arg\max_{1 \le j \le m} \beta_j$.

Нечеткий классификатор может быть представлен как функция $c = f(x, \Xi)$, где Ξ – база правил.

Пусть дано множество обучающих данных (таблица наблюдений) $\{(x_p; c_p), p = 1, \ldots, z$, определим следующую единичную функцию:

$$delta(p, \Xi) = \begin{cases} 1, \text{ если } c_p = f(\mathbf{x}_p, \Xi) \\ 0, \text{иначе} \end{cases}, p = 1,2...,z,$$

тогда численный критерий адекватности системы классификации может быть выражен следующим образом: $E(\Xi) = \dfrac{\sum_{p=1}^{z} delta(p, \Xi)}{z}$.

Проблема идентификации НК сводится к проблеме поиска максимума заданной функции в многомерном пространстве, координаты которого соответствуют параметрам нечеткой системы.

Генетический алгоритм (ГА). Оперирует популяцией искусственных элементов или хромосом, которые кодируют возможные решения, таким образом, популяция – это множество хромосом, созданных на текущем шаге работы алгоритма. Хромосома представляет собой последовательность генов. Хромосома – это одно решение задачи или точка в пространстве поиска решений. Ген кодирует один параметр задачи или координату в пространстве поиска. Обычно хромосома – это строка чисел или символов. Для оценки качества решения вводится целевая функция [2].

Работа ГА начинается с задания начальной популяции. Следующая популяция создается с использованием так называемых генетических операторов, в которых отражены важные эволюционные принципы типа наследования, выживания самых приспособленных и случайных изменений. Полученные новые хромосомы называются потомками. Цикл перехода от одной популяции к другой называется поколени-

ем. Путем регулирования процедур применения генетических операторов ГА добивается того, что приспособленность хромосом в среднем возрастает от поколения к поколению. Генерация популяций прекращается после достижения заданных критериев завершения, главным из которых является критерий обнаружения оптимального решения.

Эксперимент. Работоспособность классификатора проверена на двух выборках: iris (классификация цветков ириса) и bupa (классификация заболеваний печени) [3]. Тесты проводились по схеме кроссвалидации, т.е. набор разбивался на пять файлов, 90% набора помещается в обучающую выборку, а остальные 10% в тестовую. Результаты тестов были сопоставлены с публикаций [4], где тесты проводились на тех же данных (таблица).

Результаты эксперимента и сравнение с аналогами

Набор данных	Обучающая выборка				Тестовая выборка			
	bupa		iris		bupa		iris	
	Среднее	СКО	Среднее	СКО	Среднее	СКО	Среднее	СКО
АПК + МАПК	79,55	1,72	98,59	0,42	63,06	10,34	88,00	4,22
Ant Miner	80,38	3,25	97,26	0,74	57,25	7,71	96,00	3,27
Core	61,93	0,89	95,48	1,42	61,97	4,77	92,67	4,67
Hider	73,37	2,70	97,48	0,36	65,83	10,04	96,67	3,33
Sgerd	59,13	0,68	97,33	0,36	57,89	3,41	96,67	3,33
Target	68,86	0,89	93,50	2,42	65,97	1,41	92,93	4,33
ГА	78,14	3,06	99,65	0,67	58,97	10,49	94,93	4,95

Заключение. В ходе проделанной работы был разработан нечеткий классификатор, основанный на генетическом алгоритме. Был поставлен эксперимент, и результаты сравнены с аналогами. По результатам сравнения можно увидеть, что данный нечеткий классификатор показал себя не хуже аналогов.

ЛИТЕРАТУРА

1. Ходашинский И.А. Построение нечетких систем прогнозирования эффективности немедикаментозного лечения / И.А. Ходашинский, А.А. Зайцев, И.В. Горбунов и др. // Информатика и системы управления. 2012. № 3 (33). С. 140–150.

2. Ходашинский И.А. Технология идентификации нечетких моделей типа синглтон и Мамдани / И.А. Ходашинский // Тр. VII Междунар. конф. «Идентификация систем и задачи управления», SICPRO'08 / Ин-т пробл. упр. М., 2008. С. 137–163.

3. Knowledge Extraction Evolutionary Learning [Электронный ресурс]. Режим доступа: http://sci2s.ugr.es/keel/datasets.php

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

АЛГОРИТМ ГЕНЕРАЦИИ АССОЦИАТИВНЫХ ПРАВИЛ ДЛЯ ДАННЫХ С НЕПРЕРЫВНО МЕНЯЮЩИМИСЯ ПАРАМЕТРАМИ

Д.С. Синьков, аспирант

Научный руководитель И.А. Ходашинский, 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) [1].

Анализируемые параметры при поиске взаимосвязей в корзине – идентификаторы продуктов, встречающихся в транзакциях, поэтому изначально алгоритмы поиска ассоциативных правил разрабатывались на дискретные или категориальные данные. Но в реальных задачах существует потребность установления взаимосвязей между величинами, представленными непрерывно, например взаимосвязь между параметрами ирисов и их классами [2].

Пусть $I = \{i_1, i_2, i_3, \ldots i_n\}$ – набор параметров объектов, представленных непрерывно, $C – \{c_1, c_2, c_3, \ldots c_m\}$ – классы, к которым относятся объекты с определенными значениями параметров. D – множество всех объектов, где каждый объект имеет конкретные значения параметров из I и принадлежит к классу из C.

Задача состоит в том, чтобы установить взаимосвязи между непрерывно изменяющимися параметрами из I множества объектов D и сгенерировать правила, определяющие определенные классы из C.

В работе приводится решение данной задачи на основе теории нечетких множеств и алгоритма apriori для генерации правил.

Описание алгоритма. На первом этапе необходимо преобразовать непрерывные значения параметров объектов в категориальное представление. Для этого необходимо покрыть область определения параметра функциями принадлежности, то есть для каждого параметра из I создать лингвистическую переменную, описывающую его изменение на области определения (на рис. 1 представлен пример покрытия параметра *sepalLength* ирисов).

Таким образом, каждому непрерывному значению параметра из I каждого объекта из D будет соответствовать лингвистическое значение из $FM = \{fm_1, fm_2, fm_3, \ldots fm_n\}$, где FM – множество термов функций принадлежностей.

Результатом этапа предобработки будет преобразованная база объектов из D в D', где значения непрерывных параметров заменены

на категориальные значения, сгенерированные на основе функций принадлежности.

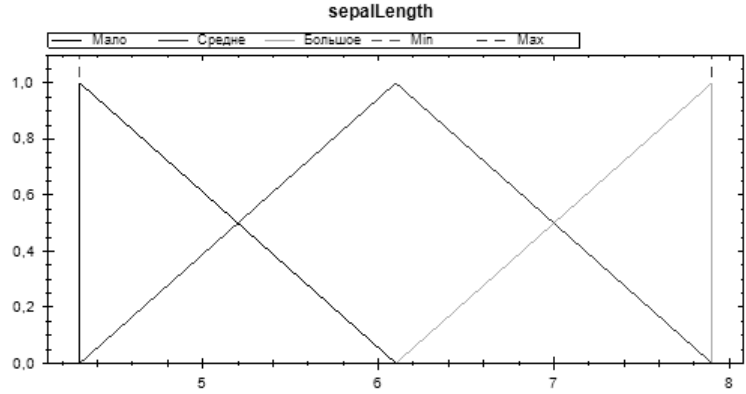


Рис. 1. Покрытие параметра sepalLength ирисов

После предобработки данных запускается алгоритм apriori, с заданной поддержкой и достоверностью. Результатом работы будеут сгенерированные правила вида

ЕСЛИ $i_{11} = fm_{11}$ и $i_{21} = fm_{21}$ и … и $i_{n1} = fm_{n1}$ ТО CLASS = c_k.

Программа комплекса. Программа для генерации ассоциативных правил была разработана на C#. Ниже показана форма представления сгенерированной базы правил (рис. 2).

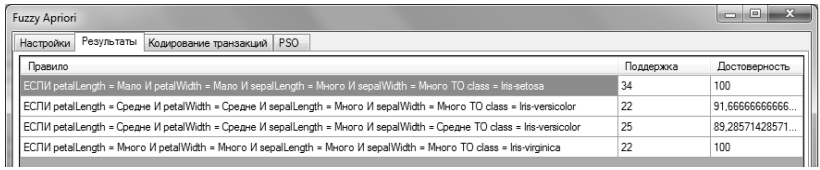


Рис. 2. Окно программы анализа, сгенерированные ассоциативные правила

Данные в программу загружаются в формате KEEL. Тестировалось приложение на данных KEEL об ирисах. Результат работы и сгенерированные правил можно видеть на рис. 2. Дальше планируется работа по созданию классификатора на основе данного генератора правил.

ЛИТЕРАТУРА

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

2. Шахиди А. Введение в анализ ассоциативных правил [Электронный ресурс]. Режим доступа к сайту: http://www.basegroup.ru/library/analysis/association_rules/intro/

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ТЕСТИРОВАНИЯ ПРОГРАММ

В.А. Соловьев, А.А. Ханефт, И.В. Черноусов, студенты каф. АСУ,
В.А. Дель, студент каф. КИБЭВС
г. Томск, ТУСУР, SoVictor_tomsk@hotmail.com
Проект ГПО АСУ-1101 (КИБЭВС-1102) – «Программное обеспечение для организации и проведения спортивного программирования»

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

Анализ, проводимый человеком, не может являться объективным. Альтернативным методом является тестирование – подача на вход программы набора тестов и сравнение реальных выходных данных с ожидаемыми выходными данными. Для достижения объективной оценки количество тестов должно быть достаточным для покрытия всех возможных ситуаций.

Задачей нашего проекта является разработка системы, позволяющей проводить автоматизированную проверку решений поставленных задач и обладающей следующими характеристиками: высокая производительность, доступность результатов проверки в реальном времени, интерактивное взаимодействие с пользователем, совместимость с правилами олимпиад по программированию ACM, возможность запуска решения на исчерпывающем наборе тестов с указанными ограничениями.

Терминология. Задачей будем называть вычислительную проблему, имеющую чётко сформулированное условие, строгий формат входных и выходных данных, алгоритм проверки соответствия входных данных выходным и ограничения на память и процессорное время.

Решение задачи – исходный код программы, написанный на одном из доступных пользователю языков программирования, получающий по заданным входным данным выходные.

Алгоритм проверки – последовательность действий, позволяющая по ожидаемым и реальным выходным данным сформировать вердикт о правильности решения.

По результатам тестирования решение получает вердикт. При одновременном выполнении нескольких условий получения генерируется вердикт, находящийся выше в таблице.

Структура системы. Разработанная нами система состоит из логически независимых блоков: интерфейса пользователя (сайта), базы данных и сервера тестирования. Пользователь взаимодействует с сайтом, информация с сайта записывается в базу данных, после чего сер-

вер обрабатывает её: ядро тестирующей системы формирует вердикт, который заносится в базу данных и передаётся на сайт (рис. 1).

Вердикты тестирования

Вердикт	Расшифровка	Условие получения
SE	System error	Ошибка на стороне сервера
CE	Compilation error	Ошибка компиляции решения
TLn	Time limit exceeded on test *n*	Превышено допустимое время работы на тесте *n*
MLn	Memory limit exceeded on test *n*	Попытка использовать больше памяти, чем дозволено
REn	Runtime error on test *n*	Программа завершилась с ненулевым кодом возврата
PEn	Presentation error on test *n*	Ошибка в формате выходных данных на тесте *n*
WAn	Wrong answer on test *n*	Получен неверный ответ на тесте *n*
AC	Accepted	Успешно пройдены все тесты, решение правильное

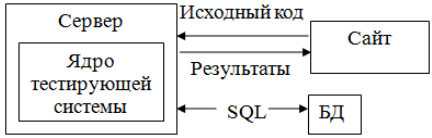


Рис. 1. Архитектура системы

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

Ядро выполняет компиляцию полученного от сервера решения, последующий его запуск на наборе тестов и отслеживание выполнения установленных ограничений [1].

Для решения поставленной задачи были использованы современные инструменты: система контроля версий Subversion, фреймворк Ruby On Rails [2], СУБД PosgreSQL.

Благодаря такому выбору разработанная система обладает гибкой архитектурой, что позволяет вносить изменения по мере необходимости, облегчает сопровождение.

Заключение. К настоящему моменту разработана автоматизированная система тестирования программ, обладающая высокой скоростью обработки поступающей информации, обеспечивающая доступность результатов проверки в реальном времени. Система поддерживает запуск решения на наборе тестов с заданными ограничениями [3].

Разработанная система может быть использована как в учебном процессе, так и для проведения студенческих олимпиад по спортивному программированию, правила которых совместимы с форматом олимпиад ACM.

ЛИТЕРАТУРА

1. ACM ICPC Regional Rules [Электронный ресурс]. Режим доступа: http://icpc.baylor.edu/info/Regional+Rules, свободный (дата обращения: 31.08.2012).

2. Ruby S. Agile Web Development with Rail / S. Ruby, D. Thomas, D. Hansson. Dallas: The Pragmatic Bookshelf, 2012. 476 p.

3. Кирнос В.Н., Дель В.А., Дорошенко Т.Ю., Соловьев В.А., Ханефт А.А. Автоматизированная система тестирования программ // Современное образование: проблемы обеспечения качества подготовки специалистов в условиях перехода к многоуровневой системе высшего образования: матер. междунар. науч.-метод. конф. 2–3 февраля 2012 г., Россия. Томск: Изд-во Том. гос. ун-та. С. 81–82.

ОПТИМИЗАЦИЯ НЕЙРОННОЙ СЕТИ ДЛЯ МОДЕЛИ ЦЕНТРОБЕЖНОГО НАСОСА

Д.И. Цыбусов, студент каф. АОИ

Научный руководитель Е.О. Иванов, аспирант

г. Томск, ТУСУР, каф. АОИ, demonbusov1@yandex.ru

Проект ГПО АОИ-1301

Для решения задач дискретной и непрерывной оптимизации активно используется искусственная нейронная сеть Хопфилда, которая представляет собой однослойную сеть с обратными связями. Оптимизирующие свойства сети Хопфилда заключаются в ее способности минимизировать функцию энергии.

В работе [2] автор с помощью нейронной сети Хопфилда решает классическую задачу оптимизации – задачу коммивояжера (ЗК). Если имеется n городов, то для решения ЗК нам потребуется $n \Downarrow n$ нейронов. Пусть каждый нейрон снабжён двумя индексами, которые соответствуют городу и порядковому номеру его посещения в маршруте. Например, $OUT_{xj} = 1$ показывает, что город x был j-м по порядку городом маршрута, тогда функция энергии, применяемая в работе [1], находится как

$$E = \frac{A}{2}\sum_x \sum_i \sum_{j \neq i} OUT_{xi} OUT_{xj} + \frac{B}{2}\sum_i \sum_x \sum_{y \neq x} OUT_{xi} OUT_{yi} + \frac{C}{2}\left[\left(\sum_x \sum_i OUT_{xi}\right) - n\right]^2,$$

где A, B, C – некоторые константы.

Тогда изменение значения весов:

$$W_{xi,yi} = -A\delta_{xy}(1-\delta_{ij}) - B\delta_{ij}(1-\delta_{xy}) - C - Dd_{xy}(\delta_{j,i+1} + \delta_{j,i-1}),$$

где δ_{ij} – символ Кронекера.

Обучение происходит до тех пор, пока система не стабилизируется.

Хопфилд и Тэнк в своих опытах утверждали, что в случае задачи с 30 городами полное число маршрутов приблизительно равно $4{,}4\times10^{30}$. Экономия, даваемая сетью, составила в этом случае 10^{20}, преимущества нейронных сетей перед полным перебором очевидно. Следующим нашим шагом мы попытаемся повторить опыты ученых с использованием языка Object Pascal.

Дальнейшие работы ведутся в направлении применимости сетей Хопфилда при оптимальном управлении группой объектов (например, водяных насосов). При этом дискретная задача оптимизации сводится к распределению нагрузки на объекты путем определения режимов их работы (рис. 1). Требуется подобрать такую функцию энергии, которая определяла бы режим работы насосов: 0 – выключить, 1 – включить, с учетом минимизации общей потребляемой энергии.

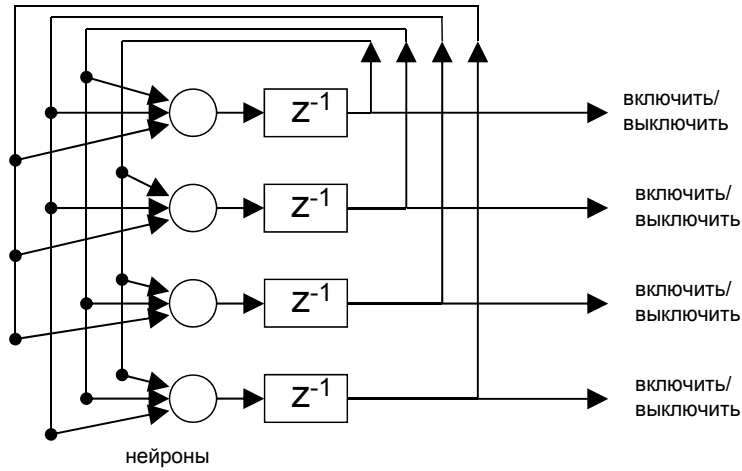


Рис. 1. Нахождение оптимумов сетью Хопфилда

ЛИТЕРАТУРА

1. Уоссерман Ф. Нейрокомпьютерная техника: Теория и практика. М.: Мир, 1992. С. 81–97.

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

ТЕСТИРОВАНИЕ ИНТЕРФЕЙСА ПРОГРАММИРОВАНИЯ ПРИКЛАДНЫХ ПРИЛОЖЕНИЙ БЫСТРЫХ ПАРАЛЛЕЛЬНЫХ АЛГОРИТМОВ АНАЛИЗА РЕЧИ

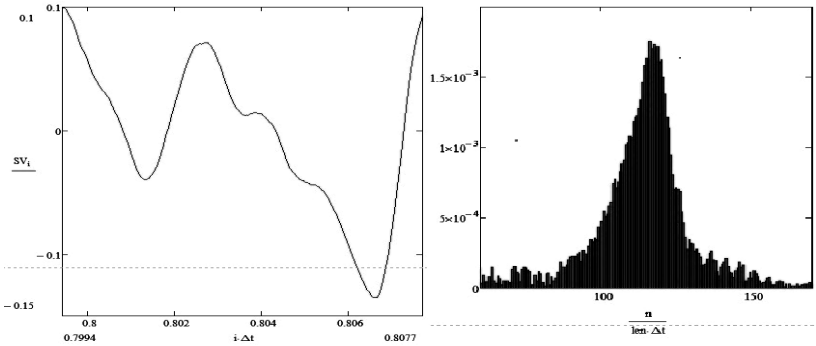
Д.А. Вольф, аспирант каф. КИБЭВС
г. Томск, ТУСУР, runsolar@mail.ru

Тестировался разработанный программный модуль для интерфейса программирования прикладных приложений быстрого параллельного алгоритма анализа речи.

В рамках настоящей работы на языке Си реализовался программный модуль быстрого численного метода анализа данных. Выбран алгоритм быстрого преобразования Фурье (БПФ) предложенный в [1], с учетом параллельного выполнения.

С помощью разработанного программного модуля доказывалось утверждение [2], что для взрослых мужчин Гауссово (или среднее) распределение основной гармоники варьируется около 130 Гц, а для женщин – 260 Гц.

На рис. 1, *а* представлен сигнал звука «У», записанный диктором (сигнал масштабирован до периода основного тона). Для определения гармоники основного тона записанный сигнал подавался на входы программного модуля, которые представляют собой 1024 параллельного входа X0…X1023. В процессе обработки данных организуются 1024 отдельных потока БПФ, реализованных на графической карте GeForce GTX 570.



а *б*

Рис. 1. Сигнал гласной буквы «у», произнесенный мужским диктором, – *а*. Частотный спектр гласной буквы «у» – *б*

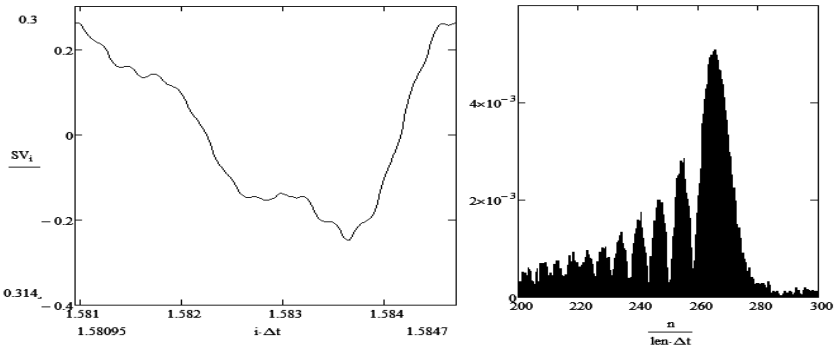
В результате обработки на выходах программного модуля Y0…Y1023 получен частотный ряд, где выход Y120 соответствует

частоте основного тона в 120 Гц, т.к. амплитуда на выходе максимальна (рис. 1, *б*), вывод – диктор мужчина (автор).

Из рис. 1, *а* несложно проверить, что частота основной гармоники для буквы «У», произнесенной диктором, равна: 1/(0,7994–0,8077) ≈ ≈ 120,5 Гц, т.е. частота гармоники основного тона для мужчины, рассчитанная при помощи программного модуля, примерно попадает в Гауссово распределение 130 Гц.

Число 1024 было выбрано неслучайно: во-первых, объединено Гауссово распределение для мужского и женского голоса, поэтому границы определены на диапазоне [60…380] Гц; во-вторых, для выбранного БПФ число отсчетов выбиралось равным степени двойки, а самое ближайшее от 380 – это 512; в-третьих, сохранялись требования теоремы Котельникова (Найквиста–Шеннона), поэтому оставалось выбрать только 2×512 = 1024 отсчета, а в пустые выборки были записаны нули.

На рис. 2, *а*, *б* представлены сигнал звука «у» и результат преобразования, соответствующий 266 Гц, записанный женским диктором (выход Y226).



а *б*

Рис. 2. Сигнал гласной буквы «у», произнесенный женским диктором – *а*. Частотный спектр гласной буквы «у» – *б*

Те же выкладки, что и для мужского диктора, применяем для женского: 1/(1,58095–1,5847) ≈ 266 Гц, т.е. частота гармоники основного тона для женщины, рассчитанная при помощи программного модуля, примерно попадает в Гауссово распределение 260 Гц.

Вывод. В результате тестирования разработанного программного модуля доказано утверждение, сформированное в работе [2]. Для быстрого нахождения частоты основного тона звука речи можно выби-

рать максимальное значение амплитуды на выходе программного модуля (интервал [60...380] Гц) т.е. выходы [Y60…Y380].

ЛИТЕРАТУРА

1. Кестер У. Проектирование систем цифровой и смешанной обработки сигналов // Техносфера. 2010. С. 108–110.

2. Раев А.Н., Матвеев Ю.Н., Голощапова Т.И. Анализ влияния состояния наркотического опьянения на характеристики голосов дикторов // Науч.-техн. вестник информационных технологий, механики и оптики. 2012. № 5. 81 с.

ИМПЕРИАЛИСТИЧЕСКИЙ АЛГОРИТМ

В.Г. Ясевич, студент каф. АОИ

г. Томск, ТУСУР, syasevich@mail.ru

Существует множество методов оптимизации, некоторые из которых являются компьютерной симуляцией естественных процессов. Здесь и далее под оптимизацией будем понимать процесс нахождения такого аргумента x функции $f(x)$, при котором удается достичь минимума или максимума этой функции на заданной области определения аргумента x.

Одним из таких методов является империалистический алгоритм, который основан на империалистическом соперничестве, в ходе которого сильные государства создавали свои колонии в отдельных частях света и боролись с другими государствами, отстаивая и захватывая другие земли, тем самым увеличивая или теряя собственную мощь.

Данный метод был предложен двумя иранскими учеными Esmaeil Atashpaz-Gargari и Caro Lucas в 2007 г. на конгрессе эволюционных вычислений (CEC 2007) Института инженеров по электротехнике и электронике (IEEE) [1].

Терминология

Страна – государство, участвующее в империалистическом соперничестве в качестве колонии или империалистического государства.

Империалист (империалистическое государство) – государство, которое борется с другими государствами за право управления колониями.

Колония – государство, которое попадает под влияние империалистических государств.

Империя – империалист и его колонии.

Сила (мощь) страны – выгодность положения относительно других стран. С математической точки зрения это означает близость к оптимальному значению функции.

Описание метода. Первым шагом метода является инициализация мира, которая заключается в случайной расстановке N_{pop} стран (т. е. в присвоении случайных значений аргумента x), выборе некоторого числа N_{imp} империалистов из этих стран и распределении оставшихся N_{col} стран среди империалистов в качестве их колоний. Распределяя колонии, на данном этапе учитывается сила империалиста – наибольшее число колоний будет у того империалиста, мощь которого выше, по сравнению с другими.

После этого происходит ассимиляция колоний, т.е. случайным образом каждая колония сближается со своим империалистом. При этом вводится случайное отклонение от направления движения колонии (рис. 1).

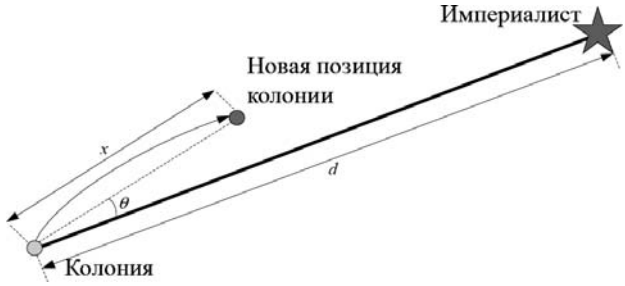


Рис. 1. Ассимиляция колонии

После ассимиляции может оказаться, что одна или несколько колоний империи могут обладать большей силой, чем империалист. В этом случае они меняются местами.

Империалистическое соперничество заключается в том, что, вычислив силу каждой империи (которая зависит от силы империалиста и в меньшей степени от силы колоний, ему принадлежащих), наиболее слабая империя теряет одну или несколько своих колоний, которые распределяются среди остальных империалистов, учитывая не только их силу, но и присутствие случайных факторов. Если империалист теряет все колонии империи, то он уничтожается.

Процесс ассимиляции и империалистического соперничества продолжается до тех пор, пока не останется всего одна империя. В идеале империалист и его колонии в этом случае будут находиться в одной точке – точке оптимума функции $f(x)$ [1] .

Программная реализация. Была разработана библиотека, реализующая данный метод. Псевдокод алгоритма выглядит следующим образом:

ВХОД $f(x)$; о.о. аргумента x; тип оптимизации (поиск минимума или максимума)

ВЫХОД вектор, являющийся точкой оптимального значения $f(x)$
НАЧАЛО
Инициализация империй (о.о. аргумента x)
ПОКА (есть империи, изменившие свое состояние)
Ассимиляция колоний (о.о. аргумента x)
Смена позиций империалиста и колонии с большей силой
ЕСЛИ (число империй > 1) ТО
Найти самую слабую империю
Выбрать слабую колонию и отдать другой империи
ЕСЛИ (у самой слабой империи нет колоний) ТО
Удалить самую слабую империю
КОНЕЦ ЕСЛИ
КОНЕЦ ЕСЛИ
КОНЕЦ ПОКА
КОНЕЦ

Одной из функций, которая была использована для тестирования алгоритма, была функция:

$$f(x, y) = x\sin(4x) + 1{,}1\, y\sin(2y). \quad (1)$$

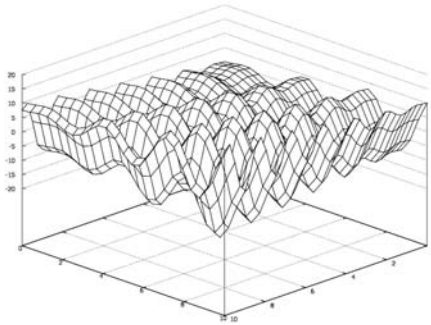


Рис. 2 . График функции $f(x, y)$

На интервале значений x и y, лежащих в пределе от 0 до 10, были найдены следующие оптимальные значения: для минимума – x = 9,039 и y = 8,668, при этом $f(x, y)$ = –18,55; для максимума – x = 9,824 и y = 10 при этом $f(x, y)$ = 19,86, что проиллюстрировано на рис. 2.

Заключение. Описанный метод был реализован в виде библиотеки на языке C#, которая позволяет решать задачу поиска оптимального значения функции $f(x)$ при заданной области определения аргумента x.

Сходимость данного метода была доказана несколькими тестами на примере различных функций. При этом для обеспечения необходимой точности результатов и быстродействия важным является правильный подбор таких параметров алгоритма, как N_{pop} и N_{imp}.

ЛИТЕРАТУРА

1. Esmaeil Atashpaz-Gargari, Caro Lucas. Imperialist Competitive Algorithm: An Algorithm for Optimization Inspired by Imperialistic Competition // IEEE Congress on Evolutionary Computation (CEC 2007). 2007. P. 4661–4667.

АНАЛИЗ СЕТЕВОГО ТРАФИКА НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

П.В. Жигулин, Д.Э. Подворчан, студенты

Научные руководители: Е.Ю. Костюченко, доцент, к.т.н., Е.М. Давыдова, доцент, к.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, каф. РЗИ, pashaworking@gmail.com

Проект ГПО КИБЭВС-1005 – «Анализ сетевого трафика на основе нейронных сетей»

На сегодняшний день все большую актуальность приобретают вопросы информационной безопасности, а также стабильности компьютерных систем. С развитием сетевых технологий также происходит и стремительное развитие угроз информационной безопасности. Естественно, что при таком темпе роста числа угроз требуется гибкая система защиты, которая будет способна самостоятельно адаптироваться под их новые проявления.

Целью нашего проекта является создание подобной системы, которая будет сканировать сетевой трафик на наличие угроз, используя для этого аппарат нейронных сетей.

На данный момент нами была разработана программа в математическом пакете MATLAB, которая использует для обучения нейронной сети базу данных, созданную университетом MIT [1]. Результаты её тестирования (способности распознавать представленные в базе атаки) представлены в таблице.

Результаты тестирования

Кол-во примеров в одном тесте	Ошибки первого рода, %	Ошибки второго рода, %
10000	7,5±3,9	0,034±0,024
7500	6,8±3,2	0,035±0,026
7000	5,5±2,6	0,036±0,025
6500	5,7±2,8	0,036±0,025
6000	6,0±2,9	0,047±0,032
5500	5,5±2,8	0,038±0,270
5000	5,9±3,0	0,049±0,036

По представленным результатам можно заключить, что нейронная сеть способна справляться с данной задачей с определенной степенью точности. Однако очевидно, что используемая база данных на сегодняшний день устарела, к тому же не все из признаков [2], по которым мы распознаем сетевые атаки,. могут быть полезны. Поэтому сейчас наша группа работает по двум направлениям: оценка информативности используемых признаков и создание собственной базы данных.

По первому направлению – оценке информативности – работает вторая часть нашей проектной группы. Для решения нашей задачи – сбор информации для собственной БД – сейчас ведется активная исследовательская работа в направлении ПО, способного сканировать исходящий трафик и выделять из него необходимые для нашей работы признаки.

После выполнения текущих задач планируется проведение серии тестов на новом наборе данных. Если будут получены удовлетворительные результаты, будет продолжена работа по оптимизации и внедрению программы. Так, возможна смена архитектуры нейронной сети, алгоритма её обучения а также возможен перенос программы на нативные языки для повышения скорости работы.

Заключение. В заключение, стоит отметить основное отличие действия нашей программы от антивирусов. В отличие от последних наша программа теоретически будет способна распознавать новые модификации сетевых атак, даже если они до этого не были известны и не были занесены в базу данных, т.к. нейронные сети на данный момент обладают достаточной гибкостью и способностью классифицировать данные.

ЛИТЕРАТУРА

1. База данных атак, составленная университетом MIT. 1999 [Электронный ресурс]. http://kdd.ics.uci.edu/databases/kddcup99/

2. Список признаков [Электронный ресурс]
http://kdd.ics.uci.edu/databases/kddcup99/task.html

СЕКЦИЯ 17

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

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

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ БЕСПРОВОДНЫХ КОММУНИКАЦИОННЫХ ПОДСИСТЕМ В СИСТЕМАХ ПРОМЫШЛЕННОЙ АВТОМАТИКИ

В.А. Афанасьев, аспирант каф. АСУ
Научный руководитель А.М. Кориков, д.т.н., проф., зав. каф. АСУ
г. Томск, ТУСУР, vladimir.afanasyev@mail.ru

Тематика применения беспроводных технологий передачи данных в АСУ ТП по-прежнему остается актуальной. Их применение дает целый ряд преимуществ, по большей части сводящихся к экономической эффективности такого решения, но сопряжено с рядом трудностей и не лишено недостатков. Не так давно беспроводные коммуникации в АСУ ТП использовались лишь в качестве подсистемы АСУ ТП, обеспечивающей передачу данных в нетребовательных к надежности и временным задержкам приложениях АСУ ТП, в случае если прокладка кабеля была крайне затруднена или вовсе невозможна, например в случае, если было необходимо обеспечить связь между географически удаленными объектами промышленного предприятия, охваченных одной АСУ.

В настоящее время в АСУП беспроводные решения применяются в основном на верхнем уровне (уровне предприятия), частично на диспетчерском уровне (где это не критично). На полевом уровне лишь для решения задач настройки и планового обслуживания оборудования, а также мониторинга ТП.

Интеграция беспроводных решений на полевом уровне в системы АСУ ТП затруднена в связи со сложностью обеспечения надежности и своевременности доставки сообщений. И если проблема обеспечения надежности так или иначе решается разработчиками базовых стандартов, через применение сложных видов модуляции (FHSS, DSSS, CSS, THSS), а также кодирования и шифрования в ряде случаев полностью снимает вопрос надежности и защиты от несанкционированного доступа, давно считавшийся слабым местом беспроводных технологий, то

проблема обеспечения своевременности доставки сообщений, а именно обеспечение должных временных характеристик функционирования беспроводной сети, в ряде беспроводных стандартов отходит на второй план, что в свою очередь и не позволяет их применять на полевом уровне АСУ ТП из-за более жестких требований, предъявляемых к временным характеристикам коммуникационных подсистем на нем.

Итак, камнем преткновения, мешающим повсеместному использованию беспроводных технологий на полевом уровне, является обеспечение надежности доставки сообщений и, что не менее важно, детерминизма и фиксированной величины задержки передачи данных от источника до получателя. Для применения беспроводных решений в качестве коммуникационных подсистем на полевом уровне АСУ ТП временные характеристики являются не менее значимым параметром, чем надежность передачи сообщений.

Исходя из важности своевременной доставки сообщений в спецификации ISA100.11a [1], выделяется шесть классов (Emergency action, Closed loop regulatory control, Closed loop supervisory control, Open loop control, Alerting, Logging and downloading/uploading) коммуникационных подсистем в системах АСУ ТП в целом. Данная классификация была разработана исходя из специфики практического применения коммуникационных подсистем в составе АСУ ТП. Согласно данной классификации важность своевременной доставки возрастает от 5-го класса к 0-му.

Например, известный стандарт ZigBee может применяться лишь при решении задач передачи данных в коммуникационных подсистемах АСУ ТП относящихся к 4–5-му классу. И это связано именно с тем, что данный стандарт беспроводной передачи данных не обеспечивает должных временных характеристик, в частности, приемлемой задержки доставки сообщения от источника до получателя («end-to-end»). На полевом уровне очень важно, чтобы коммуникационная подсистема имела минимальную величину задержки «end-to-end» с высокой степенью детерминизма. Это обеспечивает детерминизм трафика в сети и позволяет использовать такую сеть в системах реального времени (преобладающих на полевом уровне) при решении задач автоматического управления (1–2-й класс согласно ISA100.11a).

Задержка «end-to-end» в беспроводной сети определяется согласно формуле (1)

$$d_{end\text{-}end} = N[\, d_{trans} + d_{prop} + d_{queue} + d_{node} + d_{proc}], \qquad (1)$$

где N – количество роутеров в маршруте передачи сообщения +1; d_{trans} – задержка, вызванная скоростью передачи данных в линии связи, зависит лишь от количества данных (transmission delay); d_{prop} – задержка распространения сигнала (propagation delay); d_{proc} – задержка, воз-

никающая при обработке пакета сетевым узлом (проверка преамбулы, синхрослова, адреса, длины и структуры пакета, шифрование / дешифрование, кодирование / декодирование пакета в целом или его отдельных полей)) (processing delay); d_{queue} – задержка, возникающая при обработке очереди пакетов (queuing delay). При рассмотрении беспроводной сети d_{queue} часто не учитывают, считая, что в любой момент времени сетевой узел производит обработку лишь одного пакета, что зачастую не так. Пакеты могут поступать быстрее, чем роутер может их обработать. Роутер помещает их в очередь (временный буфер), пока не найдет время для их обработки и передачи. d_{queue} может меняться от пакета к пакету. Величина данной задержки зависит не столько от используемого протокола, а скорее от его программной реализации на конкретной платформе; d_{node} – задержка, возникающая при так называемой узловой обработке сигнала (nodal processing). Зачастую ее включают в processing delay. d_{node} возникает в сети с маршрутизацией пакетов и определяется временем, необходимым роутеру для определения адреса следующего сетевого узла в маршруте передачи принятого им пакета.

Данная формула дает лишь приблизительную оценку задержки end-to-end. На практике для каждого сетевого узла d_{trans}, d_{prop}, d_{proc}, d_{queue}, d_{node} различаются. Они в значительной мере зависят от таких параметров беспроводной сети, как топология, используемый базовый стандарт (PHY, MAC), протокол передачи данных, а также его реализации. В сетях с динамической маршрутизацией N изменяется скачкообразно, что очень негативно сказывается на временных характеристиках сети. Например, в меш-сети перестройка таблиц маршрутизации происходит постоянно. С одной стороны, эта их особенность позволяет оптимизировать маршруты передачи сообщений по какому-либо параметру, как следствие, повысить надежность передачи сообщений. С другой стороны, это приводит к появлению значительного джиттера, задержка end-to-end начинает скачкообразно изменяться.

Следовательно, с точки зрения обеспечения минимальной величины джиттера и самой задержки end-to-end, применение меш -сети является не целесообразным. Ведущие производители беспроводного оборудования и разработчики стандартов связи для них в случаях предъявления жестких требований к величине и джиттеру end-to-end рекомендуют использовать топологии типа звезда совместно с жестким временным разделением каналов (например, как в стандарте WirelessHART [2]). Однако использование топологии звезда и TDMA зачастую полностью не решает данную проблему. С ней необходимо начинать бороться еще при выборе/разработке протокола и, что не менее важно, при его программной реализации на конкретной аппарат-

ной платформе., так как плохая программная реализация может в конечном итоге свести все усилия на нет.

Заключение. d_{trans}, d_{prop}, d_{proc}, d_{queue}, d_{node} – это основные задержки, характеризующие работу беспроводной сети в штатном режиме (так как еще выделяется класс , возникающих при внештатных ситуациях: пропадание связи, поломка узлов, внесение новых узлов, процессы восстановления сети так и отдельных узлов после различных сбоев, плановая / внеплановая перестройка карты сети и таблиц маршрутизации). В общем случае в задержке end-to-end можно выделить чистое время (transmission delay), затрачиваемое на передачу пакета данных между двумя узлами, и так называемые издержки или накладные расходы на передачу данного пакета. Величина накладных расходов в значительной мере определяется программной реализацией.

С целью оценки временных характеристик предлагаемых беспроводных решений и возможности их улучшения был проведен следующий эксперимент. По результатам эксперимента были определены минимально достижимые величины накладных расходов и их джиттер. В качестве эталона использовался отладочный комплект TI TrxEB rev.1.5. с протоколом SimpliciTI в сетевой конфигурации точка–точка. Во второй части эксперимента производилась оценка тех же параметров для протокола передачи данных собственной разработки. Временные характеристики снимались при помощи осциллографа и программного продукта TI SmartRF Studio 7.

Замеры задержек производились при последовательной передаче фиксированного числа пакетов (от 10 до 5000) при изменении длины пакетов в пределах от 5 до 200 байт. Полученные результаты были сопоставлены. Усредненные величины накладных расходов для пакетов длиной в 5 байт расходятся на 72,171 (SimpliciTI) – 3,914 = 68,257% и для 200 байт 0,5335 (SimpliciTI) – 0,588 = –0,0545%. Исходя из полученных результатов, видно, что использование разработанного ПО, решающего ту же задачу, позволяет получить выигрыш в 68% при передаче коротких пакетов, что во временной области составляет 19,258 – 1,177 = 18,081 с. Однако получаемый выигрыш уменьшается при увеличении длины пакета и при достижении длины в 200 байт вовсе сводится на нет, что можно объяснить ростом времени, требующегося на обработку более большого пакета, и более высокой производительностью платформы, используемой TI (тактовая частота выше в 2 раза).

ЛИТЕРАТУРА

1. ISA100.11a:2008 Draft standard Wireless systems for industrial automation: Process control and related applications.

2. Deji Chen, Mark Nixon WirelessHART™ – Real-Time Mesh Network for Industrial Automation. N.Y.; Dordrecht Heidelberg; London: Springer, 2010. 276 c.

АВТОМАТИЧЕСКАЯ ФИЛЬТРАЦИЯ ИЗОБРАЖЕНИЯ, ОСНОВАННАЯ НА НОРМАЛЬНОМ РАСПРЕДЕЛЕНИИ

В.О. Чемезов, аспирант ИФПМ ТНЦ СО РАН, лаборатория полимерных композиционных материалов

Научный руководитель С.В. Панин, доцент, д.т.н.

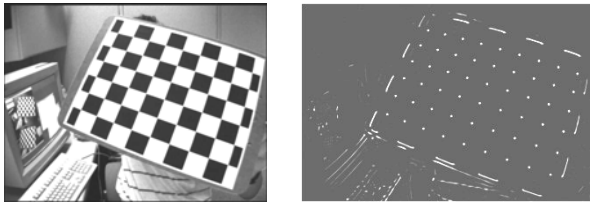
г. Томск, Институт физики прочности и материаловедения (ТНЦ СО РАН), vpointc@rambler.ru

Множество задач машинного зрения зависит от точности обнаружения пересечений клеток шахматной доски (узловых точек), так как данные пересечения обычно применяются для калибровки камер. Известные на данный момент методы либо требуют вмешательства оператора, либо имеют недостаточную точность. Ручная корректировка неприемлема для автоматизированных систем ввиду малой скорости действий оператора, а неверно определенные точки могут привести к некорректной обработке полученной информации.

В работе представлен устойчивый метод фильтрации результатов работы ChESS (Chess-board Extraction by Subtraction and Summation) алгоритма [1]. Данный метод фильтрации позволяет увеличить точность выделения узловых точек из множества полученных кандидатов.

Алгоритм фильтрации. Существует множество алгоритмов фильтрации результатов, имеющих явно выраженные особенности. Но они оценивают только поверхностные свойства представленной информации, такие как точки экстремума или принадлежность заданному интервалу значений.

Предлагаемый алгоритм основан на рассмотрении результатов работы ChESS алгоритма (отклик) (рис. 1) как распределения случайной величины. Было замечено, что локальные области имеют повторяющуюся структуру.

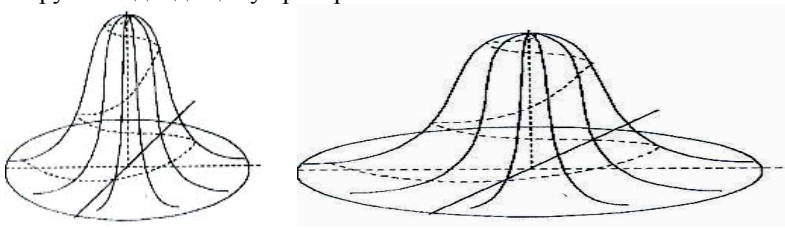


а *б*

Рис. 1. Результаты работы ChESS, *а* – исходное изображение; *б* – результат

С одной стороны, все области, содержащие узловые точки, имеют выраженный максимум и, отдаляясь от центра масс, имеют значения отклика, убывающие по нормальному закону распределения с близки-

ми по значению коэффициентами во всех направлениях (рис. 2, *а*). С другой стороны, области, не содержащие таких точек, могут иметь распределение по другим законам или по нормальному закону, но с различными коэффициентами в разных направлениях (рис. 2, *б*). Таким образом, задача сводится к расчету данных коэффициентов и их отбору по подходящему критерию.



а *б*

Рис. 2. Пример распределения в локальной области;
а – содержащей узловую точку; *б* – не содержащей узловую точку

Расчет коэффициентов. Для определения вида распределения необходимо знать его математическое ожидание, дисперсию и коэффициент асимметрии.

Идея расчета коэффициентов распределения основана на переходе от области координат с соответствующими им значениями к случайным величинам, где координата выступает в роли значения случайной величины, а значение по этой координате является вероятностью его появления. После такого перехода коэффициенты распределения легко считаются с помощью вычисления моментов случайных величин.

Для расчета потребуются три первых начальных момента и три первых центральных момента полученной случайной величины *X*, определенной в окрестности рассматриваемой узловой точки: *k*-м начальным моментом случайной величины *X*, где $k \in [1;3]$, называется величина $\upsilon_k = E\left[x^k\right]$, где $E[x] = \Sigma_x xp(x)$ – математическое ожидание дискретной случайной величины; *k*-м центральным моментом называется величина $\upsilon_k = E\left[Ix - E[x]I^k\right]$ [2].

Второй центральный момент отвечает за дисперсию распределения, а третий центральный момент – за коэффициент асимметрии.

Так как результатом работы ChESS алгоритма является область изображения, то для упрощения расчетов рассмотрим отдельно предложенное преобразование в горизонтальном и вертикальном направлениях. Результат расчета представлен на рис. 3.

Критерий отбора. Для окончательного выделения узловых точек на всем изображении осталось только отобрать точки, имеющие подходящие коэффициенты. Для этого необходимо в окрестности предполагаемой точки выбрать такую точку, которая имеет ближайшие к нулю горизонтальный и вертикальный коэффициенты асимметрии, а отношение вертикальной и горизонтальной дисперсий близко к единице. Результат представлен на рис. 4.

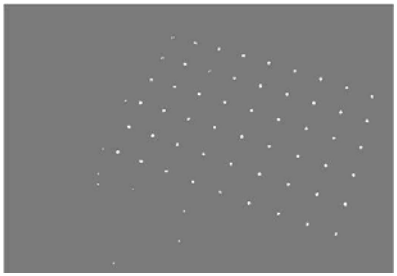


Рис. 3. Рассчитанные коэффициенты

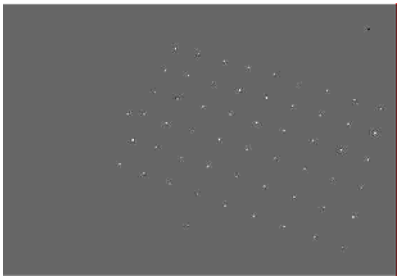


Рис. 4. Отобранные точки

Заключение. Предложенный алгоритм фильтрации может быть применен не только для обработки результатов работы алгоритмов аналогичных ChESS, но и для решения множества других задач, связанных с автоматической обработкой изображений, например поиск углов или оценка цветовых переходов.

ЛИТЕРАТУРА

1. Bennett S., Lasenby J. ChESS – Quick and Robust Detection of Chess-board Features: Пер. с англ. Cornell University Library. http://arxiv.org/abs/1301.5491.

2. Крамер Г. Математические методы статистики. М.: Мир, 1975. 648 с.

ПРОЕКТИРОВАНИЕ ИНТЕРВАЛЬНОЙ СИСТЕМЫ С ПОМОЩЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ RASILS

Т.А. Езангина, аспирант

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

г. Томск, НИ ТПУ, ИК, eza-tanya@yandex.ru

В реальных системах автоматического управления, как правило, не все параметры известны точно, поскольку они могут меняться в процессе эксплуатации системы по заранее неизвестным законам или быть недоступными для точного измерения. Если известны пределы изменения параметров или диапазоны их возможных значений, то та-

кие параметры можно отнести к классу интервально-неопределен-ных. Системы с подобными параметрами, в свою очередь, относятся к классу интервальных систем автоматического управления (ИСАУ).

Исследованию таких систем посвящено большое число публикаций отечественных и зарубежных ученых. При разработке ИСАУ может использоваться робастный подход, заключающийся в обеспечении устойчивости систем при любых значениях интервально-неопределенных параметров. Для анализа робастной устойчивости широко применяются частотные методы. При этом значительно меньше внимания уделяется использованию корневых и коэффициентных методов. В то же время робастное расширение коэффициентного подхода, основанное на свойствах интервального анализа, может быть достаточно эффективным, а в некоторых случаях и наилучшим для решения задач анализа и синтеза ИСАУ. При проектировании ИСАУ принято учитывать не только устойчивость, но и показатель колебательности.

Исследование сложных систем управления невозможно без использования современных информационных технологий. Поэтому представляет интерес разработка на основе коэффициентного метода отдельного модуля для анализа и синтеза ИСАУ.

Алгоритм анализа и синтеза. Пусть характеристический полином замкнутой интервальной системы автоматического управления имеет вид

$$D\left(s,\vec{k}\right)=B(s)F(s,\vec{k})+A(s)=\sum_{k=0}^{z} d_k(\vec{k})s^k. \qquad (1)$$

На основе теоритических сведений [2] разработаны алгоритмы (рис. 1).

Полное описание алгоритма приведено в работе [2].

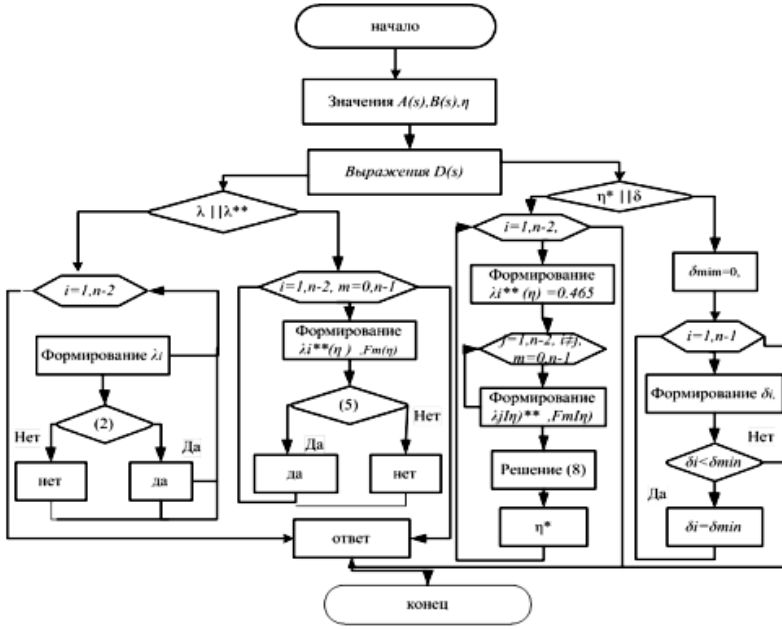
Примеры

Пусть имеется замкнутая интервальная система, содержащая ПИ-регулятор с передаточной функцией $Wp(s)=k_0+k_1 s/s$, где $k_0=3, k_1=3{,}6$ и объект управления с передаточной функцией

$W(s)=b_0/a_3 s^3+a_2 s^2+a_1 s^1+a_0$, $a_2\in[2,6;3]$; $a_1\in[0{,}8;0{,}9]$; $a_0\in[0,5;1]$.

Задано допустимое значение степени устойчивости интервальной системы η=0,3. Требуется провести анализ и синтез интервальной системы.

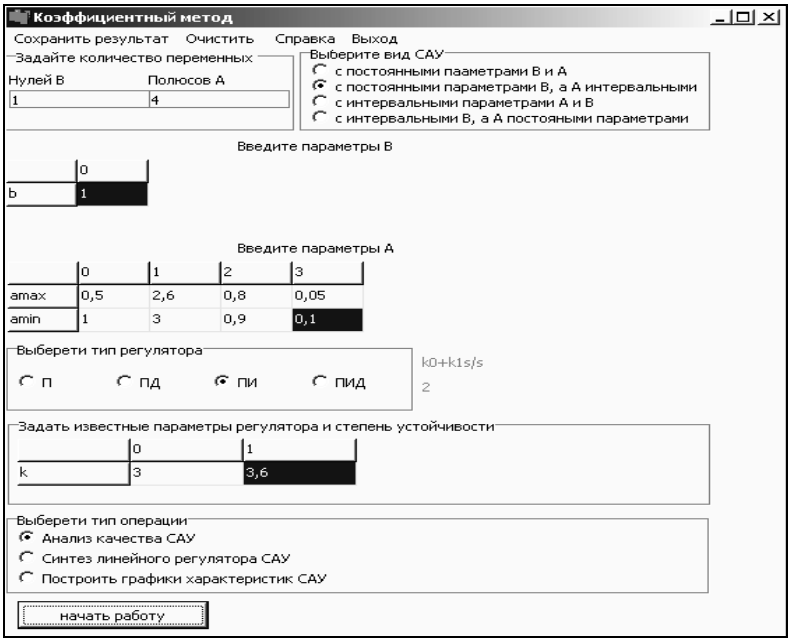
В результате анализа интервальной системы найдены показатели качества: $\eta^*=0{,}3258$, $\varphi=79°$. В результате синтеза робастного регулятора найдены следующие параметры: $\eta^*=0{,}475$, $k_1=1{,}83$, $k_2=3{,}69$.



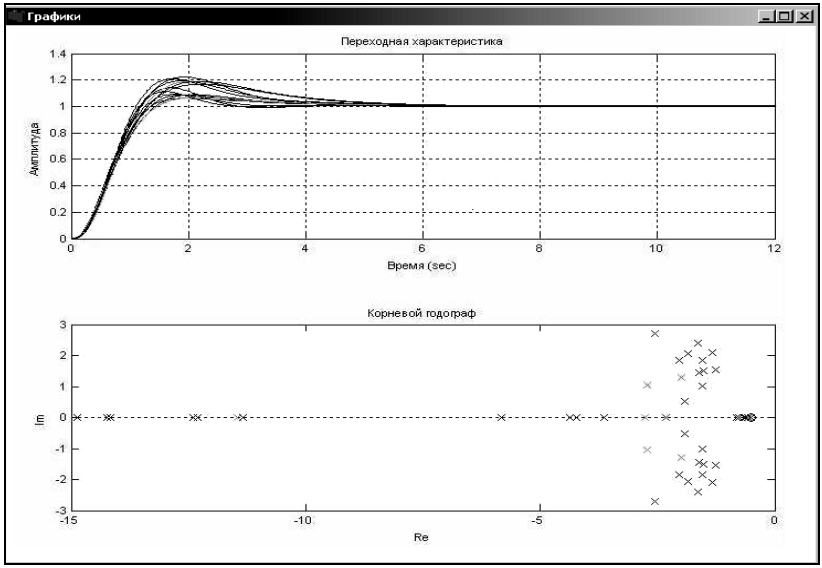
а

б

Рис. 1. Блок-схема алгоритма: *а* – анализ показателей качества; *б* – синтез робастных регуляторов интервальной системы



а



б

Рис. 2. Главное окно программного комплекса – *а*; переходные процессы – *б*

Заключение. На основе коэффициентных показателей качества и достаточных условий устойчивости разработан программный комплекс, позволяющий анализировать качества интервальной системы и синтезировать для них робастные регуляторы. Работоспособность данного программного комплекса подтверждена численными примерами.

ЛИТЕРАТУРА

1. Петров Б.Н., Соколов Н.И., Липатов А.В. и др. Системы автоматического управления объектами с переменными параметрами: Инженерные методы анализа и синтеза. М.: Машиностроение, 1986. 256 с.

2. Гайворонский С.А. Методика выбора параметров регулятора для интервальной системы автоматического управления / С.А. Гайворонский, Т.А. Езангина // Вестник науки Сибири. 2012. № 3(4). С. 143–147.

РАЗРАБОТКА КОМПЛЕКСА ЛАБОРАТОРНЫХ РАБОТ НА ПЛИС

Е.А. Федоскин, П.А. Молчанов, С.И. Анищенко, П.Г. Попенко, студенты

Научный руководитель О.В. Пехов, инженер

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

Проект ГПО 1201 – «Синтез логических схем»

Целью работы является создание комплекса лабораторных работ по курсу «Синтез электронных схем на базе ПЛИС». Он включает в себя: лабораторный программно-аппаратный комплекс, методический материал по выполнению лабораторных работ и программное обеспечение для ознакомления студентов с основами языка описания электронных схем. План лабораторных работ включает в себя разработку проектов в программируемых средах «Active-HDL», «Quartus II» и «ISE design suite». Прежде чем приступить к описанию комплекса лабораторных работ, необходимо сказать, в чем заключаются преимущества в использовании HDL по сравнению с традиционными средствами разработки электронных схем.

Преимущества использования языка описанием схем. Традиционно цифровые цепи, основанные на схемах и триггерах, были разработаны с Булевыми уравнениями. Эта методика требует записи одного уравнения для каждого информационного входа каждого триггера, и в некоторых случаях одно уравнение может представлять много схем. Это делает Булевы уравнения непрактичными для больших проектов, содержащих множество или большое количество триггеров [1].

Главные недостатки традиционных методов проектирования – это трансляция описания проекта к логическим уравнениям, что значи-

тельно упрощается аппаратными языками описаний оборудования (HDLs). С HDL можно начинать описывать спецификацию проекта, не имея Булевы уравнения. Проектировщики нуждаются в едином языке, который упростил бы документацию и стандартизацию передачи данных между фазами проекта [2]. VHDL – это большой шаг вперед к такому языку описаний.

В ходе работы над проектом был разработан комплекс лабораторных работ, охватывающий все этапы работы с ПЛИС.

Лабораторная работа №1 «Проектирование и моделирование электронных схем».

В данной работе рассмотрен пакетный интерфейс «Active-HDL». В ходе лабораторной работы студенты научатся:

– работать в программной среде «Active-HDL»;

– моделировать «vhdl»-проекты в схемном редакторе (BDE);

– программировать проекты в текстовом редакторе (HDE);

– тестировать работоспособность проектов с помощью временных диаграмм.

Лабораторная работа №2 «Создание испытательного стенда».

В данной работе рассматриваются особенности и возможности испытательных стендов (TestBench) в среде «Active-HDL». В ходе лабораторной работы студенты научатся:

– создавать испытательные стенды (TestBench);

– программировать основные тестовые процессы в «TestBench»;

– анализировать результаты тестирования проектов.

Лабораторная работа №3 «Создание электронных часов с динамической индикацией».

В данной работе рассматривается разработка проекта электронных часов с динамической индикацией. Проект представляет собой сложную схему, при проектировании которой необходимо использовать полученные ранее знания в разработке проектов в среде «Active-HDL». В ходе лабораторной работы студенты:

– ознакомятся с процессом синтеза сложных электронных схем;

– закрепят знания в разработке проектов в среде «Active-HDL».

Лабораторная работа №4 «Синтез электронных схем в среде «Quartus II» и «ISE design suite».

В ходе лабораторной работы студенты научатся:

– работать в программной среде «Active-HDL»;

– программировать «vhdl»-проекты;

– реализовывать проекты на кристаллах ПЛИС ведущих фирм.

Для ознакомления студента с новыми средствами разработки необходимо иметь программно-аппаратный комплекс, который позволял бы реализовывать операции, начиная от разработки и моделирования

электронных схем и заканчивая реализацией схемы в кристалле логического устройства. Такой комплекс должен иметь:

– набор примитивов, на которых студент мог бы выполнять различные задания;

– гибкую структуру для возможности переконфигурирования реализуемого устройства;

– возможность добавления новых примитивов;

– программный комплекс разработки получения и загрузки исполняемого кода.

Структура комплекса. Лабораторный комплекс – это персональный компьютер, с установленной операционной системой Windows. На этом компьютере установлен программный комплекс проектирования логических схем, который включает в себя:

– редактор представления электронных схем в УГО;

– тестовый редактор для описания логических схем на языке VHDL;

– компилятор проекта;

– симулятор проекта и отдельных его компонент;

– линковщик, который связывает все откомпилированные модули в единый код для последующей его загрузки в кристалл;

– загрузчик, который программирует ПЛИС исполняемым кодом.

Аппаратный комплекс состоит из платы, на которой размещен блок стабилизации напряжения питания и программируемая логическая схема.

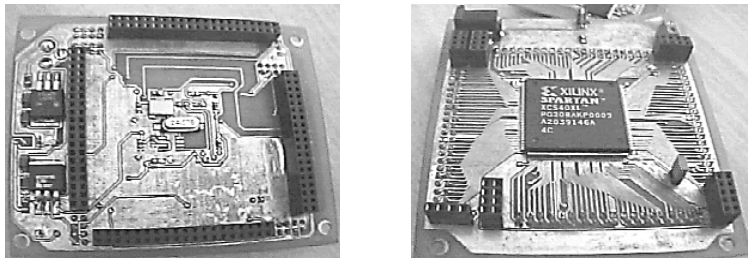


Рис. 1. Плата аппаратного комплекса (верхняя и нижняя сторона)

С верхней стороны слева можно увидеть размещение компонент, слева – стабилизаторы питания, по бокам разъемы ввода/вывода, в центре блок фильтрации и генератор тактовой частоты. С нижней стороны в центре находится ПЛИС фирмы Xilinx – Spartan XCS40XL. По углам платы видны разъемы шин питания (GND, +5V,+3.3V), разъем входа для внешнего генератора тактовой частоты, разъем портов загрузки исполнительного кода. Этот разъем предназначен для подклю-

чения кабеля к персональному компьютеру, посредством которого осуществляется загрузка исполняемого кода в ПЛИС.

Для гибкого взаимодействия примитивов с ПЛИС все её вводы выведены на внешние разъемы ввода-вывода. Возможно использование следующих примитивов: набор семисегментных индикаторов / светодиодный модуль, клавиатурный модуль, модуль памяти DRAM/SDRAM, модуль ЦАП / АЦП, модуль усилителей для управления двигателями постоянного тока / шаговыми двигателями, микропроцессорный модуль.

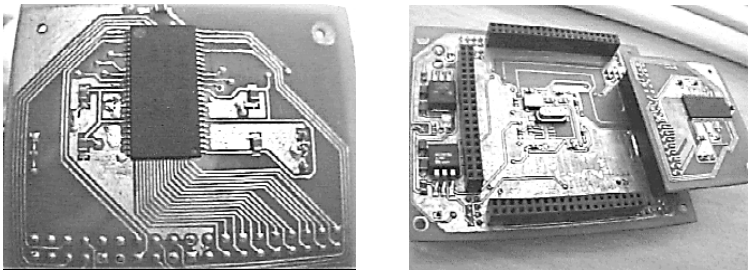


Рис. 2. Макет примитива памяти DRAM (верхняя сторона) и пример соединения основного модуля и примитива памяти

В описании лабораторного комплекса присутствуют решения различного рода задач, таких как выбор языка программирования, выбор программного продукта, разработка и реализация электронных схем. Но первоочередной задачей является обучить студента и позволить внедрить усвоенные знания о работающем комплексе, реализовать себя.

ЛИТЕРАТУРА

1. Андреев А.Е. Реализация концепции учебного процессора с помощью лабораторных стендов на ПЛИС. 2005. № 4. С. 70–71.

2. Угрюмов Е.П. Цифровая схемотехника, СПб.: БХВ-Петербург, 2005. 800 с.

ЭФФЕКТИВНАЯ МОДЕЛЬ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ НА ПРИМЕРЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ г. ТОМСК

Р.Р. Галин, аспирант

Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, ppos.grr@gmail.com

Вопрос повышения качества предоставления государственных и муниципальных услуг является актуальным и сегодня, так как он напрямую зависит от эффективности государственного управления.

В России методы и критерии оценки эффективности государственного управления определились с 2003 г., с момента проведения административных реформ. Административные реформы представляли собой внесение изменений, направленных на эффективность развития с точки зрения экономического подхода, в государственную службу, в службу местного самоуправления, а также бюджетную реформу [1, 2]. И данный подход был абсолютно новым и не однозначно подходящим для России. Утвержденные показатели эффективности характеризуют уровень социально-экономического развития регионов, но мало отражают управленческую деятельность. Социально-экономические показатели отдельно взятых регионов могут быть противоположны в силу их экономического развития, и тем самым применение «официальных» критерий оценок может отображать действительную картину развития отдельно взятого региона [3].

Государственные и муниципальные услуги в сфере молодежной политики. Город Томск – это образовательный центр Сибири с населением более 500 тыс. чел., где молодежь занимает пятую часть населения. Следовательно, реализация молодежной политики – одно из приоритетных направлений развития города. Для города важно формирование приоритетов и мер, направленных на создание условий и возможностей для успешной социализации и эффективной самореализации молодежи.

Проблема реализации социально-экономической стратегий развития молодежного сектора граждан заключается в информировании, которое позволит гражданам знать о имеющихся программах, льготах, возможностях и услугах, предназначенных для населения в рамках реализации молодежной политики и достижения одной из основных целей государственного управления – повышения уровня качества жизни человека.

Рассмотрим модель взаимодействия ОГВ в сфере молодежной политики с учреждениями, непосредственно связанными с категорией граждан «молодежь». Суть данного взаимодействия заключается в том, что необходимо консолидировать первичную информацию о молодежи и вести уведомление о возможных программах по поддержке населения. Разберем на примере Департамента записи гражданского состояния Томской области, отдел ЗАГС г. Томска и Томского района (далее – отдел). Отдел фиксирует акты гражданского состояния – действия граждан или события, влияющие на возникновение, изменение или прекращение прав и обязанностей, а также характеризующие правовое состояние граждан.

Государственной регистрации подлежат акты гражданского состояния: рождение, заключение брака, расторжение брака, усыновле-

ние (удочерение), установление отцовства, перемена имени и смерть [5].

Опираясь на предложенную модель, органы исполнительной власти в сфере молодежной политики смогут отслеживать социальную активность граждан, повышение качества услуг, повышение качества межведомственного взаимодействия. Основным достижением будет являться решение вопроса информирования граждан о государственной поддержке, что отразит эффективность государственного управления качеством жизни в рамках системы менеджмента качества. Тем самым миссия и цели органов государственной власти, которые перед ними поставлены, будут оправданы и будут соответствовать объективным потребностям общества.

Теоретически процедура оценки эффективности (качества) управления отличается от реализации контрольных функций. Если содержанием контроля является соотнесение результата исполнения решения намеченным целям, то в процессе оценивания главное – показать, насколько решение соответствовало миссии, функциям и целям данного государственного органа, а также интересам государства и общества [6]. Однако нельзя исключать тот факт, что подобные оценки эффективности являются прецедентами реорганизации, упразднения и дополнительные проверки ОГВ, что определяет настороженное отношение чиновников всех уровней к введению практики оценки их деятельности.

И, безусловно, управление является, прежде всего, функцией органов исполнительной власти, но и воздействие органов законодательной и судебной власти на ход социально-экономических процессов требует определенного содействия в принятии ряда решений, позволяющих внедрения новых методик и критерий оценки эффективности исполнительных административных ведомств. Это в свою очередь предполагает определение и обеспечение социальных стандартов для субъектов РФ и муниципальных образований, входящих в их состав.

Вывод. Для стран, с развитой рыночной экономикой, с эффективными механизмами и моделями управления социально-экономических систем задачи повышения эффективности государственного управления приобретают все большую значимость. Фактом остается то, что универсальных моделей, оптимальных для использования всеми странами, не существует. Каждое государство должно вырабатывать собственную модель оценки эффективности управления социально-экономическим развитием. Для России необходимо разрабатывать и внедрять методики и критерии эффективности государственного управления для каждого региона, учитывая влияние условий и факторов на социально-экономические показатели этого региона.

Рассмотрев вопрос повышения качества предоставления государственных и муниципальных услуг на примере муниципального образования город Томск в области молодежной политики, в первую очередь необходимо изменить модель взаимодействия органов государственной власти с населением, попадающим в категорию «молодежь». Исходя из предложенной модели, рассмотреть улучшение качества жизни населения и определить комплекс рекомендаций по созданию методики оценки эффективности государственного управления качеством жизни.

ЛИТЕРАТУРА

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

2. Положихина М.А. Оценка качества и эффективности государственного управления: методы и критерии [Электронный ресурс]. Режим доступа: http://viperson.ru

3. Дробышева В.В. Методы и проблемы оценки эффективности государственного управления в системе менеджмента качества жизни. Тамбов, 2009.

4. Загоруйко А.Е. Электронные административные регламенты. Принципы и аспекты реализации в документационном обеспечении управления. М., 2007 [Электронный ресурс]. Режим доступа: http://www.gisa.ru.

5. Положение о Департаменте записи актов гражданского состояния Томской области от 22.10.2012 № 133.

6. Бажин И. Методика оценки деятельности органов исполнительной власти // Государственная служба. М., 2009. №1. С. 77–82.

7. Балацкий Е. Новые аналитические инструменты совершенствования государственной административной системы // Проблемы теории и практики управления: Международный журнал. М., 2004. №5. С. 34–39.

8. Указ Президента РФ от 28.06.2007 № 825 (ред. от 28.04.2008) «Об оценке эффективности органов исполнительной власти субъектов РФ».

9. Указ Президента РФ от 28.04.2008 № 607 «Об оценке эффективности деятельности органов местного самоуправления городских округов и муниципальных районов».

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ИДЕНТИФИКАЦИИ ПОЛА АВТОРА ПО ТЕКСТУ

Р.А. Гурьев, студент

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

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

Век рассвета анонимности в Интернете приходит к концу, по крайне мере для большинства стран, однако на смену обычному Интернету приходит так называемый «deep web», в котором сейчас царит

полная анархия. В связи с этим проблема идентификации автора анонимного сообщения является довольно актуальной.

Целью данной работы является создание системы, позволяющей идентифицировать пол автора по тексту. В рамках этой цели требуется автоматизировать сбор материала для исследований, разработать средства для обработки, анализа и классификации текста на основе таких характеристик, как униграммы, биграммы и триграммы символов, частотные словари, морфологические характеристики слов и др., показавшие свою состоятельность при решении смежной задачи – идентификации автора текста [1]

Для решения поставленных задач была разработана система, структура которой представлена на рис. 1.

Рис. 1. Структурная схема системы

Собранная к настоящему моменту база данных содержит около 500 тысяч коротких сообщений (доля сообщений, написанных мужчинами, – 65, женщинами – 20, анонимными авторами – 15%). Источниками сообщений стали популярные интернет-ресурсы, такие как twitter.com, vk.com и др. Общий объем базы данных – более 100 Мб, длины сообщений варьируются от 5 до 864, средняя длина сообщения – 162 символа. Тексты подобраны так, что затрагивают обсуждения на различные темы: бизнес, автомобильная, кулинария и т.д.

Система состоит из группы модулей и веб-интерфейса (рис. 2), написанных на языке программирования PHP, а также классификаторов, написанных на языке Python. Посредством веб-интерфейса конфи-

гурируется режим работы модулей. Модуль парсинга позволяет в автоматическом режиме собирать сообщения, которые в дальнейшем используются для анализа, обучения и классификации. Модуль выборок позволяет сделать выборку из базы сообщений по таким критериям, как длина сообщений, пол автора и т.д., затем сохраняет её в отдельную базу выборок для последующих манипуляций. Модуль конвертации извлекает из выборки признаки текста (метаданные) и сохраняет их в базу метаданных. Для исследования текста был реализован модуль статистического анализа, включающий в себя такие функции, как расчет коэффициента корреляции Спирмена, определение доверительного интервала и U-критерий Манна–Уитни. С помощью коэффициента корреляции Спирмена можно определить, насколько схожи две группы метаданных, U-критерий Манна–Уитни позволяет определять, насколько эти же группы различны. Статистические тесты помогают проверить, возможно ли на данной выборке произвести классификацию и на основе каких признаков это будет лучше всего сделать. Классификаторы используют метаданные и набор признаков для обучения и классификации. На данный момент реализовано три классификатора: методы опорных векторов, метод релевантных векторов и наивный байесовский классификатор. Результат их работы передаётся в модуль принятия решения, который на основе этих данных выдает предположение о гендерной принадлежности автора.

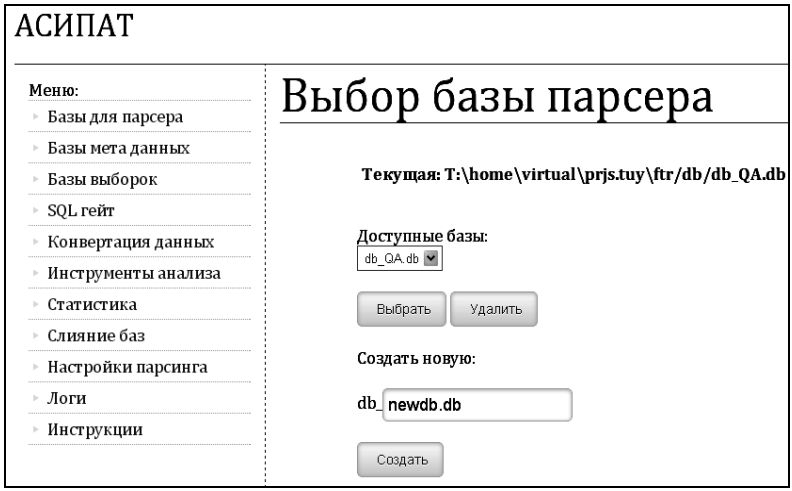


Рис. 2. Веб-интерфейс системы

Далее будут представлены полные результаты исследования.

ЛИТЕРАТУРА

1. Романов А.С. Идентификация автора текста с помощью аппарата опорных векторов / А.С. Романов, Р.В. Мещеряков // Компьютерная лингвистика и интеллектуальные технологии: матер. ежегод. междунар. конф. «Диалог 2009» (Бекасово, 27–31 мая 2009 г.). М.: РГГУ, 2009. Вып. 8(15). С. 432–437.

2. Гмурман В.Е. Теория вероятностей и математическая статистика: учеб. пособие для вузов. 9-е изд. М.: Высшая школа, 2003. 634 с.

3. Гублер Е.В., Генкин А.А. Применение непараметрических критериев статистики в медико-биологических исследованиях. М.: Высш. шк., 1973. 160 с.

РАЗМЕЩЕНИЕ ПОЛЮСОВ СИСТЕМЫ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ МЕТОДОМ ДЕЛЕНИЯ ПОЛИНОМОВ

И.В. Хожаев

Научный руководитель С.А. Гайворонский, доцент, к.т.н.
г. Томск, НИ ТПУ, khozhaev.i@gmail.com

Качество работы любой системы автоматического управления определяется положением ее полюсов, однако для обеспечения должных динамических характеристик системы достаточно жестко задать положение лишь некоторых из них – так называемых доминирующих полюсов. Для остальных полюсов системы требуется задать некоторую область расположения, удаленную от доминирующих полюсов.

В данной работе рассматривается метод расположения полюсов линейной стационарной системы путем разложения характеристического многочлена на два полинома, один из которых обеспечивает расположение доминирующих полюсов системы, а другой – расположение остальных полюсов.

Пусть характеристический полином имеет вид

$$D(s)=\sum_{i=0}^{n} a_i \cdot s^i \ , \qquad (1)$$

где a_i – коэффициенты характеристического полинома, каждый из которых однозначно определяется настройками регуляторов системы и параметрами объекта управления, n – порядок характеристического полинома.

Очевидно, что система имеет n полюсов. Обозначим полином, обеспечивающий расположение доминирующего корня как $A(s)$; результат деления исходного характеристического полинома (1) на $A(s)$ обозначим как $B(s)$; остаток от такого деления обозначим как R.

Таким образом, характеристическое уравнение можно представить в виде

$$A(s)\cdot B(s)+R=0\,. \qquad (2)$$

Исходя из всего сказанного, основную задачу данной работы определим следующим образом: необходимо разработать метод, позволяющий выделять в характеристическом полиноме множитель, обеспечивающий необходимое расположение доминирующего полюса системы. Кроме того, разрабатываемый метод должен позволять накладывать ограничения на свободные полюсы системы, а также синтезировать соответствующие настройки регуляторов.

Вывод основных соотношений. Для решения поставленной задачи необходимо, в первую очередь, определить общий вид полиномов $A(s)$, $B(s)$ и остатка R.

Для случая, рассматриваемого в данной работе, очевидно:

$$A(s)=s-s_0\,,$$

где s_0 – доминирующий полюс системы.

Коэффициенты полинома (1) и $B(s)$ связаны формулой:

$$b_i=a_{i+1}+a_{i+2}\cdot s_0;i\in[0;n-1]\,. \qquad (3)$$

Очевидно, что произведение полиномов $A(s)$ и $B(s)$, обеспечивающее желаемые свойства системы, должно быть полностью эквивалентно исходному характеристическому полиному. Таким образом, синтезируя настройки регуляторов, необходимо стремиться к равенству R=0.

Для выполнения этого условия выведем общий вид остатка R:

$$R=\sum_{i=0}^{m}a_i\cdot s_0^i=D(s_0)\,.$$

Согласно выражению (2) полином $B(s)$ определяет расположение свободных полюсов системы на комплексной плоскости. Сместим его таким образом, чтобы все его корни оказывались левее некоторой точки $(-\delta,0)$, лежащей на действительной оси комплексной плоскости.

Для этого построим D-разбиение по одному параметру. Чтобы получить уравнение кривой D-разбиения из полинома $B(s)$, выполним подстановку $s\to\delta+i\cdot\omega$; $(\delta<0)$ и выразим из полученного полинома параметр регулятора, в плоскости которого проводится разбиение.

Таким образом, на вещественной оси комплексной плоскости получим отрезок устойчивости полинома $B(s)$, однако любое значение выбираемого параметра, кроме собственно устойчивости $B(s)$, гарантирует также и расположение всех свободных полюсов системы левее некоторой прямой, что полностью соответствует поставленной задаче.

Для расположения доминирующего полюса системы необходимо, исходя из равенства R нулю, найти значения остальных параметров регулятора.

Пример

Пусть система состоит из объекта управления с передаточной функцией W_{oy}:

$$W_{oy}(s)=\frac{1}{1{,}382\cdot 10^{-5}\cdot s^4+2{,}15\cdot 10^{-3}+0{,}083\cdot s^2+1{,}476\cdot s+11{,}226}$$

и ПИ-регулятора $W_p(s)=\dfrac{K_1+K_2\cdot s}{s}$, охваченных единичной обратной связью. Необходимо поместить доминирующий полюс замкнутой системы в точку (–2; 0) комплексной плоскости, а свободные полюса – левее точки (–8; 0). Характеристический полином замкнутой системы имеет вид

$$D(s)=1{,}382\cdot 10^{-5}\cdot s^5+2{,}15\cdot 10^{-3}\cdot s^4+0{,}083\cdot s^3+1{,}476\cdot s^2+(K_2+11{,}226)\cdot s+K_1.$$

Для размещения свободных полюсов вычислим коэффициенты полинома $B(s)$:

$$B(s)=0{,}00215\cdot s^3+0{,}0789\cdot s^2+1{,}318\cdot s+K_2+8{,}589$$

и построим для него D-разбиение по параметру K_2 (рис. 1).

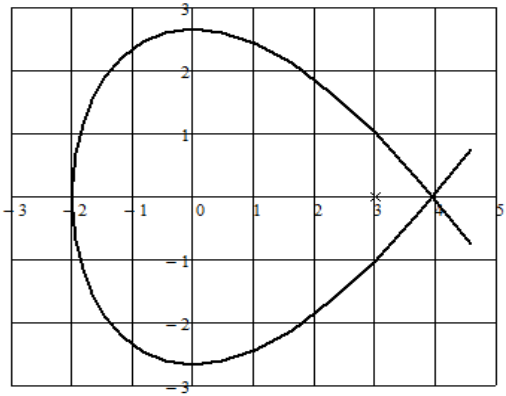


Рис. 1. Кривая D-разбиения в плоскости параметра K_2

Выберем K_2 = 3, что обеспечивает желаемое расположение свободных полюсов системы. Далее, исходя из равенства остатка $R(K_1,K_2,s_0)$ нулю, рассчитаем значение K_1 = 23,179. Для проверки полученного решения найдены полюса системы с синтезированным регулятором: –2; $-25{,}5026$; $-108{,}2028$; $-9{,}925\pm i\cdot 14{,}3377$. Таким

образом, применение предложенного подхода позволило разместить полюса системы желаемым образом.

ЛИТЕРАТУРА

1. Скворцов Л.М. Синтез линейных систем методом полиномиальных уравнений // Изв. АН СССР. Техн. кибернетика. 1991. № 6. С. 54–59.

2. Скворцов Л.М. Интерполяционный метод решения задачи назначения доминирующих полюсов при синтезе одномерных регуляторов // Изв. РАН. Теория и системы управления. 1996. №4. С. 10–13.

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК УЛЬТРАЗВУКОВОГО ДАТЧИКА LEGO MINDSTORMS

Е.С. Барисенок, О.С. Марченко, Д.А. Фаррахова, студенты

Научный руководитель О.В. Пехов, инженер

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

Проект ГПО 1202 – «Робототехника»

Lego Mindstorms – специальная серия конструкторов Lego, предназначенная для создания программируемых роботов. В ее состав входит набор обычных деталей Lego, двигатели и программируемый блок, а также специальные сенсоры (расстояния, освещенности, касания).

Выяснилось, что информация о датчиках, содержащаяся в руководстве пользователя [1] и расположенная на официальном сайте Lego Mindstorms [2], является неполной для практического использования набора. В связи с этим возникают такие проблемы, как:

– точность измерения;

– определение границы области видимости датчика;

– быстродействие датчика.

В результате анализа возникших проблем было решено провести практические исследования сенсоров на примере ультразвукового датчика и сравнить имеющуюся информацию с результатами проведенных тестов.

Внешний вид ультразвукового датчика показан на рис. 1.

Рис. 1. Внешний вид ультразвукового датчика набора Lego Mindstorms

Датчик излучает короткие ультразвуковые импульсы в направлении объекта обнаружения, которые, отразившись от поверхности объекта, возвращаются обратно. Время между моментом посылки сигнала и моментом приема отраженного сигнала соответствует расстоянию до объекта. Принцип работы ультразвукового датчика показан на рис. 2.

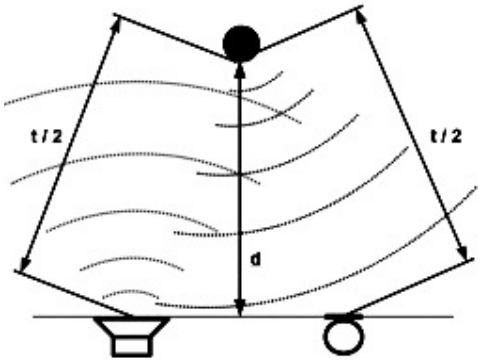


Рис. 2. Принцип работы ультразвукового датчика

Было решено, что практические исследования будут проходить в два основных этапа:

1. Статические тесты.
2. Динамические тесты.

Для проведения тестовых испытаний разработано универсальное программное обеспечение.

Статические испытания разделены на три серии: определение области видимости, исследование влияния размера и формы предмета на измерения и определение расстояния до предмета в условиях различных сред и в зависимости от материала предмета.

Для правильности алгоритма работы с ультразвуковым датчиком важно знать область видимости датчика, т.е. область, за пределами которой датчик работает с ошибкой. Для определения области видимости необходимо определить максимальное и минимальное расстояния до предмета, минимальную и максимальную высоту расположения предмета, а также угол расхождения.

При выполнении роботом, на котором установлен ультразвуковой датчик, различных заданий важно знать, какую минимальную ширину должен иметь предмет, до которого измеряется расстояние, а также необходимо знать его минимальную высоту.

На точность работы датчика влияют условия среды, т.к. на время прохождения звуковой волны могут оказывать влияние температура, давление, влажность, а также воздушные потоки. Также на работу датчика могут влиять наличие источников повышенного шума в пределах радиуса действия датчика и работа в условиях сильного дождя или

снегопада. Поэтому было принято решение провести тестовые испытания в моделированных условиях различных сред.

Также важны материал и форма предмета. Потому что некоторые материалы поглощают звуковые волны, а объекты определенной формы отражают звук в сторону от датчиков.

К динамическим испытаниям относится определение быстродействия датчика. Быстродействие – это параметр датчика, позволяющий оценить, как выходная величина следует во времени за изменениями измеряемой величины. Быстродействие, таким образом, связано со временем, необходимым для того, чтобы вклад переходного режима в выходную величину стал пренебрежимо мал в условиях требуемой точности. Однако характер переходного режима зависит только от свойств элементов измерительной системы, непосредственно связанных с датчиком.

В современном мире ультразвуковые датчики получают все большее распространение. Они применяются во многих отраслях промышленности и науки. Проведение тестовых испытаний с ультразвуковым датчиком из набора Lego Mindstorms позволяет изучить особенности работы и выявить недочеты таких датчиков. Эти знания помогут более эффективной эксплуатации оборудования с подобными датчиками.

ЛИТЕРАТУРА

1. Коллектив Lego Mindstorms: руководство пользователя. 2006. 76 с.

2. Официальный сайт Lego Mindstorms. Электронный ресурс: http://mindstorms.lego.com/en-us/Default.aspx.

МОДЕРНИЗАЦИЯ ОПЕРАЦИОННОЙ СИСТЕМЫ МИКРОКОНТРОЛЛЕРОВ

Я.Е. Мещеряков, студент

Научные руководители: Н.П. Курышкин, доцент, к.т.н.,
О.В. Любимов, , доцент, к.т.н.
г. Кемерово, КузГТУ, Yoruk91@gmail.com

С каждым годом электронная промышленность выпускает новые всё более сложные и мощные микроконтроллеры (МК), тем самым усложняя процесс разработки и проектирования электронных устройств на основе микроконтроллеров.

Эффективным решением этой проблемы является использование в электронных устройствах специального программного обеспечения в виде конечных автоматов и разработка простых и эффективных операционных систем (ОС).

Такая ОС была разработана для микроконтроллеров AVR семейства XMEGA [1]. С появлением новых микроконтроллеров она была модернизирована с уклоном на усовершенствованное ядро архитектуры 80C51.

Главными особенностями модернизированной ОС стали:

− перенос ОС на язык среднего уровня C/C++;

− поддержка МК улучшенной 1x/4x/2x-тактной архитектуры 80C51 для МК фирмы Silabs c8051Fxxx и фирмы NXP LPC700/LPC900;

− полная поддержка МК AVR семейства XMEGA серий A и D;

− высокая гибкость системы на языке C++;

− разработка специализированных универсальных драйверов для модулей микроконтроллера;

− улучшение системы приоритетов при выборе и установке задач на исполнительный конвейер;

− возможность считывания последовательности команд и их аргументов из памяти EEPROM;

− работа ОС в режиме «псевдомногопоточности».

Перенос ОС на язык среднего уровня C/C++ позволил значительно упростить разработку программ и увеличить надежность.

В таблице приведены сравнительные характеристики новых микроконтроллеров с улучшенной CISC-архитектурой на базе ядра 80C51. Именно на них была сориентирована модернизированная ОС. В таблице под максимальной скоростью понимается максимальная частота стабильной работы МК; производительность – это количество операций, выполняемых МК на максимальной частоте в MIPS (MIPS – Mega Instruction Per Second – 1 миллион операций в секунду).

Сводная таблица параметров МК

Фирма-производитель	Семейство	Максимальная скорость, МГц	Производительность
NXP	LPC700	18	4,5 MIPS
NXP	LPC900	18	9 MIPS
Silabs	C8051Fxx	От 20	1 IPS/Hz
Atmel	Xmega	32	32 MIPS

В список поддерживаемых ОС устройств попали представители классической архитектуры 80C51: МК LPC700, LPC900 фирмы NXP, c8051Fxxx фирмы Silabs с программатором и ATAVR XPLAIN A1 фирмы Atmel. Эти МК имеют очень высокую надежность (практически полное отсутствие ошибок в работе кристалла), высокую плотность кода благодаря CISC-архитектуре, имеют улучшенное ядро, способное выполнять основную часть команд за 1 / 2 / 4 машинных такта

(у классического ядра 12-тактное ядро). Также хочется отметить очень низкий ток потребления МК фирмы Silabs и возможность работы под напряжением от 0,9 В.

Благодаря концепции нового подхода к конфигурации МК, отличного от того что, по мнению Atmel, использовали и используют любители МК AVR, программирование основывается на двух принципах:

1) использование типовых модулей;

2) применение битовых масок и логических операций.

То есть, по сути, модули представляют собой кирпичики (USART, TWI, ADC и т.п.), составляющие весь МК в целом, а раз так, почему бы в таком случае не отказаться от придумывания все новых и новых имен регистров и не назвать их все на один лад, скрыв каждый за своим модулем? Подход, берущий свои корни еще в переходе от С к С++, нашел свой путь и здесь.

Приведём пример объявления простейшего типа дроби:

```
struct Drob  // Дробь)).
{ char chislitel;
  char znamenatel};
```

Для того чтобы указать член, с которым будет производиться работа, используется обычная разделительная точка:

```
test.chislitel = 1;
test.znamenatel = 2;
```

В итоге, в test у нас содержится дробь ½ (с точки зрения компилятора это массив из 2 переменных). То есть весь функционал структуры ограничивается обычным сведением под «одну крышу». Мы можем создать структуру хранения чего угодно, например содержания памяти температурного датчика. Можем также «насоздавать» члены tempLsb, tempMsb и т.п., а потом объявить переменную с типом этой структуры и вызывать каждый член из нее. Таким образом, у нас все под рукой, прибрано и подсчитано, в отличие от того же массива, где нужно было бы помнить индекс расположения того или иного байта. Обычное наведение порядка, принцип «разделяй и властвуй», который нашёл свое начало еще в самой концепции языка С.

Теперь приступим к рассмотрению драйверов для работы с модулями. Так как модули во всем семействе XMega и ядра 80C51 являются однотипными, то появляется желание писать сразу нормальный драйвер под один модуль и затем использовать его по всему семейству.

Автором была проведена модернизация системы обслуживания очереди. В прототипе исходной ОС была реализована кооперативная система обслуживания, т.е. задачи должны были кооперироваться между собой согласно приоритетам. Сейчас появилась частичная вытес-

няющая система, способная выгружать срочно потребовавшуюся задачу в один из трёх первых элементов очереди.

Все современные восьмиразрядные МК несут на борту энергонезависимую память EEPROM, в которой остаются данные после отключения питающего напряжения. Эта особенность позволила очень сильно упростить процесс разработки ОС. При этом появилась возможность визуального программирования МК. В FLASH-памяти МК хранятся только коды задач, а последовательность и аргументы хранятся в памяти EEPROM, тем самым позволяя не «дергать» камень, а лишь править исходные данные.

Постоянное переключение между задачами создает эффект «многопоточности». Например, пока подпрограмма отправляет данные в последовательный порт, МК может произвести какие-либо вычисления и выполнить что-нибудь интересное во время задержек между задачами.

Таким образом, разработанная год назад ОС для МК AVR семейства XMEGA была модернизирована с уклоном на классическое ядро 80C51, тем самым позволив создавать эффективные и очень надежные автоматизированные системы. Данная разработка нашла свое применение в создании автоматизированных систем позиционирования исполнительных органов горных машин.

ЛИТЕРАТУРА

1. Мещеряков Я.Е. Операционная система для микроконтроллеров AVR семейства XMEGA // Сб. тр. XVIII Междунар. науч.-практ. конф. «Современные техника и технологии». Томск: Изд-во ТПУ, 2012. Т. 2. С. 359–360.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПОЗИЦИОНИРОВАНИЯ БУРОВЫХ СТАНКОВ

Я.Е. Мещеряков, П.М. Обоянский, студенты

Научные руководители: Н.П. Курышкин, доцент, к.т.н.,
О.В. Любимов, доцент, к.т.н.
г. Кемерово, КузГТУ, Yoruk91@gmail.com

В Кузбассе в 2012 г. были добыты рекордные 200 млн т угля, а к 2020 г. добыча увеличится более чем в два раза. Главным приоритетом развития угольной отрасли региона должно стать применение безопасных технологий путём увеличения доли добычи угля открытым способом, а также использования предварительной дегазации угольных пластов. Всё это будет сопровождаться значительным увеличением объёма буровых и буровзрывных работ.

Второй отличительной особенностью развития экономики региона является увеличение объёмов строительства жилья и объектов ин-

фраструктуры городов. При этом расширяется сфера использования новых технологий бестраншейной прокладки коммуникаций на территориях существующей застройки – технологий горизонтального и горизонтально направленного бурения.

Качество проведения как вертикальных, так и горизонтальных буровых работ определяется точностью позиционирования платформы бурового станка, а также точностью положения в пространстве исполнительного органа – бурового става. Так, при проходке буровзрывных скважин на угольных разрезах постоянный мониторинг горизонтальности платформы бурового станка исключит заклинивание и последующую поломку бурового става. Постоянный мониторинг положения бурового инструмента при горизонтальном бурении с последующей его корректировкой позволит обеспечить точность выхода инструмента в завершающей фазе бурения.

Основными функциональными элементами электронного устройства непрерывного мониторинга положения в пространстве буровых станков и их исполнительных органов являются: датчик (первичный преобразователь), включающий гироскоп и компас-акселерометр; микроконтроллер; помехоустойчивая линия связи и вычислительное устройство.

Если контролируется положение буровой коронки, то датчик должен быть дополнен излучателем, а по пути бурения должен находиться модуль с приёмником.

Современная электронная промышленность выпускает достаточно разнообразную гамму элементов таких функциональных устройств. Разработанная авторами автоматизированная система включает:

− трёхосевой микроэлектромеханический (MEMS) гироскоп L3GD20;

− трёхосевой MEMS компас-акселерометр LSM303DLHC;

− микроконтроллер p89lpc932a1 с установленной операционной системой;

− LIN трансмиттер TJA1021;

− вычислительный модуль на основе одноплатного компьютера Raspberry Pi;

− источник стабилизированного питания;

− специализированное программное обеспечение.

Таким образом, разработанная система имеет 6 степеней свободы и позволяет измерять:

– с помощью гироскопа – величину угловой скорости крена, тангажа и рысканья;

– с помощью компаса-акселерометра – проекции ускорения на оси x, y, z.

Гироскоп имеет встроенный датчик температуры для компенсации дрейфа нуля.

Следует отметить, что выходные сигналы с гироскопа очень сильно зашумлены и наблюдается сильный дрейф нуля, также есть накапливающаяся ошибка в результате суточного вращения Земли.

Компас-акселерометр представляет собой высокой чувствительности компас с прикрученным к нему акселерометром, необходимым для вычисления поправки. Дело в том, что когда компас находится в горизонтальном положении, его показания достаточно точны, а стоит его наклонить, как в выходных данных начинаются хаос и неразбериха. Для устранения этой проблемы необходимо высчитать склонение, которое определяется положением интегральной микросхемы в пространстве.

Микроконтроллер (МК) используется в качестве «сборщика» информации, он «собирает» данные с датчиков, подключенных по интерфейсу I2C, и передает их по помехозащищённому каналу LIN к вычислительному модулю.

В качестве вычислительного модуля был использован одноплатный компьютер Raspberry Pi (модель B), несущий на борту мощный процессор ARM архитектуры Broadcom BCM2835, работающий под управлением операционной системы Linux.

На рис. 1 представлен фрагмент массива данных с датчиков в консоли вычислительного модуля Raspberry Pi. Данные снимались с акселерометра (Aks) и с компаса (Kom) по трём осям соответственно *x*, *y* и *z*.

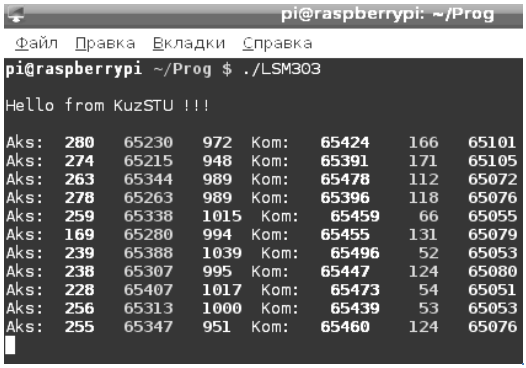


Рис. 1. Фрагмент массива данных в консоли вычислительного модуля Raspberry Pi

Разработанное программное обеспечение выполняло основательную математическую «чистку» сильно зашумленных данных, получаемых с датчиков. В качестве алгоритма очистки был использован метод скользящей медианы.

В результате программная часть обеспечивала:

- согласование и работу всей системы;
- фильтрацию шумов;
- борьбу с дрейфом в состоянии покоя;

− борьбу с вибрацией;

− расчет склонения компаса;

− минимизацию накопленной ошибки вследствие суточного вращения Земли.

Эффективность фильтрации определяется числом взятых для обработки элементов из массива исходных данных.

Заключение. Скомпонованная из функциональных блоков автоматическая система оценки положения исполнительных органов буровых станков является пока прототипом реальной системы, тем не менее она доказала свою работоспособность. До конца не решена задача эффективной фильтрации данных. Следующим шагом в её решении станет разработка и использование алгоритмов комплементарного фильтра либо фильтра Калмана и переход на помехоустойчивую сеть CAN.

РАЗРАБОТКА ПОРТАТИВНОГО АУДИОМЕТРА

М.В. Горбунов, П.К. Звеглянич, И.А. Лысенко, М.А. Михеев, Л.А. Патрашану, студенты

Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, Konfetka-921@mail.ru

Проект ГПО КИБЭВС-1209 – «Исследование речевого сигнала»

Целью проекта является создание электроакустического прибора для измерения остроты слуха – аудиометра. Аудиометры предназначены для оценки функционального состояния слухового анализатора человека путем определения порогов слышимости по воздушному и костному звукопроведению путем сравнения слуха обследуемого с характеристиками, эквивалентными порогу слышимости нормального человека.

Актуальность проблемы обусловлена, прежде всего, необходимостью оказания специализированной помощи пациентам с ушной патологией. По данным статистики Всемирной организации здравоохранения, 7% населения страдают нарушением слуховой функции. По данным Минздрава России, нарушениями слуха в нашей стране страдают примерно 6% населения. В России насчитывается 12 млн больных с нарушением слуха, в том числе детей и подростков более 600 тыс. Чем раньше нарушение слуха диагностировано и начато адекватное лечение, тем более вероятны успех терапии и выздоровление пациента. Существующие в арсенале врача-оториноларинголога методы (исследование восприятия речи) и приборы (камертон) зачастую позволяют оценить слух только приблизительно.

Важно отметить, что существующие скрининговые аудиометры могут анализировать только воздушную проводимость и только в узком диапазоне частот. Однако это не позволяет нам провести дифференциальную диагностику сенсоневральной тугоухости и вовремя начать лечение. Применение портативного скринингового аудиометра позволит врачам-отоларингологам своевременно направлять пациентов на хирургическое лечение. Также, портативный прибор легко перевозить, а значит, можно использовать на выезде, в телеметрической медицине. В перспективе портативный аудиометр может быть у каждого отоларинголога в кабинете. Таким образом, для практического здравоохранения крайне актуальными является вопрос создания недорогого портативного диагностического устройства, позволяющего провести полное исследование слуха у пациента, своевременно назначить лечение и предотвратить стойкую тугоухость и инвалидность больных. Организация производства в г. Томске позволит значительно снизить цену прибора и создать дополнительные рабочие места.

Исследуя рынок аудиометрии, можно увидеть массу дорогих аудиометров отечественного и зарубежного производства. Крупнейшими производителями аудиометров в мире являются компании «Entomed» (Швеция), «WelchAllyn» (США), «Interacoustics» (Дания) и компания «Maico» (Германия), из отечественных производителей найдена только одна компания «Биомедилен», выпускающая одну марку поликлинического аудиометра АА-2.

Проведен патентный поиск, объектом исследования стала аудиометрия как область измерений для диагностических целей. Ретроспектива поиска составила 15 лет. Классификационный индекс МПК A61B5/12. Согласно патентному поиску было найдено 72 патента. Аналогичных патентов предлагаемой разработки не было найдено.

За эти 15 лет наблюдается стабильный рост интереса к объекту исследования, появляются новые виды аудиометров, в разработку вкладываются финансовые средства, что говорит о том, что выбранная область весьма перспективна.

Опираясь на составленную функциональную схему исследуемого устройства, представленную на рис. 1, планируется создание электрической схемы аудиометра.

Электрическая схема – это чертеж, на котором показано упрощенное и наглядное изображение связи между отдельными элементами электрической цепи, выполненной с применением условных графических обозначений и позволяющей понять принцип действия устройства.

Данная схема будет соответствовать ГОСТ 27072-86 «Генераторы сигналов диагностические звуковые. Аудиометры. Общие технические требования и методы испытаний».

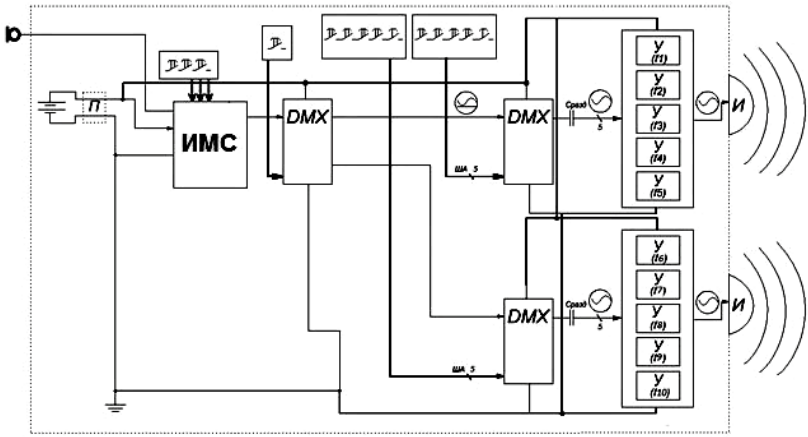


Рис. 1. Функциональная схема аудиометра: П – преобразователь напряжения питания; ИМС – интегральная микросхема ISD1416; У – усилительный каскад; И – излучатель вибрации; DMX – демультиплексор; ША – шина адреса

Ядром проектируемого аудиометра будет являться записывающая микросхема ISD1416, которая записывает нужный нам вид сигнала. Переключения частоты будут осуществляться с помощью простых переключателей. Такое решение было принято для повышения функциональности устройства.

Алгоритм работы устройства будет заключаться в следующем:

1. Запись сигнала.
2. Выбор вида проводимости с помощью переключателя – костной или воздушной.
3. Пользователь при помощи кнопок управления выбирает необходимую ему частоту и интенсивность сигнала.
4. Микросхема выдает сигнал на калибровочные усилители.
5. Переключателем задается нужный адрес.
6. На калибровочных усилителях реализуется необходимый размах напряжения.
7. Частота и уровень выбранного сигнала отображаются на индикационной панели.

ЛИТЕРАТУРА

1. Альтман Я.А., Тавартkиладзе Г.А. Руководство по аудиологии. М.: ДМК Пресс, 2003. 360 с.

2. Базаров В.Г., Лисовский В.А., Мороз Б.С., Токарев О.П. Основы аудиологии и слухопротезирования. М.: Медицина, 1984. 256 с.

3. Нигматуллин Р.Ф. Аудиометр портативный, основанный на костной проводимости. М., 2010. 94 с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ГРУППОЙ СЕРВОПРИВОДОВ

Р.А. Мирзаев, аспирант каф. технической механики
Научный руководитель Н.А. Смирнов, зав. каф. технической механики СибГАУ, д.т.н., проф.
г. Красноярск, СибГАУ, ramirzaev@mail.ru

Для разработки и отладки АСУ необходим мониторинг работы каждого элемента системы управления. Важно отметить, что в начале разработки проверку работоспособности схемотехнических и программных решений целесообразно проводить до того, как будет создан реальный прототип устройства. Поэтому актуально использование виртуальной модели системы управления.

В данной работе проводилось моделирование системы управления сервоприводами для устройства параллельной кинематики.

Автоматическая система управления (АСУ) сервоприводами состоит из персонального компьютера (ПК) и управляемого с него, контроллера сервоприводов (рис. 1).

Управляющая программа подает команды с компьютера на контроллер, в которых содержится информация о номере двигателя и его требуемом положении. Контроллер отвечает о выполненной команде и отправляет сигналы на серводвигатели для их поворота.

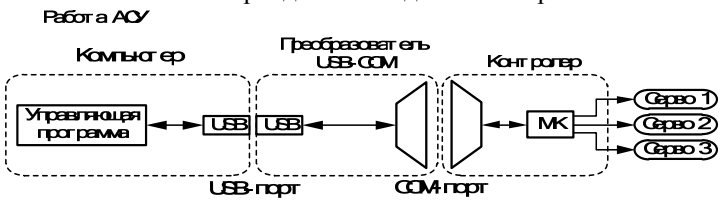


Рис. 1. Функциональная схема реальной АСУ

Данная система управления полностью промоделирована на компьютере, прежде чем был создан прототип. Моделирование работы системы управления выполняется при помощи трех программ: Serial Port Monitor, Visual Serial Ports Driver, Proteus.

Программа Serial Port Monitor является терминалом для обмена информацией с последовательным портом. Разработчик имеет возможность посылать команды на устройство и принимать сообщения. Таким образом, имитируется работа управляющей программы.

При помощи утилиты Virtual Serial Ports Driver эмулируется последовательный порт RS-232, соединенный виртуальным нуль-модемным кабелем. Создано два виртуальных последовательных порта в

системе, соединенные друг с другом для обмена информацией. Эта программа моделирует работу портов компьютера и контроллера, соединенных кабелем.

Средство разработки и тестирования Proteus моделирует работу электроники, в том числе серводвигателей и микроконтроллера Atmega-16. Для проверки разработанной программы, управляющей микроконтроллером, она загружается в виртуальную электрическую модель устройства. При корректной работе этой программой будет запрограммирован реальный микроконтроллер. В среде отладки Proteus имеется весь набор виртуальных приборов, таких как вольтметр, осциллограф, логический анализатор. Схема модели АСУ приведена на рис. 2.

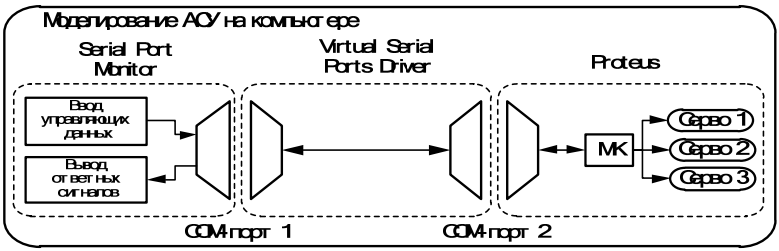


Рис. 2. Моделирование АСУ на компьютере

В исследовательском образце используется серводвигатель HXT900. Ширина импульса 450–2450 мкс. Период между импульсами – 20 мс. Угол поворота 90°. При импульсах длительностью 450 мкс серводвигатель устанавливается в положение 0°. При импульсах длительностью 2450 мкс серводвигатель устанавливается в положение 90° (рис. 3).

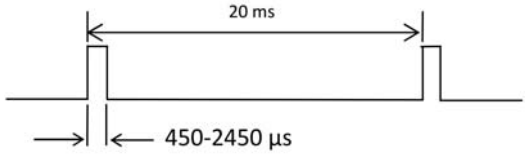


Рис. 3. ШИМ-сигнал управления сервоприводом

Структура команды от управляющей программы на контроллер: <начало><номер двигателя><требуемое положение>.

Начало – это один старт-байт в шестнадцатеричной системе равен FF, обозначает начало передачи.

Номер двигателя от 0 до 7. Система управления имеет возможность управлять положением не более 8 сервоприводов. Данное количество достаточно для абсолютного большинства устройств параллельной структуры.

Данные представляют собой ширину импульса ШИМ-сигнала, при помощи которого управляются сервоприводы. Требуемое положение предаётся одним байтом. Возможно увеличение количества байт для большей точности.

Заключение. Для отладки и тестирования работы различных элементов управления разработана виртуальная АСУ, которая будет использована при исследовании устройств параллельной структуры.

Главным результатом моделирования стала работоспособность созданного прототипа, а также отработка углов поворота сервоприводов с заданной точностью.

ЛИТЕРАТУРА

1. Бесекерский В.А., Попов Е.П. Теория систем автоматического управления. СПб.: Профессия, 2003.

2. Мирзаев Р.А., Смирнов Н.А., Смирнов А.Н. Расчет параметров движения приводов механизма параллельной структуры // Вестник СибГАУ. 2011. Вып. 5. С. 62–64.

3. Федоров Ю.Н. Справочник инженера по АСУТП: проектирование и разработка. Вологда: Инфра-инженерия, 2008.

ПОДХОД К ПОСТРОЕНИЮ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ УЧЕТА НЕФТЕПРОДУКТОВ

А.С. Озимук, бакалавр, К.В. Богданов, доцент, к.т.н.

г. Красноярск, Сибирский государственный аэрокосмический университет, каф. ИВТ, ozimuk@bk.ru, kosyag@gmail.com

В данной работе рассмотрены автоматизированные системы учета нефтепродуктов, канал последовательного обмена, произведен анализ преимуществ и недостатков систем и пути их дальнейшего развития. Приведена структура разрабатываемой системы удаленного мониторинга.

Автоматизированная система учета нефтепродуктов (датчики уровня, плотности, температуры и подтоварной воды совместно с блоком преобразователей) осуществляет измерение уровня нефтепродуктов и сжиженных газов, плотности и температуры нефтепродуктов, а также температуры сжиженных газов, уровня подтоварной воды нефтепродуктов и сжиженных газов, постоянный контроль за отсутствием несанкционированных утечек и формирование команд о предельных значениях уровня. Система обеспечивает вычисление по ГОСТ Р 8.595.2002 массы нефтепродуктов и сжиженных газов с погрешностью ±0,4% и периодическую поверку уровнемера встроенной системой контроля без демонтажа датчиков уровня. Система учета нефтепро-

дуктов обеспечивает визуальный контроль состояния ёмкостей, качества нефтепродуктов, возможные утечки и аварийные ситуации, поможет отслеживать и планировать поставки, а также просматривать общую экологическую ситуацию на АЗС, АГЗС.

На сегодняшний день на рынке оборудования для АЗС имеется довольно широкий перечень техники для измерения уровня, температуры и плотности нефтепродуктов в резервуарном парке. В России одними из самых популярных систем измерения нефтепродуктов по уровню, температуре, плотности являются следующие представители: OPW SiteSentinel, iTouch, Gamma УИП-9602, Colibry, Gilbarco veeder-root, «Струна».

Наиболее интересными на рынке являются системы Gamma УИП-9602 и Gilbarco veeder-root. Программное обеспечение для этих систем учета нефтепродуктов схожи и выполняют следующие основные функции: прием нефтепродукта, привезенного на АЗС, передача нефтепродуктов в резервуарах по смене, постоянный контроль всех параметров нефтепродукта в резервуаре и запись этих параметров. Для передачи данных от оборудования в программное обеспечение эти системы используют протокол обмена modbus RTU.

В RTU режиме данные передаются в виде 8-разрядных двоичных символов. Каждое сообщение начинается с интервала тишины равного времени передачи 3,5 символа (байта) при данной скорости передачи в сети, после чего передается байт адреса ведомого устройства (Slave) в диапазоне 1–0F7h (здесь и ниже по тексту числа, оканчивающиеся символом «h», приведены в шестнадцатеричной записи; 0F7h соответствует числу 247). Нулевой адрес обращения зарезервирован для одновременной передачи всем подчиненным (широковещательная передача). Вслед за последним передаваемым символом также следует интервал тишины продолжительностью не менее 3,5 символа.

Новое сообщение может начинаться после этого интервала. Символы кадра сообщения передаются непрерывным потоком. Если интервал тишины продолжительностью 1,5 символа возник во время передачи текущего кадра, принимающее устройство заканчивает прием сообщения и следующий байт будет воспринят как начало следующего сообщения.

Для обнаружения возможной ошибки связи в конце сообщения вставляется 16 бит поля контрольной суммы CRC, которая является результатом вычисления «Cyclical Redundancy Check» над содержанием сообщения. При передаче CRC в сообщении сначала передается младший байт CRC, затем старший.

Но и эти системы не обладают необходимой функциональностью, в частности удалённым мониторингом.

В настоящее время существует проблема удаленного мониторинга систем измерения и учета нефтепродуктов. Быстрая проверка технологических параметров в резервуарах на автозаправочных станциях (АЗС), нефтебазах (НБ), нефтехранилищах не всегда возможна и тем самым замедляет процесс закупки и учета светлых нефтепродуктов.

Удаленный мониторинг таких систем в настоящее время востребован и актуален среди владельцев небольших сетей АЗС, а также инженеров, отвечающих за снабжение крупных сетей АЗС и НБ.

Система мониторинга должна решать следующие задачи: удаленный просмотр основных параметров системы измерения и учета нефтепродуктов, хранение баз данных основных параметров, за последнее *N*-е количество времени, графическое отображение параметров за указанное *N*-е количество времени, единый веб-интерфейс или клиентское приложение с основным рабочим окном, защита канала передачи данных (клиент–сервер).

Для этого предполагается реализовать следующие модули: модуль сбора информации и отправки пакетов данных на сервер, сам веб-сервер, модуль представления информации через веб-интерфейс (тонкий клиент) или клиентское приложение, модуль защиты канала передачи данных (рис. 1).

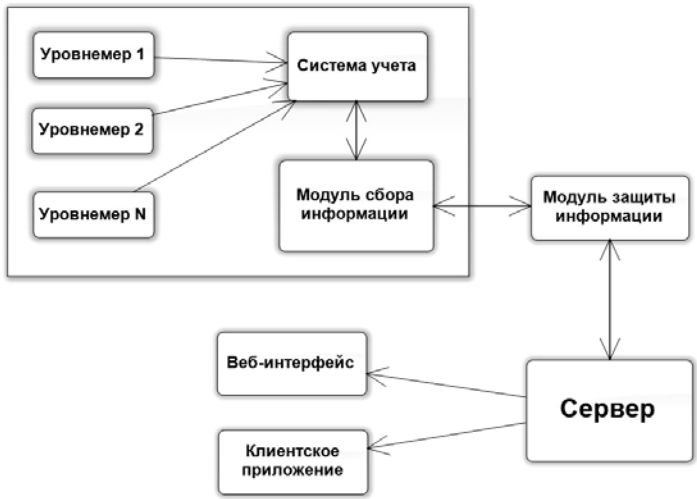


Рис. 1. Функционирование системы мониторинга

Модуль сбора информации интегрируется с системой учета нефтепродуктов и по запросу сервера передает пакеты данных. Запрос выполняется раз в 30 с.

Модуль веб-сервера выполняет следующие задачи: обработка данных; проверка на целостность пакетов данных; ведения архива, аналитики, данных *N*-е количество времени; генерация запросов; организация учета доступа к данным, через веб-интерфейс или клиентское приложение; ведение базы данных организаций.

Модуль представления информации через веб-интерфейс или клиентское приложение позволяет пользователю осуществить доступ к базе данных (архиву) и просмотру основных параметров в своем аккаунте организации.

Модуль защиты канала передачи данных обеспечивает конфиденциальность передаваемой информации.

В целом система мониторинга должна быть надежна и проста в использовании. Данная система должна облегчить и ускорить работу оператора, исключить застои АЗС из-за нехватки топлива и помочь организации максимально извлечь прибыль от своей деятельности.

К сожалению, только две системы, SiteSentinel iTouch и Colibry, обладают такими важнейшими функциями программного обеспечения, как импорт данных на удаленный ПК (мониторинг). И именно эти функции программного обеспечения есть пути развития и улучшения систем измерения и учета нефтепродуктов.

ЛИТЕРАТУРА

1. Дуглас Э.К. Сети TCP/IP / Э.К. Дуглас, Л.С. Дэвид. М.: Вильямс, 2002. 592 с.

2. Хорев П.Б. Программно-аппаратная защита информации / П.Б. Хорев. М.: Форум, 2009. 352 с.

РАЗРАБОТКА И РЕАЛИЗАЦИЯ АЛГОРИТМОВ КАЛИБРОВКИ РЕНТГЕНОВСКОГО ИЗЛУЧАТЕЛЯ РЕНТГЕНОВСКОГО РОТАЦИОННОГО КОМПЛЕКСА

А.Л. Павленко, П.С. Боев, студенты каф. КИБЭВС

Научный руководитель Н.М. Федотов, зав. лаб. безопасных биомедицинских технологий ЦТБ, к.т.н.

г. Томск, ТУСУР, pavlenko.sanya@sibmail.com

Проект ГПО КИБЭВС-0709 – «Разработка системы управления рентгеновского ротационного комплекса»

Рентгеновский ротационный комплекс (РРК) [1] предназначен для выполнения продолжительных рентгеноскопически контролируемых интервенционных процедур.

РРК применяется для визуализации операционного пространства и хирургического инструмента в общей хирургии, нейрохирургии, ор-

топедии и травматологии. В режиме непрерывного просвечивания – для слежения за положением хирургического инструмента и визуализации операционного пространства. В импульсном режиме просвечивания – для получения рентгеновских изображений коронарных сосудов сердца и легочных вен левого предсердия во время введения в них рентгеноконтрастного вещества.

Структурная схема РРК приведена на рис. 1.

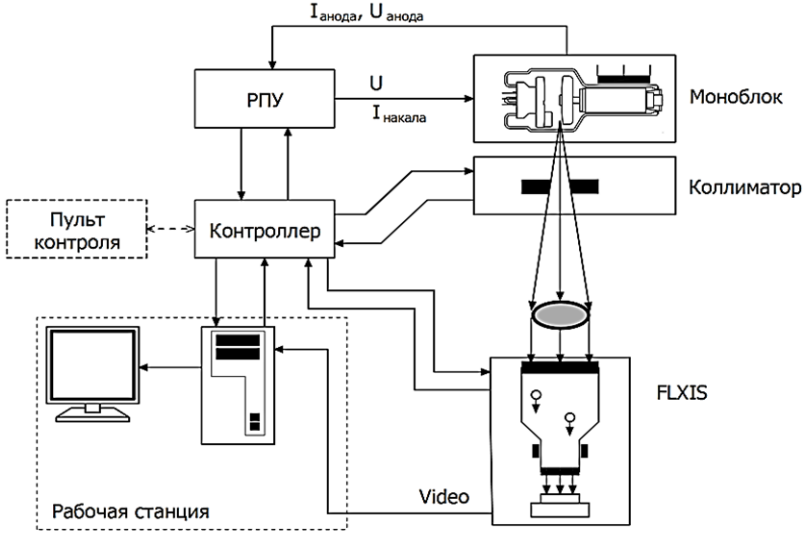


Рис. 1. Структура комплекса

Целью работы является разработка и реализация алгоритмов калибровки рентгеновского излучателя (моноблока), которая заключается в получении зависимости тока анода от тока накала для напряжений между анодом и катодом рентгеновской трубки в диапазоне 40–120 кВ, как для большого, так и малого фокусных пятен. Так же необходимо отметить, что калибровка должна выполняться за максимально короткое время, а результаты калибровки должны обеспечивать задание тока анода с погрешностью не более 10%.

Результаты работы. Экспериментальным путем по 16 точкам (2, 2,5, 3, 4, 5, 7, 10, 15, 20, 25, 30, 35, 40, 45, 50, 100 мА) были сняты графики зависимости тока анода от тока накала рентгеновской трубки для каждого из значений напряжения между анодом и катодом, равных 30, 35, 40, 45, 50 кВ. В результате их анализа было выяснено, что зависимости тока анода от тока накала в диапазоне 2–50 мА (малое фокусное пятно) описываются полиномиальной функцией регрессии 3-го поряд-

ка, которую можно найти по точкам 4, 7, 20 и 50 мА, и полученная характеристика обладает среднеквадратическим отклонением в пределах ±5%. Для описания зависимостей тока анода в диапазоне 2–100 мА (большое фокусное пятно) в пределах погрешности ±5% подходит полиномиальная функция регрессии 5-го порядка. При этом функция регрессии находится по точкам 4, 7, 20, 50, 75 и 100 мА.

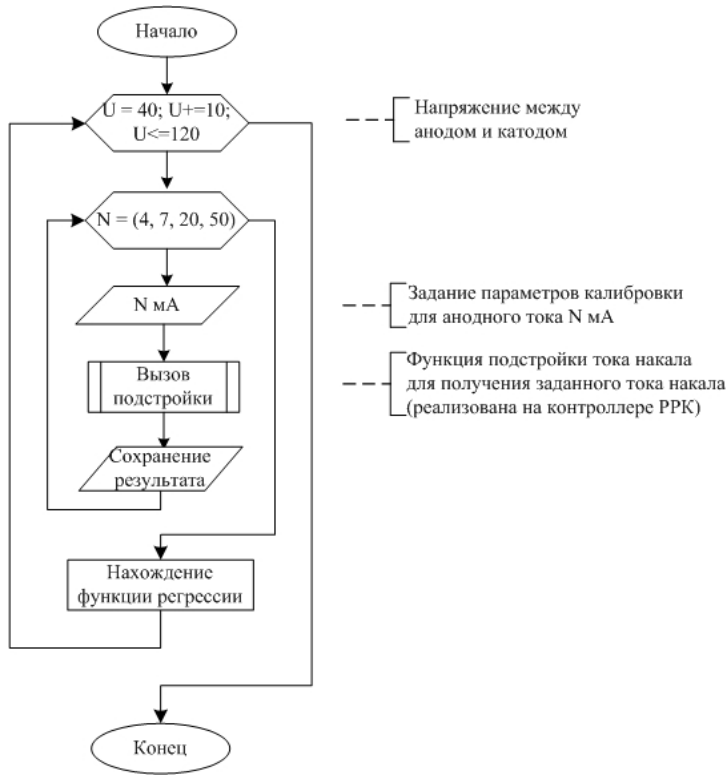


Рис. 2. Основной алгоритм калибровки малого фокусного пятна

Основываясь на полученных результатах анализа, были разработаны алгоритмы калибровки. Осуществляется калибровка следующим образом: для каждого из фокусных пятен производится снятие точек зависимости тока анода от тока накала для набора напряжений (40, 50, …, 120) между катодом и анодом рентгеновской трубки. Для малого фокусного пятна снимается по 4 точки, для большого – по 6 точек для каждого значения напряжения из приведенного выше набора. Затем, используя полученные точки, находятся функции регрессии 3-го по-

рядка для малого фокусного пятна и 5-го порядка для большого фокусного пятна. Полученные функции регрессии используются в дальнейшем при задании режима работы РРК. Основной алгоритм калибровки малого фокусного пятна приведен на рис. 2.

Заключение. Разработаны и реализованы алгоритмы калибровки рентгеновского излучателя рентгеновского ротационного комплекса. Данные алгоритмы позволяют значительно снизить время, затрачиваемое на калибровку, и как следствие позволяют сохранить ресурс рентгеновской трубки, так как требуют снятия минимального количества точек, в отличие от простых систем калибровки, когда производится полное снятие зависимости. Также выполняется требование по точности получаемых зависимостей.

ЛИТЕРАТУРА

1. Разработка ротационного рентгеновского аппарата с кольцевым штативом для оперативного создания 3D-изображений сердца / Н.М. Федотов, А.И. Оферкин, А.И. Буллер и др. // Доклады ТУСУРа. 2010. № 2 (22), ч. 2. С. 97–101.

ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ ПАМЯТИ

О.В. Пехов, аспирант, инженер

Научный руководитель А.А. Шелупанов, проректор по НР, зав. каф. КИБЭВС, д.т.н., проф.

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

Оперативная память (ОЗУ) является важным компонентом вычислительной системы, от стабильности ее функционирования во многом зависит работа системы в целом. В связи с этим часто встречается задача тестирования ОЗУ на отказоустойчивость. Наиболее типичными ситуациями тестирования модулей памяти на отказоустойчивость можно считать две:

– выявление дефектных модулей памяти на раннем этапе тестирования при производстве ЭВМ;

– определение устойчивости функционирования исправных модулей при разгоне модулей памяти.

Особенности ОЗУ как объекта диагностики состоят в следующем:

– нет возможности прямого доступа к внутренним точкам схемы;

– ячейки памяти имеют электрическую связь через адресные шины и шины данных, и при наличии дефектов может возникать взаимное влияние ячеек, нарушающее работу устройства [1].

Тестирование памяти производится с целью выявления места и характера неисправности ОЗУ. Дефекты памяти могут быть связаны

как с неисправностью непосредственно модулей ОЗУ, так и с дефектами внешнего оборудования. Они могут проявляться в виде замыкания разрядов адресов и данных, отдельных неисправных ячеек, искажений отдельных ячеек при нагревании, пульсациях питания и т.п. [2].

Технически существуют следующие виды тестирования:

– аппаратное тестирование – требует наличия специального оборудования для диагностики памяти, не требующего подключения к персональному компьютеру (ПК);

– аппаратно-программное тестирование – оборудование реализовано как отдельное физическое устройство, подключаемое к компьютеру, но тестирование производится «вшитой» программой, которая выполняется ЦП;

– программное тестирование – осуществляется с помощью специального ПО.

Аппаратные решения, используемые для тестирования ОЗУ, выполнены в качестве конструктивно законченных устройств. Большинство подобных устройств находится в ценовом диапазоне от 1000 до $6000. Функционал устройств направлен на обнаружение дефектов памяти различных типов и форматов модулей.

а *б* *в*

Рис. 1. Внешний вид устройств: *а* – JS-9500; *б* – B+K Precision 898A; *в* – RAMCHECK

Устройство «JS-9500», производитель Hongyang E-toolsfix Co., Ltd (Китай) [3] (рис. 1, *а*). Это устройство позволяет выявить физические дефекты, для текущих значений токов и напряжений и определить параметры задержек. Оно подходит для тестирования модулей памяти на производстве, так как производит все тесты в режиме реального времени, диагностирует функциональные сбои, автоматически производит операции записи/чтения, имеет высокую скорость обработки результатов. Для вывода результатов используется панель цветных светодиодов. Технические характеристики прибора:

– поддержка и автоопределение: типа модулей памяти (SDRAM, DDR, DDR2, DDR3), объема модулей памяти (От 64 Мб до 16 Гб);

– ширина шины данных: 64 бит;

– размеры: 390×260×50 мм, масса 4,5 кг;

– стоимость от $1320.

Достоинствами устройства «JS-9500» являются: поддержка модулей памяти различных типов и объемов и высокая скорость тестирования. К недостаткам можно отнести светодиодную панель, не удобную в качестве средства отображения.

«B+K Precision 898A Simm tester», производитель B+K Precision (США) [4] (рис. 1, *б*), представляет собой автономный портативный прибор, для тестирования модулей памяти. Устройство снабжено интуитивно-понятным пользовательским интерфейсом: ЖК-дисплей и 4 клавиши позволяют осуществлять управление через многоуровневую систему меню. Технические характеристики:

– выявление и идентификация ошибок: сбои, связанные с мощностью и шумом, размыкания и короткие замыкания, сбои синхронизации, ошибки сохранения данных;

– поддерживает типы модулей памяти: SDRAM, PM DRAM, FPM, EDO; объемом от 8 до 256 Мб;

– размеры: 178×152×64 мм, вес: 1,59 кг;

– стоимость $1175.

К достоинствам устройства можно отнести небольшой размер, возможность выбора режима тестирования и способа отображения результата. Недостаток устройства – поддержка только устаревших типов модулей.

Устройство «RAMCHECK», производитель INNOVENTIONS, Inc (США) [5], (рис. 1, *в*), представляет собой модульную, независимую от платформы систему тестирования памяти. Она обеспечивает простое и быстрое тестирование памяти различной конфигурации. Технические характеристики:

– показывает подробную информацию о структуре памяти;

– поддерживает типы модулей: FPM, EDO, SDRAM, DDR, DDR2, DDR3 объемом От 8 Мб до 2 Гб;

– ЖК-дисплей с возможностью отображения графиков;

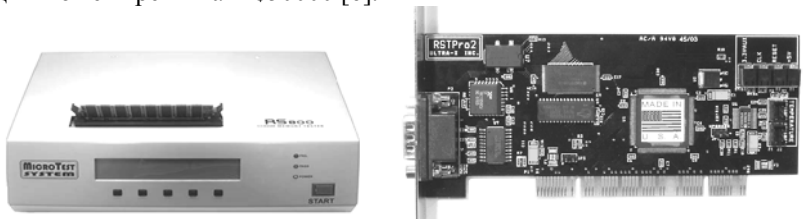
– возможность подключения к компьютеру через USB;

– размеры: 250×160×65 мм, масса 4 кг;

– стоимость от $6000.

Устройство оснащено 4-строчным ЖК-дисплеем. Тестирование памяти сопровождается выводом подробных результатов на экран. Устройство обеспечивает высокую точность результатов испытаний. Тестер «RAMCHECK» может быть расширен для работы с различными форм-факторами памяти. В комплект поставки входит специальное ПО для компьютера, оно позволяет регистрировать и сохранять ре-

зультаты испытаний в памяти ПК. Недостатком устройства является высокая цена. Стоимость устройства без дополнительных модулей расширения составляет $6000, стоимость в расширенной комплектации может превышать $50000 [6].



а *б*

Рис. 2. Внешний вид устройств: *а* – RS800; *б* – RST Pro 2

«RS800-166» SDRAM Tester MicroTestSystem, INC (США) [7] (рис. 2, а)). Особенности устройства:

– ЖК-дисплей;
– подключение компьютеру через USB-порт;
– автоматическое определение особенностей тестируемой памяти;
– поддерживаемая тактовая частота: 100, 133, 166 МГц;
– поддержка работы с SPD: программирование/чтение/проверка;
– размеры: 410×280×101 мм, масса ~ 3 кг;
– стоимость $1800.

RS800 обладает функционалом, аналогичным «RAMCHECK», но поддерживает только устаревшие модули памяти типа SDRAM объемом от 8 Мб до 1 Гб. Нет поддержки дополнительных адаптеров.

Плата RAM Stress Test Professional 2 (RST Pro2) производства США (рис. 2, *б*) – пример аппаратно-программного решения. Она выполнена в качестве отдельного устройства, устанавливаемого в PCI-слот компьютера (существуют модификации платы для установки в слоты Mini-PCI, PCI-Express и USB). Стоимость данного устройства составляет $600 [8].

Тестирование памяти с помощью RST Pro2 позволяет устранить влияние программного обеспечения ПК. Для проверки модулей памяти в устройстве реализовано 24 (из заявленных 30) различных алгоритма, поддерживающих память различных типов (SDRAM, DDR, DDR2, RDRAM). Устройство позволяет тестировать объемы памяти до 64 ГБ. Также имеется возможность чтения информации микросхемы SPD. RST Pro2 позволяет выбрать область памяти, подлежащую тестированию. Настройки самого теста памяти включают диапазон тестируемых адресов памяти, выбор режима кэширования данных, периода регене-

рации памяти и количества циклов тестирования. Достоинства RST Pro2:

– нахождение точного физического адреса ошибки;

– возможность полностью автоматизированного тестирования;

– возможности мониторинга температуры и удаленного слежения за результатами тестирования.

Из недостатков продукта можно выделить следующие:

– сравнительно большое время нахождения ошибки;

– результат теста зависит от используемого оборудования [9].

Исходя из обзора инструментов тестирования памяти, были сделаны следующие выводы:

– аппаратно-программные решения позволяют тестировать память в системном окружении и выявлять ошибки. RST Pro2 позволяет тестировать большинство видов памяти, недостатком является необходимость тестового стенда. Такое решение подходит для конечных пользователей и системных администраторов, обслуживающих однородные по конфигурации парки ПК;

– аппаратные решения обладают высокой скоростью тестирования и большой точностью результатов. Применение устройств позволяет уйти от необходимости тестовых стендов. Лидером рынка устройств проверки памяти является «RAMCHECK», так как он очень функционален и обладает множеством дополнительных опций, но высокая стоимость прибора является его главным недостатком.

ЛИТЕРАТУРА

1. Тестирование памяти [Электронный ресурс] / Intel IT Galaxy Сообщество IT-профессионалов. Режим доступа: http://ru.intel.com/business/community/index.php?automodule=blog&blogid=7822&showentry=761. Загл. с экрана.

2. Bianca Schroeder, Eduardo Pinheiro, Wolf-Dietrich Weber. DRAM Errors in the Wild: A Large-Scale Field Study [Электронный ресурс] / University of Toronto. Режим доступа: http://www.cs.toronto.edu/~bianca/papers/sigmetrics09.pdf. Загл. с экрана.

3. JS9500 (SD/DDR/ DDR2/DDR3) Memory Tester [Электронный ресурс]. Hongyang E-toolsfix Co., Ltd. Режим доступа: http://www.toolsfix.com/en/products/ product_78.html. Загл. с экрана.

4. B+K 898A SIMM Tester [Электронный ресурс]. TEquipment.net An Interworld Highway, LLC Company. Режим доступа: http://www.tequipment.net/BK898A.html. Загл. с экрана.

5. Ramcheck [Электронный ресурс] / INNOVENTIONS Inc. Режим доступа: http://www.memorytesters.com/ramcheck/ramcheck.htm. Загл. с экрана.

6. Тестеры для проверки SIMM-DIMM модулей. RAMCHECK plus [Электронный ресурс]. ОАО «Техно». Режим доступа: http://www.techno.ru/txt/4_2/5.htm. Загл. с экрана.

7. RS800-166 SDRAM Tester [Электронный ресурс] / MicroTestSystem. Inc. Режим доступа: http://www.microtestsystem.com/rs800-166.html. Загл. с экрана.

8. RAM Stress Test Professional 2 Product view [Электронный ресурс] / Ultra-x, Inc. Professional PC diagnostic tools. Режим доступа: http://www.uxd.com/rstpro2.shtml. Загл. с экрана.

9. RAM Stress Test Professional 2 – программно-аппаратный комплекс тестирования модулей памяти [Электронный ресурс]. Проект ixbt.com – Специализированный российский информационно-аналитический сайт, освещающий вопросы цифровых технологий и современных решений на их базе. Режим доступа: http://www.ixbt.com/mainboard/rst-pro2.shtml. Загл. с экрана.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ НАСОСНОЙ СТАНЦИИ

А.М. Плеханов, студент каф. КИБЭВС

Научный руководитель И.Ш. Замалиев, зам. нач. управления РС АСУ ТП ООО «РН-Информ», maclautsmechom@gmail.com

Автоматизированная система управления технологическим процессом создаётся для дистанционного наблюдения и управления технологическим процессом и оборудованием насосной станции с автоматизированных рабочих мест оператора, ведения технологических режимов насосной станции (управление и блокировки по технологическому оборудованию площадок) в соответствии с технологическим регламентом.

Целями создания системы являются:

– повышение качества ведения технологического режима и его безопасности;

– повышение оперативности действий персонала;

– повышение надежности управления объектом.

Система должна иметь функционально и территориально распределенную структуру. В состав системы должны входить:

− автоматизированное рабочее место АРМ оператора;

− станции управления насосными агрегатами СУНА (по одной на каждый насосный агрегат, всего три);

− станция управления общестанционная СУО.

СУНА должна обеспечивать сбор информации и управление оборудованием НА, маслосистемой двигателей и маслосистемой насосов.

СУО должна обеспечивать сбор информации и управление оборудованием блоком дренажных насосов, блоком сепараторов, блоком фильтров, блоком гребёнки, блоком откачки промывной воды и кустом водозаборных скважин.

Функциональная схема системы представлена на рис. 1.

В качестве станций управления используются программируемые логические контроллеры DirectLOGIC. Драйверы для контроллеров разрабатываются на языке релейной лестничной логики в программном пакете DirectSOFT.

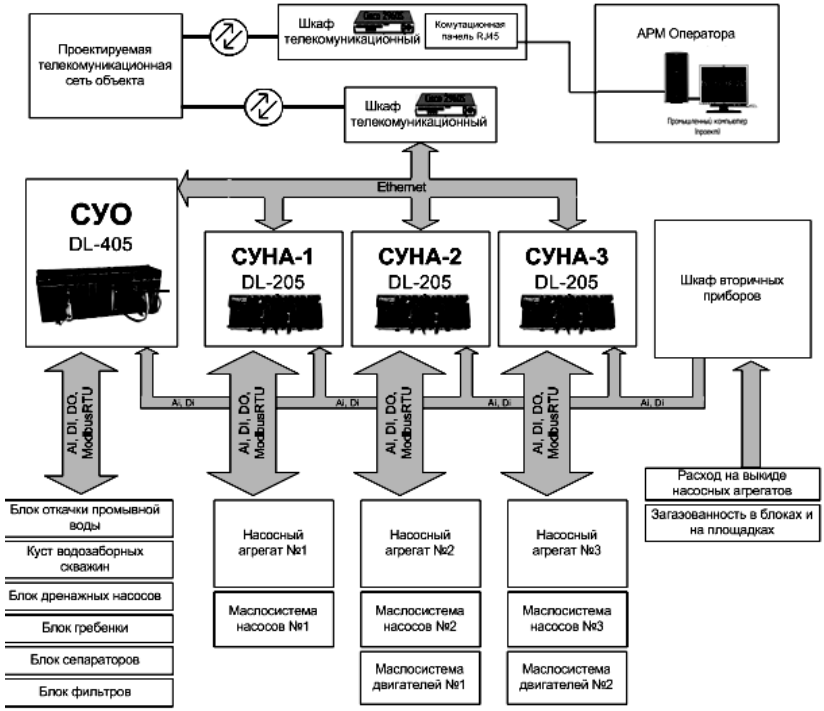


Рис. 1. Функциональная схема

Алгоритмы системы. Порядок выполнения алгоритма. Алгоритм выполняется циклически. Все алгоритмические модули выполняются в определенной последовательности, один раз в течение цикла.

Результаты решения алгоритмического модуля передаются на АРМ оператора, полевому оборудованию или другим алгоритмическим модулям только после полного завершения выполнения алгоритма данного модуля.

Для коммутации и осуществления передачи данных используются:

– интерфейсы RS-232, RS-485 с протоколом последовательного обмена данными Modbus RTU;

– сетевой интерфейс Ethernet с протоколами DDE, OPC, Modbus TCP, ECOM.

ЛИТЕРАТУРА

1. Руководство пользователя контроллера DL205. 3-е изд.: в 2 кн. Кн. 1. Automationdirect.com™ Incorporated, 2011. 418 с.

2. Руководство пользователя контроллера DL205. 3-е изд.: в 2 кн. Кн. 2. Automationdirect.com™ Incorporated, 2011. 236 с.

3. Коммуникационные модули Ethernet ПЛК DL05/06/205/405. Руководство пользователя – Automationdirect.com™ Incorporated, 2011. Перевод – ПЛК-системы. М., 2011. 114 с.

4. Программное обеспечение для программирования DirectSOFT5 – Automationdirect.com™ Incorporated. 2006. 247 с.

5. Контроллеры DirectLOGIC основы программирования. ПЛК-системы. М., 2009. 132 с.

6. Аналоговые модули ввода/вывода DL205. Руководство пользователя – Automationdirect.com™ Incorporated. 2002. 339 с.

7. Аналоговые модули ввода/вывода DL205. Руководство по эксплуатации Automationdirect.com™ Incorporated, 2005. 222 с.

АВТОМАТИЗИРОВАННАЯ УСТАНОВКА ХИМИЧЕСКОЙ ОБРАБОТКИ ПЕЧАТНЫХ ПЛАТ

В.А. Бахарев, А.И. Радостев, студенты каф. КИБЭВС

Научный руководитель Л.А. Торгонский, доцент

г. Томск, ТУСУР, alexandrradostev@gmail.com

Печатные платы широко применяются в производстве изделий приборостроения. средств вычислительной техники. Выполняемая работа посвящена созданию автоматизированной установки для химической обработки печатных плат (ПП). В процессе химической обработки ПП включают в себя следующие операции:

– травление рисунка проводников в металлической фольге платы;

– отмывка плат после травления рисунка проводников;

– сушка плат после отмывки.

Производительность, не в пример производственным [1] , не является определяющей для разрабатывае-мой установки, Её применением решаются задачи снижения затрат времени оператора на перечисленных этапах обработки, улучшения условий контроля параметров режима обработки, повышения повторяемости результатов. Важным является и образовательный фактор выполнения работы по созданию установки, так как в процессе выполнения проекта приобретается опыт решения практических задач проектирования действующей технологической установки с микропроцессорным управлением.

Упрощённая кинематическая схема установки представлена на рис. 1. В схеме выделяются 5 технологических зон, относительно которых по горизонтали предусмотрено перемещение с помощью управ-

ляемоей эстакады (Э) с балкой (Т1). Балка Т1 имеет степень свободы на перемещение по вертикали и вместе с эстакадой Э является мостовым краном. На балку навешивается с помощью кронштейна-скобы С и технологических отверстий заготовка платы П (с рисунком для травления) и вместе с балкой Т1 плата может перемещаться по вертикали относительно ёмкостей с растворами Р1, Р2 и полости С2 сушки платы.

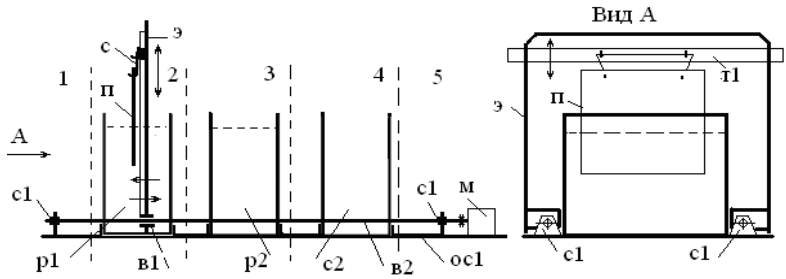


Рис. 1. Кинематическая схема установки

В зону 1 мостовой кран с помощью винтовой пары В1 (винтовые валы В2 и приводные гайки в эстакаде Э) и двигателя М перемещается в начале технологического цикла по включению установки и в процессе работы после завершения цикла. Винтовые валы, соединённые с двигателем М, установлены на стойках С1. В зоне 1 оператор навешивает плату П на балку Т1, после чего инициирует запуск технологического цикла.

В зоне 2 плата опускается в ёмкость Р1 с раствором травителя и исполняется травление рисунка платы. В качестве травителя выбран раствор хлорного железа как распространённый и менее агрессивный по безопасности применения. В зоне 2 контролируется время травления платы П, уровень и концентрация раствора, его температура, предусмотрен подогрев и барботирование раствора подачей воздуха в нижнюю область ёмкость Р1 от электромеханического насоса.

В зоне 3 размещена ёмкость Р2 с промывочной жидкостью, в качестве которой использована проточная вода, к источнику которой и накопителю слива ёмкость подключена эластичными трубками с управляемым клапаном подачи воды. Слив предусматривается стоком по фиксированному уровню промывочной жидкости. В ёмкости допустимо подключение подачи воздуха в жидкость для барботирования при промывке.

После промывки (с контролем времени) плата транспортируется в камеру С2 сушки зоны 4. В камеру С2 подаётся через эластичный

шланг подогретый воздух от фена. Контролируются время и температура сушки.

По завершении сушки плата транспортируется в зону 5, выдаётся звуковой сигнал, включается визуальный индикатор завершения цикла. Оператор снимает плату с кронштейном С и инициирует возврат транспортного крана в зону 1 для установки следующей платы и повторения технологического цикла.

Габаритные размеры установки определяются размерами пяти технологических зон, каждая из которых выбрана по 60 мм по горизонтали, высотой и шириной эстакады Э, определяемых размерами обрабатываемой платы. Высота эстакады принята равной 300 мм, а ширина – 200 мм, что соответствует возможности работы с платами до 125 мм на сторону. Электронный блок управления и питания двигателей транспорта эстакады Э и балки Т1 выполнен автономным и подключается к установке гибкий шлейф через разъём, установленный на основании ОС1. На рис. 1 блок управления и питания, как и узлы перемещения балки Т1, подачи воздуха, воды и подогретого воздуха подключения датчиков, не показаны. Длительности этапов обработки платы в зонах 2–4 технологического цикла (30–50 мин), управление подогревом, барботированием, термосушкой устанавливаются с блока управления установкой.

Установка находится в процессе подбора, отработки и изготовления и узлов конструкции. Ряд материалов, связанных с технологией и технологическим оснащением оборудования обработки ПП, приведен в [2].

ЛИТЕРАТУРА

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

2. Печатные платы [Электронный ресурс]. http://www.tech-e.ru/pechatnii-platy.php

АВТОМАТИЗАЦИЯ ОБРАБОТКИ СПУТНИКОВЫХ СНИМКОВ

И.Н. Шишкин, аспирант каф. КИБЭВС

Научный руководитель А.А. Шелупанов, проф., д.т.н

г. Томск, ТУСУР, sin@keva.tusur.ru

Процесс обработки данных дистанционного зондирования Земли (ДЗЗ) представляет собой последовательность следующих этапов:

1) прием данных с искусственного спутника Земли (ИСЗ);
2) распаковка принятых данных;
3) географическая привязка данных;

4) калибровка;

5) тематическая обработка.

Первые 4 этапа являются продолжительными и не требующими вмешательства человека, но этап тематической обработки зачастую требует вмешательства специалиста. Поэтому в рамках пятого этапа возможна обработка с заранее определенными параметрами для оценки снимка (облачность, охватываемая территория и т.п.).

Схема автоматизированной системы для обработки данных ДЗЗ представлена на рис. 1.

Рис. 1. Схема автоматизированной системы

Прием данных с ИСЗ происходит в автоматическом режиме согласно расписанию пролета спутников над зоной охвата антенной системы. Принимаемые данные сохраняются на терминал приема. После окончания сеанса приема данные передаются на сервер автоматической обработки. На нем в автоматическом режиме происходит распаковка, геопривязка, калибровка и обработка спутниковых сников со стандартными параметрами.

После обработки спутниковых снимков начинается процесс тайлинга (построение мозайки) для дальнейшего размещения на специализированном электронном географическом ресурсе – геопортале.

Размещение спутниковых снимков на геопортале является удобным, так как:

1) не требуется специального программного обеспечения для просмотра спутниковых снимков;

2) благодаря размещению ресурса в сети Интернет доступ к данным можно получить из любой точки мира;

3) возможно разграничение доступа к данным;

4) спутниковые снимки размещаются с географической привязкой;

5) возможно наложение векторных слоев.

Использование геопортала позволяет организовать архив снимков с возможностью просмотра снимков на определенную дату. Данные хранятся в виде тайлов, которые, конечно, ниже по качеству оригинальных снимков, но при этом занимают в разы меньше места на жестком диске. Но при необходимости можно востановить снимок из

исходных данных, принятых со спутника, которые хранятся в «запакованном» виде.

На рис. 2 представлено размещение трех снимков со спутника Terra на геопортале ТУСУРа.

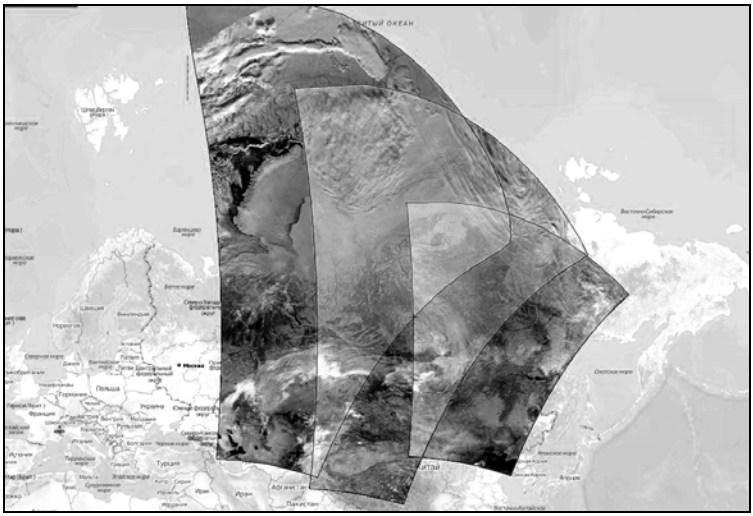


Рис. 2. Размещение снимков на геопортале

Автоматизация обработки данных ДЗЗ позволяет избавить людей от рутинных процессов распаковки, калибровки и геопривязки. Кроме того, размещение данных на геопортале позволяет оценить снимки и при необходимости выполнить более подробную тематическкю обработку.

МОДИФИЦИРОВАННЫЙ МЕТОД ДИХОТОМИИ

С.А. Лигачёв, С.А. Швед, студенты каф. ЭСАУ
Научный руководитель А.А. Светлаков, проф. каф. ЭСАУ, д.т.н.
г. Томск, ТУСУР, ivan.tchubiry@yandex.ru

Одной из повсеместных и наиболее часто встречающихся в самых разнообразных отраслях научной, научно-технической, производственной и т.п. деятельности современного человека является задача решения различного рода нелинейных скалярных уравнений. С ней приходится сталкиваться всякий раз, когда мы имеем дело с той или иной (какой-либо) скалярной нелинейной функцией $y = f(u)$ скаляр-

ного же аргумента u, и нам необходимо по ее заданному значению y_0 определить такое значение u_0 ее аргумента u, при котором она принимает значение y_0.

Актуальность данной задачи в практически необозримом множестве реальных ситуаций и их многообразие обусловили предложение целого ряда вычислительных методов и алгоритмов ее решения, базирующихся на различных идеях и подходах к их синтезу. Одним из подобных методов является метод дихотомии (греч. *dicha* – на две части + *tome* – сечение). Термин «метод дихотомии», используется как синоним терминов «метод деления отрезка пополам» (МДОП). Несмотря на то, что данный метод обладает целым рядом достоинств, которые обусловливают его привлекательность и предпочтительность его применения по сравнению с другими известными методами решения нелинейных уравнений, в настоящее время он не нашел широкого практического использования. Основной причиной его малой популярности и неширокого практического использования является низкая скорость сходимости последовательности приближенных решений, вычисляемых с его применением, и, соответственно, большие объемы вычислений, необходимых для получения достаточно точных решений. В связи с этим возникла необходимость модифицировать данный метод, дабы увеличить скорость сходимости.

Описание решения нелинейного уравнения модифицированным методом деления отрезка пополам (ММДОП).

1. Строим график функции.
2. Находим (примерно) точку пересечения функции с осью абсцисс.
3. Берём небольшой отрезок на оси абсцисс таким образом, чтобы эта точка находилась внутри выбранного отрезка.
4. Вычисляем значения функций от аргументов, равных «левой» и «правой» границе отрезка – $\varphi(a_k)$ и $\varphi(b_k)$, где a_k – «левая» граница отрезка; b_k – «правая» граница отрезка; k – номер итерации.
5. Вычисляем коэффициенты:

$$\nu_{a,k} = \frac{|\varphi(a_k)|^{-1}}{|\varphi(a_k)|^{-1} + |\varphi(b_k)|^{-1}}; \quad \nu_{b,k} = \frac{|\varphi(b_k)|^{-1}}{|\varphi(a_k)|^{-1} + |\varphi(b_k)|^{-1}}.$$

Причем найденные коэффициенты должны удовлетворять следующему условию: $\sum_{i=1}^{2} \nu_i = 1$.

6. Вычисляем приближенное решение с учетом найденных коэффициентов: $u_k = \nu_{a,k} \cdot a_k + \nu_{b,k} \cdot b_k$.

7. Вычисляем значение функции от u_k.

8. В зависимости от знака полученного значения функции поступаем следующим образом:

а) Если функция возрастающая, то

$$a_k = \begin{cases} a_{k-1}, \text{ если } y_k > 0; \\ u_k, \text{ если } y_k < 0; \end{cases} \qquad b_k = \begin{cases} u_k, \text{ если } y_k > 0; \\ b_{k-1}, \text{ если } y_k < 0. \end{cases}$$

б) Если функция убывающая, то

$$a_k = \begin{cases} a_{k-1}, \text{ если } y_k < 0; \\ u_k, \text{ если } y_k > 0; \end{cases} \qquad b_k = \begin{cases} u_k, \text{ если } y_k < 0; \\ b_{k-1}, \text{ если } y_k > 0. \end{cases}$$

В обоих случаях получаем новые a_k и b_k, т.е. новый отрезок, который меньше предыдущего и который также содержит точку пересечения функции с осью абсцисс.

Повторяем п. 4–8 до тех пор, пока не найдем корень уравнения с нужной нам точностью (точность с каждой итерацией увеличивается).

Некоторые результаты экспериментальных исследований и сравнение МДОП и ММДОП представлены в таблице.

Результаты экспериментальных исследований

Вид уравнения	Отрезок	Количество итераций		Вычисленное решение	
		ММДОП	МДОП	ММДОП	МДОП
Заданная точность: $1 \cdot 10^{-4}$					
$3^x + 2x - 2 = 0$	[0; 1]	5	15	0,3027	0,3027
$(x-2)\cos x = 1,$ $-2\pi \le x \le 2\pi$	[–5; –3]	5	18	–4,5593	–4,5593
	[–3; 0]	4	19	–1,8346	–1,8346
	[4; 6]	4	16	5,0468	5,0468
$2\operatorname{arctg} x - 3x + 2 = 0$	[1; 2]	4	15	1,2689	1,2689
$\left[\log_2(x+2)\right](x-1) = 1$	[–1,5; 0]	9	16	–1,2638	–1,2638
	[0; 2]	5	16	1,5474	1,5474
$\sin(x - 0,5) - x + 0,8 = 0$	[1; 2]	6	15	1,7485	1,7485
$2e^x + 3x + 1 = 0$	[–2; 0]	6	16	–0,6733	–0,6733
$\cos(x + 0,3) = x^2$	[–1; 0]	4	17	–0,9065	–0,9065
	[0; 1]	6	17	0,7222	0,7222
$3^{x-1} - 4 - x = 0$	[–5; –3]	2	16	–3,9959	–3,9959
	[2; 3]	6	15	2,7363	2,7363
$2x^3 - 9x^2 - 60x + 1 = 0$	[–4; –3]	5	16	–3,6828	–3,6828
	[–1; 1]	5	17	0,0166	0,0166
	[6; 9]	5	16	8,1662	8,1662
$5\sin x = x - 1$	[–3; –2]	6	18	–2,3952	–2,3952
	[–1; 1]	4	16	–0,2534	–0,2534
	[2; 3]	3	17	2,7780	2,7780

Заключение. Представленные выше результаты исследований МДОП и ММДОП позволяют заключить, что количество итераций, необходимых для вычисления решений u_k с заданной точностью (с погрешностью, не превышающей заданного значения Δu) при использовании ММДОП оказывается значительно меньше, чем в случае использования МДОП.

Применение ММДОП более предпочтительно по сравнению с МДОП во всех тех случаях, когда наряду с отмеченными выше важнейшими свойствами используемый метод решения нелинейных уравнений должен обеспечивать более высокую скорость сходимости вычисляемых решений к истинным решениям данных уравнений.

БАЗА ДАННЫХ И УСТРОЙСТВО ОТОБРАЖЕНИЯ ЛАЗЕРНОГО БЕСПРОВОДНОГО УРОВНЕМЕРА (ЛБУ)

А.С. Туратпаева, магистр каф. ЭМИС

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

г. Томск, ТУСУР, alima_turatpaeva@mail.ru

В современных промышленных технологических процессах необходим контроль количественных характеристик и расхода сырья в различных местах хранения.

Задачи, требующие измерения уровня различного сырья, исключительно многообразны и встречаются в различных областях техники. Измерение уровня требуется в большинстве производственных процессов; в системах экологического мониторинга и безопасности; для учета массы, расхода при их хранении и транспортировке. Актуальность измерения уровня различного сырья возрастает по мере повышения степени автоматизации производственных процессов, систем контроля и учета [1].

Рис. 1. Пример интерфейса уровнемера

Немаловажной задачей в измерении уровня является оболочка визуализации информации об уровне наполнения резервуаров, которая отображает информацию об объеме хранимого продукта, о движении продукта, аварийных ситуациях и т.д. Пример внешнего интерфейса приведен на рис. 1 [2].

В процессе разработки приложения визуализации уровнемера будут учтены общие требования к пользовательским интерфейсам [3]:

1) физическая согласованность относится к использованию аппаратных средств (в данном случае – клавиатура и мышь) и подразумевает использование одинаковых последовательностей действий при выполнении одинаковых операций;

2) синтаксическая согласованность относится к порядку появления элементов интерфейса на экране и к терминам, применяемым для обозначения команд и функций.;

3) семантическая согласованность относится к значениям элементов интерфейса.

Выполнение требований согласованности обеспечивает:

1) снижение трудоемкости реализации проекта за счет использования типовых решений;

2) выработку у пользователя единых представлений и навыков при работе с системой, снижение количества вопросов и ошибок;

3) сокращение описательной части документации.

Учитывая тот аспект, что практически вся отображаемая информация хранится в базе данных и вся информация передается в реальном времени, то целесообразно было использовать новый способ поиска данных, позволяющий получать данные быстрее по сравнению с использованием уже имеющихся методов и способов в больших объемах данных.

В данной работе применяется новый способ поиска в базах данных. Этот метод представлен системой NBITSearch, программным ядром для системы управления базами данных, хранилищ данных большого объема, поисковых систем любых объектов [4].

Система назначена для компактного индексирования больших массивов данных на жестком диске, организующем скоростной четкий и нечеткий поиск объектов при минимальных затратах оперативной памяти. Скорость выборки результатов диапазонных запросов с жесткого диска может быть в 10–100 раз выше (в большом массиве данных), чем аналогичная скорость в стандартных реляционных СУБД, и может быть в 1000 раз выше (также в большом массиве данных), чем аналогичная скорость в решениях полным перебором. Время выборки результатов линейно зависит от числа объектов, попадающих в результирующее множество [4].

Автором были проведены сравнительные работы различных интерфейсов систем измерения уровней веществ, предложены динамический интерфейс, логическая структура базы данных, а также использован новый способ быстрого поиска.

ЛИТЕРАТУРА

1. Измерение уровня жидких продуктов: теория и практика [Электронный ресурс]. Режим доступа: http://www.3v-engineering.ru/information/1/3/, свободный. Загл. с экрана.

2. Оболочка визуализации ResViewer [Электронный ресурс]. Режим доступа: http://www.limaco.ru/ru/production/102/123/, свободный. Загл.с экрана.

3. Требования к разработке пользовательских интерфейсов/ Корпоративный стандарт, редакция 4.0 от 21.12.2005, с дополнениями от 06.08.2007 и 14.11.2008.

4. Индексирование и быстрый поиск [Электронный ресурс]. Режим доступа:http://www.nbitsearch.com/Articles/NBITSearch%20parameters%20RU.pdf, свободный. Загл. с экрана.

МОДЕРНИЗАЦИЯ КОНСТРУКЦИИ РАДИОНАВИГАТОРА

А.В. Южаков, студент каф. КИБЭВС

Руководитель А.М. Глущенко, вед. инженер-конструктор

ОАО «ИСС им. М.Ф. Решетнёва»

г. Томск, ТУСУР, artem.tghcd@gmail.com

Предметом разработки является модернизация конструкции радионавигатора, основной задачей которого является определение координат космического аппарата, на котором он установлен. Входными данными являются сигналы от спутниковых систем ГЛОНАСС и GPS.

Значительное внимание при разработке было уделено уменьшению массы блока при неизменных показателях прочности конструкции. Это было осуществлено за счет отхода от традиционных рамочных конструкций [1]: рамка, на которой установлена печатная плата, была объединена с ребрами жесткости на внешней поверхности крышки и двумя фланцами. Еще одним плюсом такого подхода является упрощение изготовления конструкции.

Компоновка была произведена с учетом стандартных требований: минимальная длина проводников, размещение мощных ЭРЭ ближе к теплопроводящему основанию [2].

Также на печатной плате были сделаны вырезы, по форме соответствующие модулям питания, с целью установки этих модулей непосредственно на алюминиевую крышку прибора. Таким образом, была увеличена теплопередача.

Соединение различных блоков было осуществлено посредством использования импортных соединителей типа D-Sub, которые значительно превосходят отечественные как по надежности, так и по количеству контактов, хотя и являются довольно дорогими.

В результате работы был разработан блок ВИП. Массогабаритные показатели радионавигаторов различных модификаций АРН сведены в таблицу.

Массогабаритные показатели приборов

Наименование модификации радионавигатора	Масса прибора, кг	Габаритные размеры блока, мм
АРН-1	7,6	180×260×210
АРН-2	7,1	180×260×210
АРН-3	3,6	176×280×200

Таким образом, масса прибора с новым блоком ВИП на данный момент составляет 3,6 кг. Благодаря использованию упомянутых изменений она уменьшилась на 3,5 кг. Ухудшение каких-либо показателей при этом не проявилось.

ЛИТЕРАТУРА

1. Жаднов В.В. Особенности конструирования бортовой космической аппаратуры / В.В. Жаднов, Н.А. Юрков. Пенза: ПГУ, 2012. 107 с.

2. Браун М. Источники питания. Расчет и конструирование. К.: МК-Пресс, 2007. 267 с.

ЗАРЯДНО-РАЗРЯДНОЕ УСТРОЙСТВО ЭНЕРГОПРЕОБРАЗУЮЩЕГО КОМПЛЕКСА

С.С. Безносиков, студент 5-го курса, каф. КИБЭВС

Руководитель С.М. Мельников, вед. инженер-констуктор ОАО «ИСС»

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

Геостационарные спутники выполняют на сегодняшний день множество задач, таких как: телекоммуникация, радиоместоопределение (системы навигации GPS, ГЛОНАСС и др.), главной задачей большинства геостационарных спутников является формирование изображений видимой земной поверхности. Спутниковые системы связи с геостационарными спутниками-ретрансляторами идеально подходят для решения таких задач, как организация телевизионного и звукового вещания на обширных территориях и предоставление высококачественных телекоммуникационных услуг абонентам в удаленных и труднодоступных регионах. Кроме того, с их помощью можно быстро создавать крупномасштабные корпоративные сети и резервировать наземные магистральные каналы связи большой протяженности. Также сейчас проводится создание мультисервисных сетей (объединяющих в едином пакете такие услуги, как передача данных, телефония, цифровое телевидение, видеоконференция и доступ в Интернет) на основе

технологии VSAT. Если учесть особенности нашей страны, где во многих районах только спутниковые системы обеспечивают населению телевидение и радиовещание, а также услуги связи, то становится очевидной необходимость разработки новых станций спутниковой связи с возможностью передачи больших потоков информации.

Увеличение энергопотребления современных спутниковых систем создает необходимость увеличения мощности питания.

Питание всех узлов спутника производится либо от солнечной батареи (на солнечном участке), либо от аккумуляторной батареи спутника (на теневом участке траектории движения спутника). Для непрерывного функционирования спутника необходимо бесперебойное питание всех систем и устройств.

КЭП совместно с БС и АБ образуют автономную систему электропитания, обеспечивающую стабилизацию напряжения на шинах 100 и 27 В с заданным качеством во всех штатных режимах работы и диапазонах нагрузок и совместное функционирование БС и АБ.

Основными узлами КЭП являются:

– Шунтовой стабилизатор, формирующий шину 100 В.

– Стабилизатор напряжения, формирующий шину 27 В.

– Зарядно-разрядное устройство, обеспечивающее разряд и заряд АБ при избытке мощности БС.

Целью работы является разработка зарядно-разрядного устройства (ЗРУ) модульного комплекса энергопреобразующего (КЭП) для использования в составе системы электропитания (СЭП) геостационарных космических аппаратов.

Основные требования при проектировании РЭС состоят в том, чтобы создаваемое устройство было эффективнее своего аналога или прототипа, то есть превосходило его по качеству функционирования, степени миниатюризации, мощности и технико-экономической целесообразности.

Современные методы конструирования должны обеспечивать:

– уменьшение объема и массы;

– расширение области использования микроэлектронной базы;

– увеличение степени интеграции, миниатюризацию межэлементных соединений и элементов несущих конструкций;

– электромагнитную совместимость;

– широкое внедрение методов оптимального конструирования;

– максимальное использование стандартизации.

Конструкция блока должна обеспечивать устойчивость к нагрузкам при наземной эксплуатации, транспортировании и запуске без нарушения работоспособности.

Корпус должен быть легким и обеспечивать нормальный тепловой режим работы прибора;

Печатный узел закрепляется на теплопроводящую раму, обеспечивающую отвод тепла от печатной платы. Внутри теплопроводящей рамы встроена тепловая труба, обеспечивающая распределение температуры по всему объему рамы. Теплопроводящая рама большей стороной крепится к основанию корпуса конструкции для отвода тепла.

Все приборы КЭП устанавливаются на центральную сотовую панель платформы КА. Тепловой режим приборов обеспечивается за счет термостатирования их посадочных мест с помощью двух резервированных жидкостных контуров СТР, встроенных в сотовую панель. Жидкостной коллектор контролирует температуру устройства в целом.

ЛИТЕРАТУРА

1. Соколов В.В., Могучев В.И., Пыльцов В.А., Фомин А.Н. Оценка возможностей систем спутниковой связи с различными видами орбит космических аппаратов / Зарубежная радиоэлектроника. 1996. №2.

2. Комплекс энергопреобразующий. Техническое описание. Платформа «Экспресс-1000Н». Подсистема терморегулирования. Спецификация.

СИСТЕМА НАКОПЛЕНИЯ ЗНАНИЙ

И.В. Ботнаренко, Я.К. Кротов, И.С. Куренков, Д.С. Терентьев, студенты каф. КИБЭВС

Научный руководитель Е.М. Давыдова, доцент, к.т.н.

г. Томск, ТУСУР, ФВС, SertyRUS@gmail.com

Проект ГПО ФВС-1207 – «Система накопления знаний»

О необходимости пересмотра существующей системы контроля результатов обучения давно известно и немало сказано.

Создать стимулы активизации самостоятельной работы студентов, упорядочить требования преподавателей к уровню знаний, вовремя измерять успеваемость и т.д. – все это может быть достигнуто при использовании рейтинговой системы.

Целью данной работы является создание рейтинговой системы студентов, являющейся основой оперативного контроля обученности студентов. Разработка этой системы проводилась на примере кафедры КИБЭВС Томского государственного университета систем управления и радиоэлектроники (ТУСУР).

В соответствии с этим выделены следующие важнейшие задачи, стоящие перед нами в процессе выполнения работы:

- анализ учебного плана по специальностям КОИБАС и ПиТЭВС;
- изучение и выбор метода расчета рейтинга;

- анализ информации об оценках студентов;
- создание структуры базы данных рейтинговой системы студентов;
- визуализация на сайте рейтинговой системы студентов.

В федеральном государственном образовательном стандарте главным является то, что дисциплины разделены на циклы (гуманитарный, математический и т.д.). В учебном плане наиболее важны следующие данные: периоды экзаменационных сессий, продолжительность дисциплин и отчетность по каждой дисциплине.

В результате анализа учебного плана и федерального государственного образовательного стандарта было решено:

− разделить дисциплины на блоки специальностей, так как нельзя сравнивать оценки предметов из разных блоков (например, гуманитарные предметы и естественнонаучные предметы);

− внутри блоков специальностей для каждой дисциплины рассчитывается коэффициент трудности дисциплины: количество часов этой дисциплины делится на количество часов самого продолжительного предмета в блоке;

− олимпиады, научно-исследовательские работы, спортивные достижения, конференции, и т.д. на рейтинг не влияют, дынные о них заносятся в виде дополнительной информации о студенте.

В итоге нам необходимы следующие данные:

- специальность;
- название дисциплин;
- блоки специальностей (название и входящие дисциплины);
- количество часов каждой дисциплины;
- отчетность по дисциплине;
- семестр(-ы), в котором(-ых) изучается дисциплина;
- данные о практиках (учебных или производственных).

Метод расчета среднего арифметического показателя – один из наиболее распространённых способов центральной тенденции, представляющий собой сумму всех наблюденных значений, деленную на их количество. От данного метода пришлось отказаться, так как он не может более компетентно выразить точность рейтинговой отметки.

Метод расчета моды – значение во множестве наблюдений, которое встречается наиболее часто. При экспертной оценке с её помощью определяют наиболее популярные типы продукта, что учитывается при прогнозе продаж или планировании их производства. Данный метод не подходит для расчета рейтинга, так как наиболее повторяющиеся оценки не могут служить основательным доводом к определению знаний студента.

Изучив всевозможные методики расчета рейтинга, был сделан свой метод расчета рейтинга студентов, который был назван как метод «медианы». Для расчета рейтинга методом «медианы» необходимо

сначала вычислить коэффициент трудности предмета (коэффициент трудности = количество часов одного предмета / количество часов самого большого предмета (в блоке)). Затем умножить коэффициент трудности на предметную оценку за конец сессии. Получившиеся оценки одной группы специальности записать в ряд и взять медиану (посередине). Отсюда и название метода, метод «медианы».

Оценки, выставленные по результатам сессии, определяются следующим образом:

– зачет кодируется: 1 – если студент сдал, 0 – если нет;

– экзамен кодируется по 5-балльной шкале;

– курсовая работа кодируется по 5-балльной шкале.

При анализе информации об оценках было изучено три метода занесения оценок в базу данных:

1) с помощью библиотеки PHPExcel;

2) с помощью конверторов;

3) просто создать в базе данных отдельную таблицу, которая хранит все оценки.

Первый метод, который был рассмотрен, это был метод передачи данных с помощью библиотеки PHPExcel. Что же такое PHPExcel? PHPExcel – отличная библиотека с огромным функционалом по работе с форматами xls, xlsx. Можно считывать, записывать, менять форматирование, задавать формулы, а из xlsx можно и картинки вытаскивать. Форматом чтения не ограничиваются файлами Excel, он также может прочитать такие файлы как Excel 2007, BIFF5 (Excel 5.0/Excel 95), BIFF8 (Excel 97 и более поздние), PHPExcelSerializedSpreadsheet, SymbolicLink, CSV. Также с помощью этой библиотеки мы можем сохранять данные в другом формате, например PDF. Минус этого метода то, что PHPExcel очень требователен к памяти. Для одной ячейки надо около 1 КБ памяти. При работе с большими таблицами вы можете столкнуться с определенными трудностями.

Второй метод, который был рассмотрен, это был метод передачи данных помощью конверторов, т.е. для простоты передачи данных потребуется поменять формат Excel на формат CSV. Для быстрого импорта данных в MySQL используется следующее так называемое выражение манипулирования данными «LOAD DATA INFILE».

Проблемы быстрого импорта данных заключаются в том, что при использовании запроса «LOAD DATA INFILE» вы должны учитывать следующее:

- у пользователя БД должна быть привилегия FILE, но не всякий хостинг позволяет менять привилегии пользователя;
- может возникнуть проблема вставки строк с отсутствующими значениями;
- остаётся проблема загрузки больших файлов.

Также следует заметить, что если используется LOCAL:

1) необходимо разобраться с путём к файлу: абсолютный или относительный. Относительный – это относительно клиента – путь, откуда клиент был запущен;

2) если передачу файла ведёт клиент, то сохраняется его копия во временном каталоге не сервера БД, а операционной системы и читается сервером БД уже оттуда (БД необходимо обеспечить доступ к каталогу и свободное место на диске);

3) команда отработает, только если и сервер, и клиент разрешают её. Например, на сервере должна быть установлена переменная – local-infile=1.

Если LOCAL не используется:

1) БД читает файл по абсолютному пути;

2) если путь относительный, то от пути директории данных сервера или директории текущей базы данных. Всё решает наличие или отсутствие «./» перед файлом. Всё же могут возникнуть проблемы с доступом. Если файл вдруг находится не в каталоге текущей БД, то надо переключиться, используя USE, а потом не забыть переключиться назад;

3) если установлена системная переменная secure_file_priv, то файл должен находиться по указанному в ней пути.

На основании анализа выявлено, что первые два метода не подходят, был сделан вывод, что можно просто создать отдельную таблицу в базе данных и самостоятельно вводить данные. Оценки предоставляются в электронном виде Excel секретариатом кафедры КИБЭВС.

Для реализации данной рейтинговой системы студентов необходимо создать соответствующую базу данных. В качестве предметной области была выбрана «Система накопления знаний». В базе данных хранится информация о студентах и их оценках. Также в БД находится информация о блоках специальностей, входящих в них дисциплинах, количество часов каждого предмета и вид отчетности по этому предмету. Имеется информация о специальности, на которой обучается студент, а также о личных заслугах каждого студента, таких как участие в олимпиадах, публикациях, спортивных мероприятиях и т.д.

Данная система расчета рейтинга будет отображена на сайте кафедры КИБЭВС (keva.tusur.ru). Сайт кафедры разработан на Drupal.

Сценарий работы: пользователь заходит на сайт кафедры КИБЭВС. Переходит в раздел «Студент» и во вкладку «Рейтинг студентов». После успешного выполнения данной операции появляется строка поиска, в которую пользователь должен ввести фамилию, имя и номер группы. Результатом поиска должна стать информация о студенте:

– фамилия, имя и отчество;

– фото (необязательно);
– номер группы;
– специальность;
– гистограмма, созданная на основе данных рейтинга;
– дополнительные заслуги студента (олимпиады, проекты и т.д.).

Студенты могут не только посмотреть свой рейтинг, но и сравнить его с рейтингом других студентов.

При этом отметим, что пользователями для данной системы будут являться не только студенты, но и их родители, которые волнуются, переживают и интересуются успеваемостью своего ребенка, а также работодатели, которые заинтересованы в поиске работников по своим определенным критериям. Для всех этих пользователей будет создан свой персональный интерфейс.

В итоге данная система предназначена не только для учета успеваемости, но и для поиска подходящего работодателя, для начала успешного будущего.

Главное отличие нашего сайта от сайта «Оценка» состоит в том, что рейтинг студентов отображается в виде столбцовой диаграммы. Наша система позволяет работодателям находить студентов с самыми высокими баллами по нужной им специальности. Также наша система предоставляет возможность студентам сравнивать свои показатели в учебе с другими студентами.

ЛИТЕРАТУРА

1. Диканская Н.Н. Оценочная деятельность как основа управления качеством образования // Стандарт и мониторинг в образовании. 2003. №3.

2. Костылев Ф.В.. Учить по-новому: нужны ли оценки-баллы. М., 2000.

3. О показателях качества образования // Высшее образование в России. 2004. №11. С. 92–96

4. Рейтинговая система // Высшее образование в России. 2001. №4.

СИСТЕМА ЭЛЕКТРОПИТАНИЯ КОСМИЧЕСКИХ АППАРАТОВ С ШУНТОВЫМИ СТАБИЛИЗАТОРАМИ

Д.А. Деревянкин, студент каф. КИБЭВС

Руководитель М.И. Сараев, вед. инженер-конструктор

ОАО «ИСС им. М.Ф. Решетнёва»

г. Томск, ТУСУР, ФВС, q.sky.high@gmail.com

Солнечное излучение является практически неограниченным источником энергии в космическом пространстве. Для преобразования энергии солнечного излучения в электрическую энергию на борту космических аппаратов используются солнечные батареи, эффективно

работающие при хорошем освещении. В условиях тени или затемнения солнечные батареи не производят никакой энергии. Следовательно, для обеспечения бортовых потребителей бесперебойным электропитанием необходимо запасать некоторую часть энергии, производимой солнечной батареей в период освещения, и отдавать ее в нагрузку в период тени. Таким образом, в системе электроснабжения обязательно должны входить солнечная батарея и аккумуляторная батарея. Когда космический аппарат находится на освещенной стороне Земли, солнечные батареи обеспечивают энергией потребители и перезаряжают аккумуляторы, которые, разряжаясь, питают потребители энергии все время, пока космический аппарат находится в тени [1].

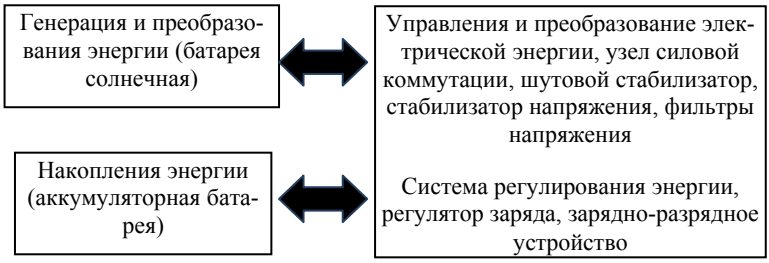


Рис. 1. Важнейшие узлы типичной системы электроснабжения космического аппарата

В бортовых системах электроснабжения любого типа выходы солнечной и аккумуляторной батарей должны быть включены так, чтобы обеспечить бесперебойное электропитание различных бортовых подсистем. В течение орбитального дня аккумуляторная батарея будет заряжаться, а в течение орбитальной ночи (также при пиковых нагрузках, когда нагрузочной способности солнечной батареи недостаточно) – разряжаться. Эти процессы осуществляются с помощью системы управления и преобразования энергии.

По принципам работы СУПЭ подразделяются на два класса:

– рассеивающие системы, не отбирающие от солнечной батареи максимальную мощность. В таких СУПЭ избыточная энергия, производимая солнечной батареей и не используемая бортовыми подсистемами, рассеивается в параллельном стабилизаторе;

– нерассеивающие системы, в любой момент времени отбирающие от солнечной батареи максимальную мощность благодаря наличию следящего преобразователя.

Система электропитания (СЭП) является одной из важнейших частей в составе оборудования спутника, обеспечивая энергией все его служебные системы и полезную нагрузку космической аппаратуры.

Важнейшими характеристиками СЭП являются качество выходного напряжения, масса, габариты, КПД, надежность и стоимость.

Одним из способов достижения требуемого качества является использование оптимальной структуры энергопреобразующей аппаратуры (ЭПА), входящей в состав СЭП.

В настоящее время существует ЭПА, предназначенная для работы с 6, 18 и 40 секционными БС. В такой аппаратуре использованы шунтовые стабилизаторы с широтно-импульсным модулятором силового ключа, причем число шунтовых стабилизаторов равно числу секций солнечной батареи. При реальной работе большинство каналов шунтового стабилизатора либо полностью закорачивают секцию солнечной батареи, либо пропускают весь ток в нагрузку. То есть фактически большинство каналов работает в дискретном режиме. При этом конструкция всех шунтовых стабилизаторов одинакова, в результате этого появляется большое количество избыточных элементов, приводящее к усложнению и удорожанию конструкции ЭПА [2].

ЛИТЕРАТУРА

1. Четти П. Проектирование ключевых источников электропитания. М., 1990. 240 с.

2. Варламова Р.Г. Справочник конструктора РЭА. Общие принципы конструирования. М., 1980. 480 с.

УСТРОЙСТВА ПЕРЕНОСА РИСУНКА В ПРОИЗВОДСТВЕ ПЕЧАТНЫХ ПЛАТ

К.И. Чугаевский, А.В. Леонидов, студенты каф. КИБЭВС

Научный руководитель Л.А. Торгонский, доцент

г. Томск, ТУСУР, Inexcitus@live.ru

Целью представляемой работы является создание установки переноса рисунка проводников на печатную плату (ПП) для последующего травления. К переносу изображения плата должна быть подготовлена очисткой поверхности от загрязнений и жировых пятен. При наличии на заготовках плат визуально наблюдаемой тёмной оксидной пленки её следует удалить травлением в течение 3–5 с раствором хлорного железа с последующей промывкой в проточной воде и сушкой. Очистка и сушка платы производяится перед переносом рисунка проводников с максимальным сроком хранения в затемнённом сухом месте не более 4 часов.

Качество переноса изображения на 90% определяет качество изготовленной платы. Распространёнными методами переноса изображений на печатные платы являются [1]:

– метод масочной шелкографии;

– метод фотолитографии (с применением жидких и твёрдых, негативных и позитивных фоторезистов);

– метод термопереноса.

Метод термопереноса является наименее затратным, но критичным к браку переноса рисунка. Тем не менее им широко пользуются в производстве ПП. Альтернативой для применения в производстве плат является метод фотолитографии с плёночными (сухими) фоторезистами [1, 2].

В работе рассматриваются технические средства переноса изображений на ПП методом фотолитографии. Упрощённая схема установки представлена на рис. 1.

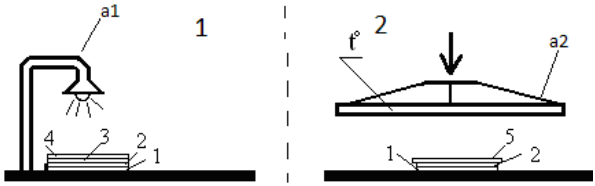


Рис. 1. Схема установки

Установка предусматривает средства для засветки и операции прогрева на отдельных этапах процесса. В схеме выделяются 2 технологические зоны. В зоне 1 выполняется облучение печатной платы в ультрафиолетовом диапазоне спектра. Подсветка осуществляется светильником a1. Контролю подлежат частота спектра облучателя, расстояние до платы от источника, время экспозиции при засветке. Место оборудовано ограничительными фиксаторами для фиксации пакета с заготовкой ПП.

В зоне 2 выполняется подогрев ПП с экспонированным фоторезистом через буферную тепловую прокладку (*5*) под регулируемым давлением. При подогреве контролируется температура прижимающей тепловой плиты a2 (100–120º), давление прижима и время подогрева 2–10 с.

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

После экспонирования с пакета снимаются прижимная пластина и фотошаблон. На остаток пакета прокладывается прокладка из гладкой бумаги и в зоне 2 подвергается контролируемому прогреву для задубливания фоторезиста. После задубливания и визуального контроля на отсутствие дефектов плата передаётся на выполнение проявления и последующих прочих операций химической обработки.

Габаритные размеры модуля экспонирования определяются высотой разборного светильника а1 и размерами площадки под фиксацию пакета с экспонируемой платой 250×250 мм. На площадке установлен разъём для подключения электронного блока контроля освещённости пакета и управления светильником а1.

Габаритные размеры модуля прогрева при задубливании фоторезиста по высоте в поднятом состоянии нагревающей плиты не превышает 120 мм. Размеры площадки основания модуля прогрева и модуля экспонирования равны. Модуль прогрева пакета через разъем подключается к электронному блоку контроля давления, температуры и управления временем термоэкспозиции. Модулю придаётся вентилятор охлаждения нагревательной плиты после прогрева. Допустим вариант исполнения модуля с применением комплектного специализированного ламинатора для прогрева экспонированного пакета с встроенным блоком индикации и управления, специфицированными габаритами и собственной упаковкой.

Электронный блок контроля и управления выполнен автономным и подключается к модулям устройства гибкими шлейфами через разъёмы, установленный на основаниях модулей. На рис. 1 электронный блок контроля и управления, как и вентилятор, не показаны.

Полезные к проектированию устройств сведения по процессам и материалам, связанным с технологией и технологическим оснащением оборудования обработки ПП, приведен в [2].

Установка находится в процессе подбора, отработки и изготовления узлов конструкции.

ЛИТЕРАТУРА

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

2. Avislab [Электронный ресурс]. http://www.avislab.com

СЕКЦИЯ 18

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель секции – **Шелупанов А.А.**, проректор по НР ТУСУРа, зав. каф. КИБЭВС, д.т.н., профессор,*
*зам. председателя – **Конев А.А.**, доцент каф. КИБЭВС, к.т.н.*

СТЕГАНОГРАФИЯ С ИСПОЛЬЗОВАНИЕМ ИЗОБРАЖЕНИЯ В КАЧЕСТВЕ КОНТЕЙНЕРА

М.А. Ананев, А.Е. Анфилофьев, К.С. Крючков, А.А. Онищенко, студенты
Научный руководитель Е.М. Давыдова, доцент, к.т.н
г. Томск, ТУСУР, каф. КИБЭВС, makernew@mail.ru
Проект ФВС КР.71801-018101

Информация является одним из ценнейших предметов современной жизни. Получение доступа к ней с появлением глобальных компьютерных сетей стало невероятно простым. В то же время легкость и скорость такого доступа значительно повысили и угрозу нарушения безопасности данных при отсутствии мер относительно их защиты, а именно угрозу несанкционированного доступа к информации.

Актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации. Современные компьютерные технологии, прогресс в области глобальных компьютерных сетей и средств мультимедиа обеспечивает возможность разработки и реализации новых методов, предназначенных для обеспечения компьютерной информационной безопасности. Компьютерные технологии придали новый импульс развитию и совершенствованию такого направления в области защиты информации, как компьютерная стеганография.

В настоящее время в связи с широким распространением цифровой фототехники и мониторов высокого разрешения в глобальной сети Интернет появляется все больше высококачественных графических файлов. Такие файлы очень хорошо подходят на роль стегоконтейнеров для скрытой передачи личных сообщений (рис. 1, 2).

Стеганография применяется в таких областях, как защита личной тайны, цифровые водяные знаки, электронная цифровая подпись и электронная торговля [1].

В данной работе показаны результаты завершенного проекта. В качестве методов стеганографических преобразований были выбраны: метод LSB или метод наименьших значащих битов, метод квантования, метод Куттера–Джордана–Боссена, метод Коха–Жао, метод Бенгама–Мемона–Эо–Юнга. Для каждого из методов программа высчитывает количество символов, которое можно «встроить» в сообщение, а также предоставляет выбор для таких функций, как знак конца сообщения или смещения.

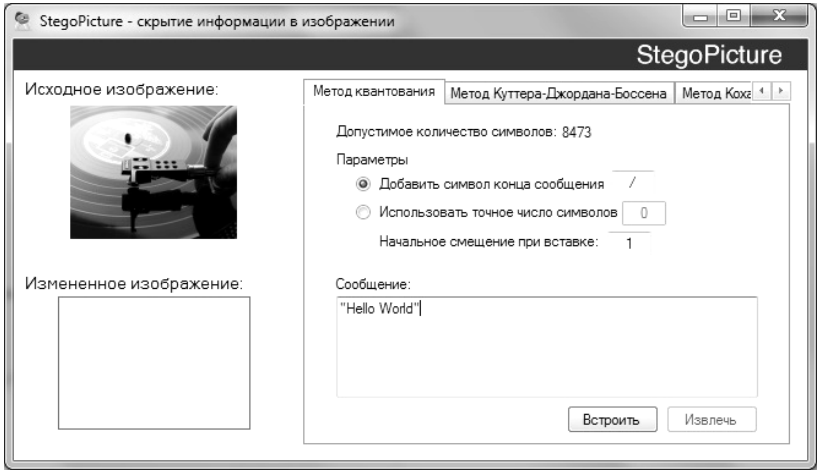


Рис. 1. Встраивание сообщения в стегоконтейнер

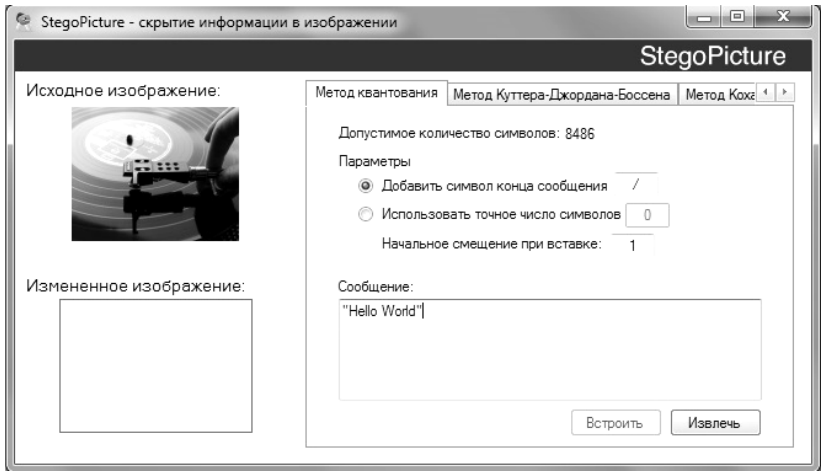


Рис. 2. Результат извлечения сообщения из стегоконтейнера

ЛИТЕРАТУРА

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стаганография. Аспекты защиты. М.: Солон-Пресс, 2002.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М.: МК-Пресс, 2006г.

3. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовая книга, 2009.

4. Саймон Сингх. Книга шифров. Тайная история шифров и их расшифровки: Пер. А. Галыгин. М.: АСТ, Астрель, 2007.

АНАЛИЗ ЖУРНАЛОВ ОПЕРАЦИОННЫХ СИСТЕМ И ПРИЛОЖЕНИЙ

М.М. Антонов, Е.И. Литвинцев, А.В. Моргуненко, Д.С. Никифоров, И.Ю. Поляков, А.И. Пономарев, студенты

Научный руководитель А.И. Гуляев, аспирант

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

Компьютерно-техническая экспертиза (КТЭ) является классом инженерно-технических экспертиз, проводимых в целях поиска криминалистически-значимой информации на носителях, ее всестороннего исследования, и, как следствие, получения доказательственной информации и установления фактов, имеющих значение для уголовных, гражданских и административных дел, сопряженных с использованием компьютерных технологий. Для получения базовых знаний в этой области мы выделили несколько направлений:

- Unix-системы.
- Восстановление данных цифровых носителей.
- Основы анализа сетевого трафика.
- Криптографические методы защиты информации.
- Web-серверы.

На основе полученных знаний были написаны статьи, объединенные общей тематикой «Компьютерная экспертиза».

При изучении данных материалов мы сделали вывод, что основной задачей при проведении компьютерной экспертизы является поиск и анализ журналов событий операционной системы и прикладных программ. В данных файлах содержится много информации о том, что, кто и когда делали при помощи какого-либо программного средства. Например, по файлам истории интернет браузера можно определить, какие ресурсы и в какое время посещались, по журналу событий операционной системы – понять какие приложения запускались, или же выявить все ошибки работы приложений.

Продолжая двигаться в данном направлении, мы занялись поиском различных лог-файлов, изучали их структуру, выделяли информативные записи и собирали из них общую картину того, что происходило с данным компьютером в определенные отрезки времени, или же узнать содержание какой-либо переписки.

Проблема состояла в том, что данные файлы хранятся в разных местах и имеют различную структуру, это усложняет поиск файлов и их прочтение. Существуют различные программные средства для чтения различных лог-файлов, но они узко специализированы, и пути к интересующим нас файлам необходимо указывать вручную (например Log Monitor или Zabbix-Agent). Также неудобно то, что содержимое файлов не фильтруется, то есть все пометки, необходимые исключительно для системы, выводятся на экран и затрудняют анализ информации.

Для упрощения задачи анализа скриптов unix-систем были написаны sh-скрипты, которые автоматически выделяли из лог-файлов необходимую нам информацию и собирали их в один простой файл .txt – сортировка по временным меткам. В дальнейшем подобные средства были реализованы для систем WINDOWS и их приложений. Автоматизирована система поиска лог-файлов.

ЛИТЕРАТУРА

1. Федотов Н.Н. Форензика – компьютерная криминалистика. М.: Юридический мир, 2007.

2. Mendel Cooper. Advanced Bash-Scripting Guide. Искусство программирования на языке сценариев командной оболочки / Пер. А. Киселев.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА «АНОНИМНЫЙ ЗВОНОК»

А.А. Чичерин, студент

Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, chicherin.and@gmail.com

Предложена методика сокрытия признаков, которые могут быть использованы для определения личности абонента при совершении телефонных звонков.

Целью работы является создание автоматизированной системы (АС), с помощью которой возможно совершение звонков на аппараты телефонной сети общего пользования и телефоны сотовых сетей, при которых невозможно идентифицировать лицо, совершающее звонок. Данная система может быть востребована при даче показаний в ходе судебного процесса, а также при совершении звонков частными лица-

ми, при которых они не уверены в своей безопасности, например, при звонках по телефонам доверия в различные социальные службы.

Признаками, позволяющими идентифицировать абонента, являются:

− номер абонента;

− информация, которую можно выделить из звукозаписи разговора;

− сопоставление информации о местоположении абонента с видовой информацией (например, с камер видеонаблюдения или визуальным наблюдением).

Базовой технологией выбрана VoIP, в качестве сигнального протокола используется протокол SIP, для передачи голосового потока – RTP.

Для сокрытия IP-абонента от VoIP-провайдера была реализована схема передачи данных с использованием анонимной сети I2P, представленная на рис. 1.

Программное обеспечение разрабатывалось для платформы iOS на языке программирования Objective-C с использованием библиотеки PjSIP.

В качестве алгоритма изменения голоса был выбран алгоритм сдвига частоты основного тона (pitch shift) [1], основанный на использовании быстрого преобразования Фурье, по следующим причинам:

1) существующая реализация на языке программирования C [2];

2) успешное применение данного алгоритма в реальном времени, реализованное на платформе iOS [3].

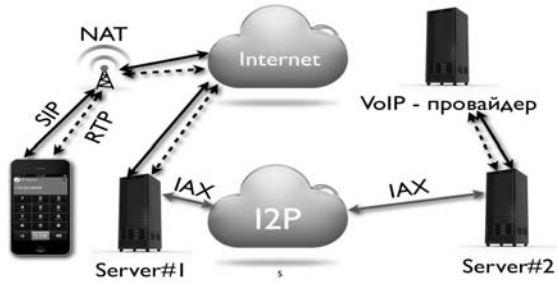


Рис. 1. Схема АС с использованием I2P

Для возможности дальнейшего анализа производится запись как оригинального голосового потока, так и после применения эффекта «pitch shift».

Графики, полученные с помощью свободно распространяемого ПО «praat» [4], представлены на рис. 2.

Заключение. Было разработано ПО, позволяющее искажать голос при совершении телефонных звонков. Реализована конфигурация АС с использованием анонимной сети I2P, позволяющая скрывать местоположение абонента.

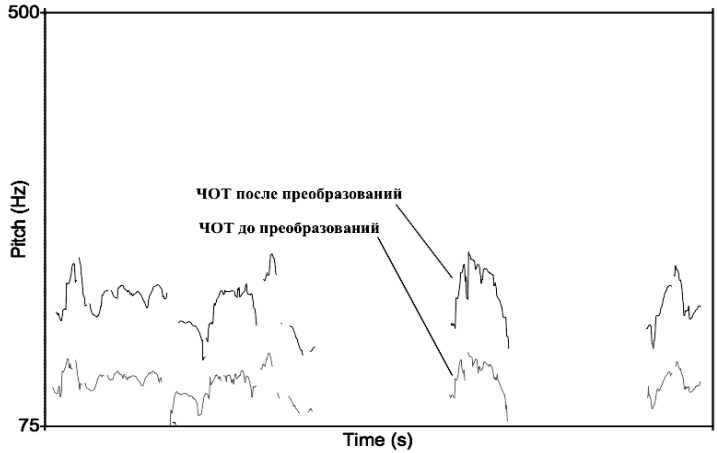


Рис. 2. Частота основного тона

ЛИТЕРАТУРА

1. Жернило В.Р. Компьютерная фоноскопия. М.: Академия МВД России, 1995. 203 с.

2. Pitch Shifting Using The Fourier Transform [Электронный ресурс]. Режим доступа: http://www.dspdimension.com/admin/pitch-shifting-using-the-ft/, свободный. Яз. англ.

3. AudioGraph [Электронный ресурс]. Режим доступа: https://github.com/tkzic/audiograph, свободный. Яз. англ.

4. Praat [Электронный ресурс]. Режим доступа: http://www.fon.hum.uva.nl/praat/, свободный. Яз. англ.

ПРИМЕНЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОЭНЕРГЕТИКЕ НА ПРИМЕРЕ ОАО «ТЮМЕНЬЭНЕРГО»

Н.В. Чижов, студент каф. КИБЭВС

г. Томск, ТУСУР, ФВС, chizov.nv@yandex.ru

Электроэнергетика – отрасль энергетики, включающая в себя производство, передачу и сбыт электроэнергии [1]. Компании, занимающиеся сбытом электроэнергии, включают в себя как минимум следующие элементы, образующие систему информационной безопасности:

1) межсетевой экран;

2) антивирусное ПО;

3) система предотвращения\обнаружения вторжений;

4) подсистема управления электронными правами доступа;

5) подсистема централизованного управления доступа к портам компьютера.

Информация – это актив, который имеет ценность [2]. Активом, имеющим ценность, являются данные, составляющие конфиденциальную информацию. Актуальной проблемой является организация среды обработки конфиденциальной информации, в которую будет входить подсистема управления электронными правами доступа к конфиденциальной информации. Такая подсистема позволяет реализовать централизованную политику управления электронными правами с возможностью делегирования части полномочий ответственным лицам.

Oracle Information Rights Management 10g – это одно из интересных Enterprise решений на рынке тем, что компания Oracle разработала технологию, которая позволяет контролировать информацию везде, где она хранится и используется [3]. Следует отметить и тот факт, что Oracle IRM решает проблему управления вне репозитория.

а) Если документы или почтовые сообщения являются собственностью компании, запечатаны, то они защищены от подделки. Если необходимо удалить документ, то оно может быть изъято с помощью удаления ключа аутентификации с сервера Oracle.

б) Версии. На сервере запретить работу с документами выше определенной версии.

Также обеспечивается управление на основе классификации ролей. Это достигается IRM, обеспечивая подход по управлению доступом к большинству документов в имеющейся классификации информации. Например:

1) рабочие документы;

2) объявления компании;

3) годовая отчетность.

На рис. 1 и 2 можно продемонстрировать, как работает схема классификации ролей.

Стоит отметить процесс запечатывания. Запечатывание – это процесс наложения некой маски на файл. Маска состоит из слоя кодирования + ЭЦП + ссылки на серверы IRM.

В процессе запечатывания размер файлов увеличивается на ~1% от размера файла. Запечатанный документ имеет метку «s». 123.pdf => 123.spdf. Процесс запечатывания может быть произведен вручную или автоматически. Для того чтобы распечатать документ, необходимо иметь Oracle IRM Server, на котором находятся [3] (рис. 3).

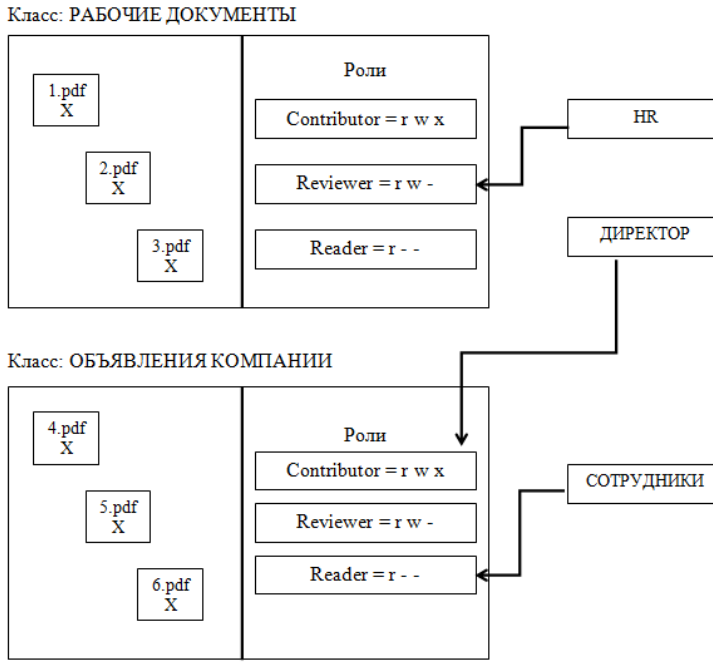


Рис. 1. Пример классификации ролей

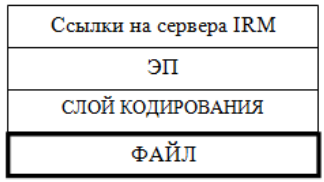


Рис. 2 Схема запечатывания

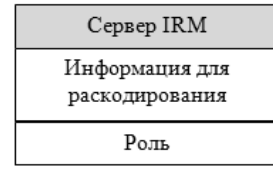


Рис. 3. Состав IRM сервера

ЛИТЕРАТУРА

1. Википедия, Свободная энциклопедия [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/;

2. ГОСТ Р ИСО/МЭК 17799-05. Информационные технологии. Средства обеспечения: Свод практики для менеджмента информационной безопасности.

3. Oracle IRM, Configuring Oracle Information Rights Management [Электронный ресурс]. Режим доступа: http://docs.oracle.com/cd/E21043_01/doc.1111/e14495/configirm.htm#CFHHBCBC.

СПЕЦИАЛИЗИРОВАННЫЙ СЕРВЕР ДЛЯ ВЗЛОМА

Т.Ю. Дорошенко, К.С. Крючков, К.А. Шинкаренко, студенты
Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, tankem@mail.ru
Проект ГПО 0905 – «Специализированный сервер для взлома»

Риск информационной безопасности – это потенциальная угроза эксплуатации уязвимости актива или группы ценных свойств с целью нанесения вреда организации [1]. Наиболее эффективными мерами уменьшения рисков являются превентивные меры, т.к. они подразумевают устранение уязвимостей и угроз еще на этапе разработки и до начала эксплуатации системы [2]. Такой подход требует от специалиста не только знания типов уязвимостей, но и умения их устранять, при этом должный уровень квалификации специалист может получить исключительно при работе с реальными системами. Создаваемый программный комплекс позволяет приобрести необходимый опыт.

Создать условия, максимально близкие к реальной ситуации, позволяет работа с виртуальными машинами. В этом случае пользователь наделяется всеми правами, которыми он бы обладал, работая непосредственно с компьютером. Более того, использование виртуальных машин позволяет надежно изолировать ресурсы операционных систем с запущенными в них приложениями.

Таким образом, разрабатываемая система, структурная модель которой представлена на рис. 1, разделяется на две подсистемы: веб-сервер и сервер виртуализации.

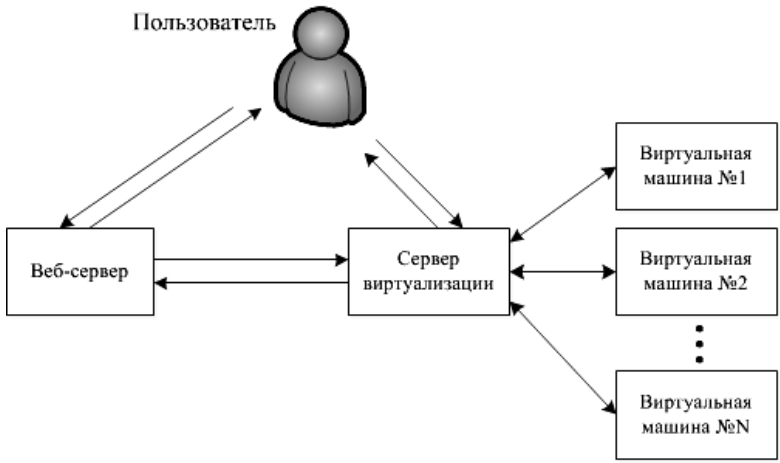


Рис. 1. Структурная схема разрабатываемой системы

Веб-сервер предоставляет интерфейс, при помощи которого пользователь может регистрироваться в системе и выбирать из перечня уязвимые сервисы для их установки на новую виртуальную машину. Сервис представляет собой программное обеспечение, содержащее уязвимость, устранить которую предстоит пользователю. Контроль факта устранения уязвимости осуществляется при помощи специального для каждого сервиса инструмента (скрипта) – чекера. Сервер виртуализации предоставляет ресурсы для хранения, запуска и работы виртуальных машин.

Разрабатываемая система предназначена для решения следующих задач:

1) подготовка и аттестация работников предприятий и учреждений в области ИТ-безопасности;

2) получение студентами опыта использования теоретических знаний по устранению уязвимостей;

3) организация и проведение соревнований CTF (Capture the flag).

Дальнейшая работа над системой предполагает расширение базы уязвимостей, создание системы интерактивных подсказок в ходе работы с сервисами и разработку цикла лабораторных работ для студентов, обучающихся по направлению ИБ.

ЛИТЕРАТУРА

1. ГОСТ Р ИСО/МЭК 27001. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.

2. Превентивные меры снижения рисков [Электронный ресурс]. Режим доступа: http://www.penetrationtest.ru/service/ Preventive_measures_detail.html, свободный (дата обращения: 17.02.2012).

ПРОЕКТИРОВАНИЕ СИСТЕМЫ СОЗДАНИЯ ЗАПРОСОВ НА ВЫДАЧУ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

В.Б. Егоров, студент, Н.С. Михайлов, аспирант

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, evb.gdev@gmail.com

С каждым годом актуальность задачи внедрения электронного документооборота возрастает, о чём свидетельствует принятие федеральной целевой программы «Электронная Россия», действующей до 2015 г. Одной из главных характеристик любого документооборота является юридическая значимость документов в нём. Эта проблема реализуется с помощью электронной подписи [1] и инфраструктуры открытых ключей (Public Key Infrastructure – PKI) [2]. Ключевым элементом этой инфраструктуры является сертификат ключа проверки

электронной подписи, который осуществляет связь между владельцем и его открытым ключом (ключ проверки электронной подписи). Как гласит 63-ФЗ «Об электронной подписи» [1], сертификат ключа проверки электронной подписи (сертификат) – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

При выпуске сертификатов удостоверяющий центр может использовать централизованную или децентрализованную схемы выдачи [2].

При работе с удалёнными регионами или труднодоступными районами (что является актуальным для Томской области) более приемлемой является децентрализованная схема выдачи. Кроме того, в таком случае вероятность сохранения в тайне закрытых ключей пользователя увеличивается, так как он не передаёт их в удостоверяющий центр. Основной проблемой для реализации децентрализованной схемы выдачи является отсутствие у пользователей удобных и актуальных на момент создания запроса на сертификат программных средств.

Основной целью данной работы является проектирование и реализация автоматизированной системы (АС), позволяющей создавать запросы на выдачу сертификата ключа проверки электронной подписи. Для достижения этой цели были поставлены следующие задачи:

– изучение структуры сертификата ключа проверки электронной подписи;

– проектирование структуры приложения и его модулей;

– реализация функции формирования запроса на выдачу сертификата;

– реализация функции формирования подписи к электронному документу.

Требования, предъявляемые к сертификатам ключа проверки электронной подписи, устанавливаемые уполномоченными органами федеральной власти, могут меняться. В связи с этим следует обеспечить расширяемость и изменяемость АС в соответствии с этими требованиями при минимальном изменении её исходного кода.

Для обеспечения расширяемости и изменяемости АС удобно использовать клиент-серверную архитектуру [3]. Благодаря этому обеспечивается удобный доступ всех копий клиентского приложения к изменяемым данным (рис. 1).

Клиентская часть (клиент) представляет собой приложение с динамически создаваемым интерфейсом. В этом случае после запуска клиент загружает необходимые данные с сервера, на основе которых формируется пользовательский интерфейс.

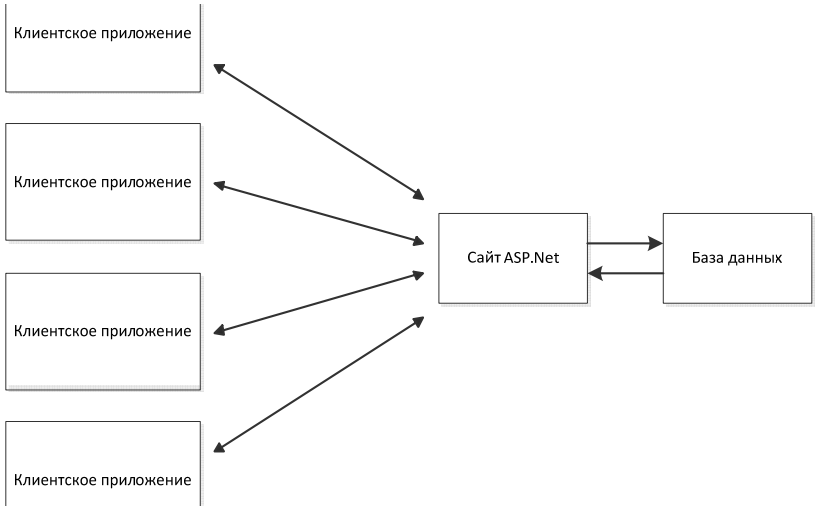


Рис. 1. Клиент-серверная архитектура приложения

В качестве серверной части (сервера) удобно использовать размещенный в сети Интернет сайт. Это обеспечит доступ на сервер клиентских приложений с использованием стандартных веб-интерфейсов. Для хранения данных на сервере следует использовать базу данных.

В ходе работы были изучены структура сертификата ключа проверки электронной подписи, нормативные документы, регламентирующие эту структуру, спроектирована автоматизированная система, позволяющая создавать пользователям удостоверяющего центра запросы на выдачу сертификата и его модули. АС спроектирована таким образом, что при изменении структуры сертификата и требований к его заполнению пользователю не придётся обновлять клиентскую часть. Настройки для динамического интерфейса и структуры сертификата будут автоматически загружены с сервера удостоверяющего центра. Были реализованы и протестированы функция создания запроса на получение сертификата ключа проверки электронной подписи и функция формирования электронной подписи к документу.

ЛИТЕРАТУРА

1. Российская Федерация. Законы. Об электронной подписи: Федер. закон: принят Гос. думой 25 марта 2011 г.: одобр. Советом Федерации 30 марта 2011 г. М., 2011.

2. Полянская О.Ю., Горбатов В.С. Инфраструктуры открытых ключей. М., 2007. 368 с.

3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 4-е изд. М., 2012. 944 с.

РАСЧЕТ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

С.А. Елистратов, студент 5-го курса
Руководитель М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, ФВС, каф. КИБЭВС

Расчет показателей надежности удостоверяющего центра производится по требованиям Приказа ФСБ РФ от 27 декабря 2011г. №796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

Целью работы является определение компонентов удостоверяющего центра (далее – УЦ) и расчет показателей надежности элементов и всего УЦ в целом.

Основными составляющими удостоверяющего центра являются:

– центр сертификации (далее – ЦС);
– центр регистрации (далее – ЦР);
– архив;
– репозиторий;
– АРМ администратора;
– АРМ расчета конфликтных ситуаций (далее – АРМ РКС);
– конечные пользователи.

Схема взаимодействия элементов УЦ представлена на рис. 1 [1].

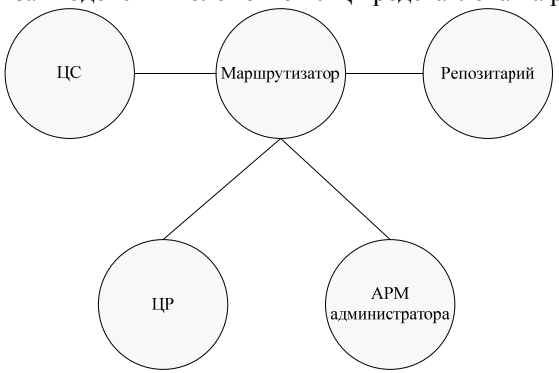


Рис. 1. Схема взаимодействия элементов УЦ

Репозиторий расположен на отдельном сервере, территориально удаленном от данного УЦ, и является общим для публикации СОС всех УЦ системы УЦ. Поэтому при расчете показателей надежности данный элемент не учитывается.

На данной схеме не изображен архив, в связи с тем, что физически он располагается на сервере ЦС [2]. Также на данной схеме не отобра-

жается АРМ РКС, так как он не подключен к другим элементам, соответственно не влияет на показатели надежности УЦ.

В соответствии с [1] и [2] были определены технические компоненты элементов и их взаимосвязь между собой.

Компоненты ЦС:

– eToken;
– ПАК Соболь;
– источник бесперебойного питания (далее – ИБП);
– сервер.

Компоненты ЦР:

– ПАК Соболь;
– ИБП;
– Сервер.

Компоненты АРМ Администратора:

– eToken;
– ПАК Соболь;
– ИБП;
– АРМ.

Компоненты взаимодействуют по последовательно-параллельной схеме, в которой ИБП с источником питания АРМ и Сервера соединен параллельно. Взаимосвязь компонентов, на примере компонентов ЦС, приведена на рис. 2.

Рис. 2. Последовательно-параллельное соединение элемента ЦС

Для расчета показателей надежности, таких как интенсивность отказов, вероятность безотказной работы и коэффициента готовности использовались формулы, описанные в [3, 4] (таблица).

Интенсивность и вероятность безотказной работы

Элемент	Интенсивность (1/ч)	Вероятность безотказной работы (за год)	Вероятность безотказной работы всей системы
ЦС	$3{,}77\times10^{-5}$	0,72	0,28
ЦР	$3{,}76\times10^{-5}$	0,72	
АРМ Администратора	$2{,}39\times10^{-5}$	0,67	
Маршрутизатор	$2{,}5\times10^{-5}$	0,8	

Для расчета коэффициента готовности за полезное время работы системы было решено брать время работы УЦ с момента получения свидетельства об аккредитации, при том условии, что УЦ работал без сбоев. Общее время восстановления равняется 2 ч согласно [2].

Таким образом, коэффициент готовности равен 0,998.

Заключение. Из полученного результата для коэффициента готовности следует, что в данном УЦ работают квалифицированные специалисты по наладке, поиску причин неисправности системы, а также правильно организована служба поддержки с целью уменьшения времени ожидания по приведению ее в работоспособное состояние.

Низкая вероятность безотказной работы всего УЦ связана с последовательным включением в систему компонентов, обеспечивающих защиту от НСД, а именно ПАК Соболь и eToken. В дальнейшем необходимо рассмотреть варианты учета ПАК Соболь в элементах УЦ, его влияние на работоспособность УЦ.

ЛИТЕРАТУРА

1. КриптоПро ЖТЯИ.00067-02 90 01 КриптоПро УЦ. Общее описание / КриптоПро. М., 2012. 114 с.

2. Регламент Подчиненного Удостоверяющего центра ФГУП «ЦентрИнформ» Санкт-Петербург [Электронный ресурс]. Режим доступа: http://ca.centerinform.ru/docs/reg_puc63_spb.pdf, свободный. Загл. с экрана. Яз. рус.

3. Шелупанов А.А. Обеспечение надежности функционирования удостоверяющих центров: НИР / А.А. Шелупанов, Р.В. Мещеряков, Е.М. Давыдова и др. 2007. 65 с.

4. Голинкевич Т.А. Прикладная теория надежности: учеб. для студентов вузов. М.: Высш. шк., 1977. 160 с.

ЛАБОРАТОРНЫЙ СТЕНД СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

А.А.Гридин, студент каф. КИБЭВС

Научный руководитель А.С. Ковтун, инженер ЦТБ ТУСУРа

г. Томск, ТУСУР, ФВС, zelgadis.tomsk@gmail.com

В проделанной работе были рассмотрены принципы работы контроллеров UNITECO и GATE-4000, составлена схема размещения элементов СКУД, частично собран стенд.

Система контроля и управления доступом (СКУД) – совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение/регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через двери, ворота, проходные [1].

Основные задачи:

– ограничение доступа на заданную территорию;

– идентификация лица, имеющего доступ на заданную территорию;

– управление доступом на заданную территорию.

Дополнительные задачи:

– учёт рабочего времени;

– ведение базы персонала / посетителей [2].

В качестве исходных данных использовались руководства по эксплуатации предоставленного оборудования, а также план аудитории 108 ФЭТ ТУСУРа. Стенд состоит из турникета, двери, дверной стойки и лабораторного стола (рис. 1).

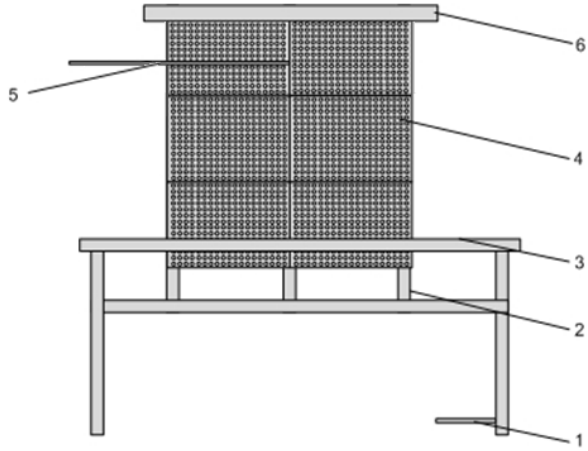


Рис. 1. Внешний вид стола лабораторного стенда СКУД: *1* – полка для системного блока ПСБ-01; *2* – задняя рама ЗР-01; *3* – стол С5-1800; *4* – панель перфорированная ПП-02; *5* – полка приборная короткая ППК-1500; *6* – комплект освещения на регулируемом кронштейне 5КО-36

В результате анализа предоставленного оборудования, а также плана аудитории было решено:

– расположить два монитора (один для основной работы – конфигурирования и настройки системы СКУД, второй для дополнительного поиска информации в Интернете), контроллеры UNITECO, GATE-4000, блок питания СКАТ-1200 и две патч-панели на лабораторном столе стенда;

– мониторы прикрепить к перфорированным панелям с помощью кронштейнов;

– расположить на двери электромагнитный замок и две электромеханические защелки;

– расположить на дверной стойке считыватель, кнопку и кодовую панель;

– провода расположить в кабель-канале, которые следует проложить от устройств к патч-панелям;

– студенты будут коммутировать устройства с помощью двух патч-панелей, одна из которых будет необходима для питания устройств, другая – для передачи сигналов между устройствами.

Взаимное расположение элементов стенда, без учета расстояния между турникетом и стендом, представлено на рис. 2, толстой линией выделены устройства, тонкая линия – кабель-канал, в котором будут располагаться провода, идущие от устройств.

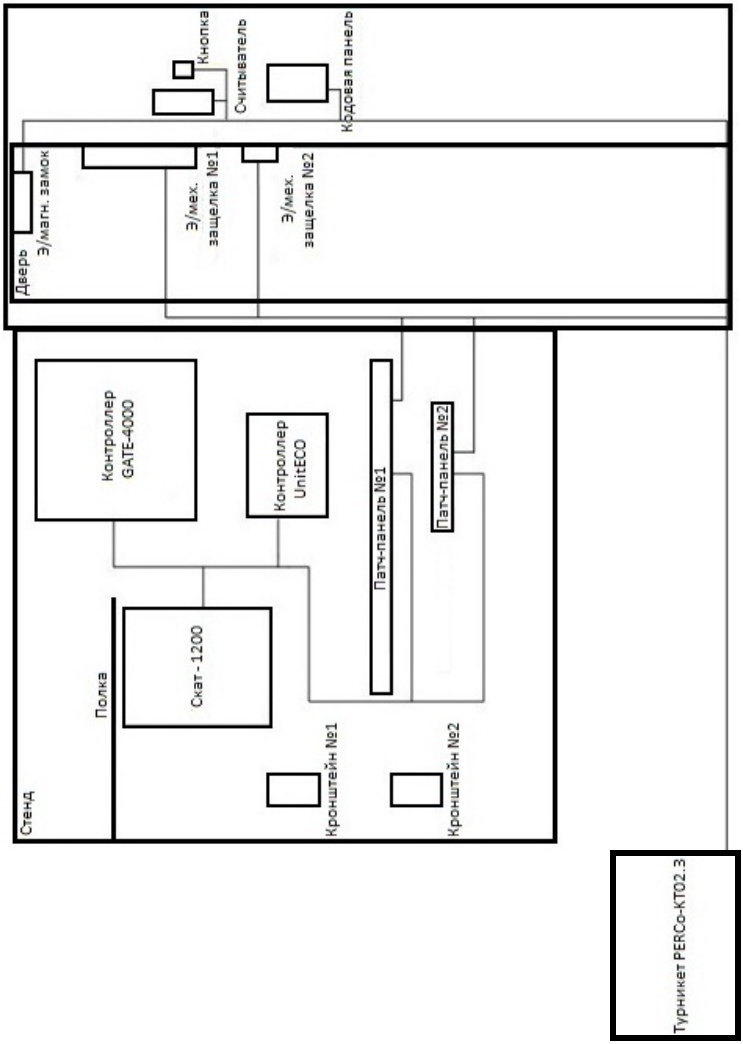


Рис. 2. Взаимное расположение элементов стенда

В данный момент дверь и дверная стойка отсутствуют, размещена только одна патч-панель, обеспечивающая питание элементов стенда, к ней подключены контроллеры UNITECO, GATE-4000 и блок питания СКАТ-1200.

В дальнейшем, в рамках дипломной работы, планируется закончить лабораторный стенд и написать методические указания по обучению на нем студентов, согласуя действия со своим научным руководителем.

ЛИТЕРАТУРА

1. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. М.: Горячая линия – Телеком, 2010. 272 с.

2. Пожарный эксперт. Статья «Автономные системы контроля доступа (СКУД) – установка, монтаж» [Электронный ресурс]. Режим доступа: http://www.pozharnyj-expert.ru/avtonomnye-sistemy-kontrolja-dostupa-skud-ustanovka-montazh – свободный (дата обращения: 27.02.2013).

СИСТЕМА АУТЕНТИФИКАЦИИ НА ОСНОВЕ QR-КОДОВ

А.Ю. Исхаков, студент

Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.

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

Аутентификация является динамично развивающейся областью обеспечения информационной безопасности. Это обусловлено тем, что по мере появления новых прогрессивных способов для ее реализации, появляются также и новые средства для осуществления нелегального получения привилегий в системе безопасности.

Процедура аутентификации являются неотъемлемой составляющей в вопросе обеспечения пропускного режима в организации. Одним из современных способов осуществления контроля доступа и пропускного режима на предприятии являются электронные проходные [1]. Внешне электронные проходные выполнены в виде турникетов различного вида – триподы [1], роторные турникеты [1] или калитки, в стойки которых встроены контроллер и считыватели бесконтактных карт доступа.

Считыватели, использующиеся в электронных проходных, имеют разный принцип действия и работают со следующими устройствами:

– ключи-брелоки «Touch memory». Металлическая таблетка, внутри которой расположен чип ПЗУ;

– карты с магнитной полосой. В данное время чаще всего используются в банковских картах, нежели в СКУД [2]. Существуют магнит-

ные карты с низкокоэрцитивной и высококоэрцитивной магнитной полосой и с записью на разные дорожки;

– карты со штрих-кодом. На карту наносится штриховой код. Существует более сложный вариант – штрих-код закрывается материалом, прозрачным только в инфракрасном свете, считывание происходит в ИК-области;

– Proximity-карты. Технология в настоящее время занимает лидирующие позиции среди средств идентификации в системах контроля доступа. Относительно невысокая цена Proximity-карт позволяет использовать их на объектах с большим числом работников и посетителей, таких как кинотеатры, метро или крупные офисы;

– смарт-карты (с контактными чипами).

Стоит отметить, что при использовании вышеперечисленных средств контроль аутентификации (проверка факта легального предъявления карты) возлагается на охранников-контролёров. Очевидно, что при большом потоке посетителей влияние человеческого фактора может негативно сказаться на надежности такой схемы аутентификации. Это связано со снижением концентрации внимания при рутинной сверке проходящих через СКУД субъектов с фотографиями в системе (особенно если внешность злоумышленника была целенаправленно замаскирована под легального пользователя).

Для решения этой проблемы возможны следующие варианты:

– применение технологий биометрической аутентификации;

– добавление второго фактора аутентификации.

Ввиду большой стоимости биометрических средств была предпринята попытка рассмотреть возможность добавления дополнительного фактора без ущерба для удобства и времени проведения аутентификации.

Предлагаемый механизм предполагает использование мобильного устройства связи (смартфон или коммуникатор) в качестве носителя пользовательского идентификатора. Считывателем является программно-аппаратный комплекс, включающий персональный компьютер, веб-камеру и программное обеспечение для работы системы, включающее модули интеграции с распространёнными СКУД.

Для исключения возможности перехвата идентификатора пользователя предлагается использовать технологию OTP (One time password) для генерации уникальных идентификаторов пользователей [2]. Метод одноразовых паролей позволит избежать возможности проведения атаки человек посередине, которой подвержено большое количество столь популярных сегодня Proxomity-карт в случае применения сторонних считывателей.

Коммуникация сканера и мобильного устройства предполагаются посредством использования современной технологии QR (quick response) [3] кодов. Сегодня она находит широкое применение в маркетинговой и рекламной деятельности.

Второй фактор включает в себя защиту от несанкционированного доступа к приложению-аутентификатору (в случае потери/кражи мобильного устройства) путём использования графических паролей.

Схема работы предложенного способа аутентификации посетителей изображена на рис. 1.

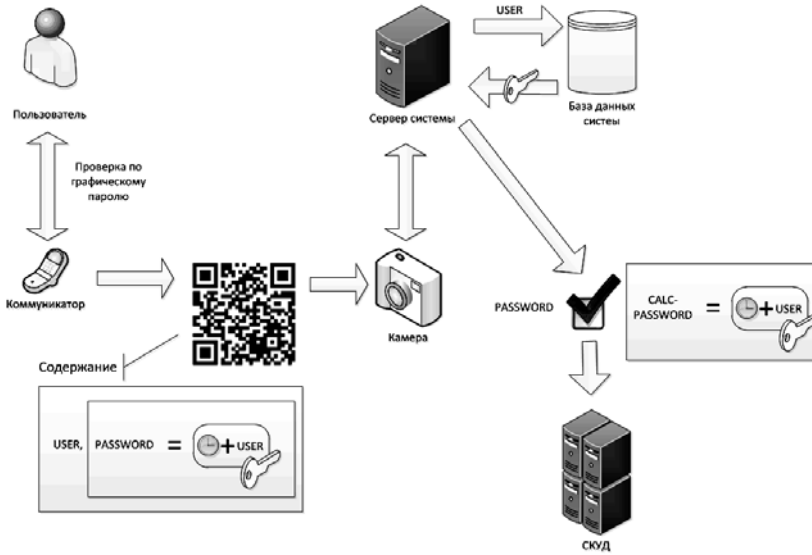


Рис. 1. Предложенная схема аутентификации

Характерными чертами традиционных электронных пропусков являются высокая стоимость изготовления карт, а также незащищённость от внешних воздействий (хрупкость, стирание краски и т.д.). Кроме того, довольно часто возникает проблема, когда сотрудники забывают свои электронные пропуска в автомобиле, в кабинете и т.д., что сложно сказать о средстве мобильной связи.

Предлагаемая система аутентификации позволяет не только добиться дополнительного уровня защиты, но и решить многочисленные практические неудобства в использовании традиционных электронных пропусков без необходимости применения многочисленных организационных мер.

ЛИТЕРАТУРА

1. Электронные проходные [Электронный ресурс]: Электрон. дан [Москва]. Режим доступа: http://sotops.ru/catalog/elektronnye-prohodnye-Perco, свободный. Загл. с экрана.
2. Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам: учеб. пособие для вузов / Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. Гриф УМО. М.: Горячая линия – Телеком, 2009. 552 с.
3. QR код [Электронный ресурс]: Электрон. дан. [Москва]. Режим доступа: http://www.qrcc.ru/qrcode.html, свободный. Загл. с экрана.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ПОСЕЩЕНИЙ ОСОБОЙ ЭКОНОМИЧЕСКОЙ ЗОНЫ ТЕХНИКО-ВНЕДРЕНЧЕСКОГО ТИПА «ТОМСК»

А.Ю. Исхаков, студент

Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.

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

Особая экономическая зона (ОЭЗ) – это территория, наделенная особым юридическим статусом и экономическими льготами для привлечения иностранных инвестиций и развития предпринимательской деятельности [2]. В России ОЭЗ начали развиваться в 2005 г. после принятия Федерального закона 116-ФЗ «Об экономических зонах в Российской Федерации» от 22.07.2005 [1].

Цель создания особых экономических зон – развитие высокотехнологичных отраслей экономики, импортозамещающих производств, туризма и санаторно-курортной сферы, разработка и производство новых видов продукции, расширение транспортно-логистической системы. ОЭЗ – это интегрированный инструмент экономического развития.

В связи с большой социальной значимостью данного проекта (развитие особых экономических зон находится под личным контролем Президента РФ) территорию ОЭЗ постоянно посещает большое количество людей, являющихся как гражданами РФ, так и иностранцами. Учитывая факт, что на территории зоны функционируют инновационные предприятия, работающие в том числе и на стадии НИОКР, актуальным является вопрос обеспечения безопасности интеллектуальной собственности компаний-резидентов.

Данная задача является одной из основных в работе службы безопасности ОАО «ОЭЗ ТВТ «Томск». Для ее решения подразделение ведет контроль и учет всех посещений территории ОЭЗ: все объекты оборудованы системами аудио- и видеофиксации, единой системой

контроля и управления доступом, на всех объектах действуют пропускной и внутриобъектовый режимы.

Учитывая высокую посещаемость ОЭЗ «Томск», актуальным является вопрос автоматизации контроля и учета посетителей. Таким образом, была поставлена задача автоматизировать процесс регистрации и учета посетителей объекта. Кроме того, необходимо было обеспечить возможность накопления статистических данных и формирования отчетов.

Таким образом, решение поставленной задачи сводится к разработке распределенной автоматизированной информационной системы (АИС) [3] с возможностью разграничения прав доступа.

В разрабатываемой автоматизированной системе можно выделить несколько основных модулей:

– ядро системы. Обеспечивает взаимодействие всех модулей комплекса, работу с базой данных. Позволяет вести учётную политику в системе, конфигурировать внешний вид и настраивать пользовательские фильтры;

– модуль «Поиск и фильтрация». Один из основных модулей системы. Обеспечивает возможность контекстного поиска по всем типам информации, хранящейся в базе данных;

– модуль «Календарь событий». Имитирует настольный календарь, позволяющий связывать все виды событий с временными интервалами. Поддерживается хронографическая типизация событий различными цветовыми схемами (прошедшие, текущие запланированные события);

– модуль «Подача заявок». Внешний по отношению к системе модуль. Позволяет полностью перевести процесс подачи заявки на посещение в электронную форму. Используется другими подразделениями, курирующими вопросы привлечения посетителей в ОЭЗ;

– модуль «Генератор отчетов». Предназначен для формирования пользовательских отчетов.

Разработанная автоматизированная информационная система успешно внедрена в производственный процесс и была высоко оценена руководящим составом предприятия. В дальнейшем возможно усовершенствование системы путем разработки модуля для интеграции с используемой на предприятии системой СКУД [3], что позволит обеспечить репликацию баз данных двух систем.

ЛИТЕРАТУРА

1. Закон Российской Федерации «Об особых экономических зонах в Российской Федерации» от 22 июля 2005 г. № 116-ФЗ // Собрание законодательства Российской Федерации. 2005. с изм. и допол. в ред. от 06.12.2012 г.

2. Россия. Особые экономические зоны [Электронный ресурс]. URL: http://www.russez.ru (дата обращения: 18.01.2013).

3. Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам: учеб. пособие для вузов / Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. М.: Горячая линия – Телеком, 2009. 552 с.

ОРГАНИЗАЦИЯ РАБОЧЕГО МЕСТА ОПЕРАТОРА ВИДЕОНАБЛЮДЕНИЯ ПРИ БОЛЬШОМ КОЛИЧЕСТВЕ КАМЕР

Е.А. Калашникова, студентка каф. КИБЭВС

Научный руководитель А.С. Ковтун, инженер ЦТБ ТУСУР

г. Томск, ТУСУР, ФВС, diva.90@list.ru

Видеонаблюдение уже несколько десятков лет остается самой информативной, самой заметной подсистемой безопасности. Системы сигнализации обладают наибольшей удельной эффективностью на рубль вложений, однако после того как сигнализация установлена, никакое ее наращивание уже не очень повышает защищенность объекта. Видеонаблюдение же позволяет обрабатывать огромное количество информации, и, как правило, чем больше видеокамер установлено на объекте, тем выше его защищенность. Однако большое количество видеокамер, большое количество информации – это море, в котором можно захлебнуться, если не организовать эффективную систему управления этой информацией.

Простейший способ помочь оператору в эффективной организации системы управления – это выбор видеокамер для отображения не по их номеру, а указанием на плане местности – это существенно облегчает управление в критической ситуации: не надо суматошно вспоминать номер камеры или искать его в длинном списке, висящем на стене возле оператора.

Помимо выбора одиночных камер, нередко полезно организовать так называемый залповый вывод нескольких сигналов с одного участка (из одного помещения) на несколько мониторов. На компьютеризованном плане помещения оператор мышью (или пальцем на чувствительном экране) выбирает помещение, и на видеомониторах сразу отображается несколько камер из этого помещения. Разнесение камер на эти мониторы должно быть осмысленным и единообразным.

На самом деле чистое видеонаблюдение при наличии большого количества видеокамер встречается редко. Раз уж объект настолько сложный или ответственный, что на нем расположено много видеока-

мер, то наверняка присутствуют и другие охранные подсистемы – сигнализации, контроля доступа. Так что рабочее место оператора, по сути, является интегрированным, позволяющим управлять интегрированной системой безопасности. Даже если доминирующей системой является система видеонаблюдения, все равно система окажется в той или иной степени интегрированной. Существующие сегодня компьютерные системы видеонаблюдения, или системы, поддержанные компьютерными АРМ, всегда интегрированные. Раньше встречались аппаратные системы на матричных коммутаторах на десятки тысяч видеокамер (например, в некоторых аэропортах), но ныне повсеместно для управления системами используются компьютеры с интегрирующим программным обеспечением, да и старые аналоговые видеосистемы все более тесно интегрируются с охранной сигнализацией хотя бы посредством встроенных средств видеокоммутаторов и видеомультиплексоров.

И это существенно, ведь наблюдать вручную сотни или тысячи видеосигналов нереально – для этого потребуются десятки или сотни операторов. Система сама должна отобрать наиболее интересные (опасные, подозрительные) картинки и показать их оператору.

Таким образом, видеонаблюдение не является самостоятельной системой, оно предназначено для верификации тревог или контроля развития ситуации, когда из других источников информации становится известно, что проблема на таком-то участке, и оператор вручную просматривает всего несколько видеокамер – один участок.

Однако исходя лишь из данных охранной сигнализации и других систем, довольно трудно выбрать, какие каналы наблюдения наиболее интересны в данный момент. Может помочь автоматизированный анализ самих видеосигналов, но в любом случае система сможет лишь выделить несколько видеокамер как потенциально наиболее интересных, и уже оператор должен вручную сам определить, какой канал (или несколько каналов) заслуживает внимательного изучения. Например, по сигналу разбития стекла могут представлять интерес несколько видеокамер внутри здания (если преступник проник внутрь) или несколько – снаружи (если он убегает). Даже сигнал от детектора движения в одной из камер часто не дает информации, в поле зрения какой следующей камеры покажется нарушитель, ведь поле зрения той камеры он уже пробежал, туда смотреть бесполезно – разве только просматривать запись за последние несколько секунд. Таким образом, основной постулат организации операторского рабочего места при большом количестве видеокамер – возможность быстро окинуть взглядом несколько изображений, выбрать среди них одно, изучить его пристально, переключиться на соседнее и обратно. В примитивном

случае это реализуется в виде многооконного отображения нескольких сигналов, из которых оператор выбирает один для внимательного рассмотрения во весь экран. В примитивном потому, что при такой организации рабочего места после выбора для просмотра одного изображения остальные больше не видны оператору, и он может не заметить, что там начались события более интересные, чем в том канале, который он сейчас рассматривает в полноэкранном режиме. Если проектировщики не очень ограничены в габаритах АРМ оператора, лучше использовать несколько небольших мониторов (или один большой в многооконном режиме) в качестве обзорных и один высококачественный для внимательного изучения выбранного канала. Некоторые системы позволяют осуществлять выбор пальцем на чувствительном экране многооконного обзорного монитора.

Качество изображения на основном мониторе должно быть ограничено только видеокамерой. Потому строки должны быть строго на грани разрешения глаза – примерно 1 угловой минуты. При большем значении строки будут видны и будут раздражать оператора, при меньшем – потеряется часть информации, разрешение будет ограничено не техническими средствами, а зрением оператора. Таким образом, например, аналоговый видеомонитор диагональю 17» (43 см) должен быть расположен на расстоянии около 140 см. В реальности расстояние может быть меньше, ибо зрение большинства людей, особенно после нескольких часов дежурства, далеко от идеала, кроме того, качественные черно-белые аналоговые мониторы не имеют четко выраженных строк. Хотя у некачественных мониторов строки четных и нечетных полукадров могут сдваиваться, так что реальный размер строки окажется вдвое больше теоретического. Если же используется ЖК-монитор или высококачественный компьютерный монитор высокого разрешения, то необходимо применять вычислительные алгоритмы сглаживания и осуществлять вывод одной строки видеосигнала на 1,5–2 физические строки монитора, тогда изображение также станет гладким и можно будет экран приблизить к оператору, что более комфортно, без риска раздражения глаз видимой строчной структурой.

ЛИТЕРАТУРА

1. Омельянчук А. Организация рабочего места оператора видеонаблюдения при большом количестве камер // Технологии защиты. 2009. №4.

РАДИОВОЛНОВОЕ СКАНИРОВАНИЕ

А.А. Казанцев, И.И. Земсков, студенты
А.В. Максимов, ст. преподаватель
г. Томск, ТУСУР, РТФ, каф. РЗИ, kazantsev-inetbiz@mail.ru
Проект ГПО РЗИ-1304 – «Радиоволновое сканирование»

Цель работы: математическое обоснование метода визуализации по фазовому портрету объекта в радиодиапазоне.

Моделируемое устройство должно отвечать следующим параметрам:

1) иметь 3 сканирующих устройства (далее СУ) для уменьшения вероятности возникновения «мертвых зон» на реальном сканируемом объекте;

2) длина базы сканирующего устройства $B = 0{,}3$ м;

3) частота излучаемых электромагнитных волн $f = 60$ ГГц, длина волны $\lambda = 0{,}005$ м;

4) амплитуды излучаемых колебаний $A_1 = A_2 = 1$;

5) расстояние от СУ до сканируемого объекта $OC = 1{,}5$ м;

6) максимальный радиус сканируемого объекта $R = 0{,}75$ м.

Работа устройства основана на принципе интерференции электромагнитных волн в радиодиапазоне, это позволит получить интерференционную картину от тела под радиопрозрачной одеждой. СУ имеют по два излучателя и одной приемной антенне на собственных базах, причем излучатели находятся по краям базы, а центр приемной антенны смещен на расстояние 1/3 длины базы от первого излучателя, и 2/3 длины базы от второго. Каждое СУ подвижно относительно оси, расположенной за центром приемной антенны, что и создает разность хода, необходимую для получения интерференционной картины. СУ излучает когерентные узконаправленные монохроматические электромагнитные волны в направлении сканируемого объекта и считывает интенсивность в сканируемой точке. Зная некоторые параметры СУ, возможно рассчитать расстояние от СУ до сканируемого объекта. Используя полученные данные, возможно определить местонахождение посторонних предметов на сканируемом объекте и визуализировать полученные данные.

Описание работы устройства. СУ расположены так, что каждое может отсканировать 120° дуги сканируемого объекта. В начальный момент времени все СУ находятся на уровне высоты сканируемого объекта. Сканирование происходит только в горизонтальной плоскости. Перед началом сканирования прибор определяет угол поворота СУ в зависимости от радиуса текущего горизонтального сечения сканируемого объекта. СУ устанавливается в начальное положение относительно определенного ранее угла, излучает электромагнитные вол-

ны, считывает интенсивность в данной точке и поворачивается на заданный угол. Данная операция повторяется, пока не будет достигнут максимум определенного ранее угла поворота СУ. После завершения сканирования в горизонтальной плоскости, СУ смещается вниз по вертикали на заданное расстояние, и операция сканирования повторяется с момента определения угла поворота СУ. Данные операции выполняются до тех пор, пока не будет отсканирован весь объект.

Для простоты вычисления калибровочным сканируемым объектом выбран цилиндр. Сечение цилиндра в горизонтальной плоскости – окружность. Решив несколько простых геометрических задач, можно перейти к следующим уравнениям:

1. Угол поворота сканирующего устройства в зависимости от радиуса сканируемого объекта

$$a_c = \arccos\left(\frac{OC^2 - 2R*OC*\cos\left(\frac{\alpha_B}{2}\right) + R^2*\cos(\alpha_B)}{R^2 + OC^2 - 2R*OC*\cos\left(\frac{\alpha_B}{2}\right)}\right),$$

где $\alpha_в$ – угол дуги сканируемого объекта.

2. Расстояние от сканирующего устройства до сканируемого объекта:

$$AC^2 = R^2 + OC^2 - 2R*OC*\cos\left(\arcsin\left(\frac{OC}{R}*\sin(\alpha')\right)\right),$$

где α' – угол поворота сканирующего устройства;

3. Расстояния от излучателей сканирующего устройства до сканируемого объекта:

$$r_1 = \sqrt{\left(\frac{1}{3}B\right)^2 + AC^2}\,; r_2 = \sqrt{\left(\frac{2}{3}B\right)^2 + AC^2}\,.$$

Имеются две рупорные антенны, излучающие монохроматические электромагнитные волны с частотой f = 60 ГГц. Интенсивность в точке сканирования равна: $I = I_1 + I_2 + 2\sqrt{I_1 * I_2} * \cos(k * \Delta r)$, I_1 и I_2 – интенсивность первой и второй электромагнитной волны соответственно, где $I_i = A_i^2$, k – волновое число, равное $k = \frac{2\pi}{\lambda}$; Δr – разность хода, равная $\Delta r = r_2 - r_1$.

Используя заданные параметры и полученные соотношения, с помощью программного комплекса MathCad® 13 построена интерференционная картина сканируемого объекта (рис. 1).

Для наглядного искажения интерференционной картины при изменении формы сканируемого объекта добавляется некоторая неровность. Неровностью будет служить выпуклость на объекте с высотой всего 1 см на протяжении короткого участка (рис. 2).

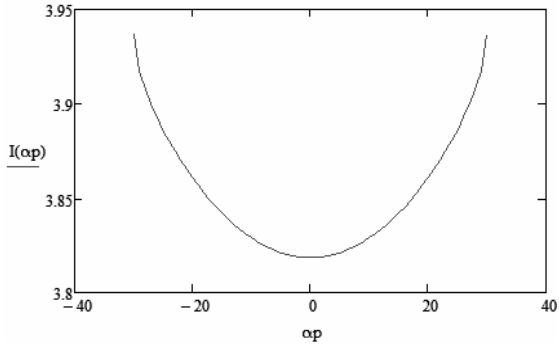


Рис. 1. Интерференционная картина сканируемого объекта

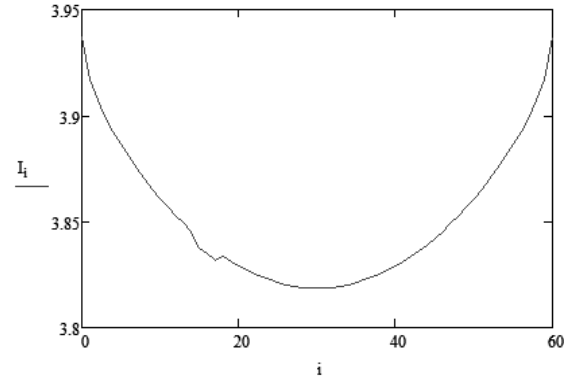


Рис. 2. Интерференционная картина сканируемого объекта с небольшой выпуклостью на поверхности

Таким образом, можно наглядно убедиться, что при изменении формы сканируемого объекта меняется и его интерференционная картина, что позволяет определить наличие посторонних предметов на сканируемом объекте. Однако для визуализации сканируемого объекта по фазовому портрету необходимо решить обратную задачу – найти расстояние от сканирующего устройства до сканируемого объекта, имея только данные об интенсивности интерференционной картины в некоторой области. Это позволит визуализировать объекты произвольной формы.

Из формулы $I = I_1 + I_2 + 2\sqrt{I_1 \times I_2} \times \cos(k \times \Delta r)$ выражаем Δr:

$$\Delta r = \frac{\arccos\left(\frac{I - I_1 - I_2}{2\sqrt{I_1 * I_2}}\right)}{k}. \qquad (1)$$

С другой стороны $\Delta r = \sqrt{\left(\frac{2}{3}B\right)^2 + AC^2} - \sqrt{\left(\frac{1}{3}B\right)^2 + AC^2}$. Выражаем AC^2:

$$AC^2 = \frac{\frac{1}{9}B^2 + \Delta r^4 - \frac{10}{9}\Delta r^2 B^2}{4\Delta r^2}. \quad (2)$$

Подставив результат (1) в уравнение (2), можно посчитать квадрат расстояния от сканирующего устройства до сканируемого объекта, зная всего несколько параметров: интенсивность в точке, амплитуды излучаемых электромагнитных волн, частоту электромагнитных волн или их длину волны и базу сканирующего устройства.

Заключение. В ходе выполнения работы в рамках ГПО посчитаны параметры математической модели радиоволнового сканирующего устройства. Пользуясь полученными данными, разработана программа, позволившая рассчитать фазовый портрет (интерференционную картину) сканируемого объекта. На основе полученных данных сделан вывод о том, что метод визуализации по фазовому портрету объекта в радиодиапазоне применим для создания реального радиоволнового сканера, предназначенного для выявления посторонних предметов на сканируемом объекте.

СПОСОБ ПОСТРОЕНИЯ СХЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ И ЭЛЕМЕНТАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ

М.А. Косенко, студент
Научный руководитель А.А. Конев, доцент
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, kma528@yandex.ru

Разграничение доступа к информации заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможность беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий [1].

Как правило, для разграничения доступа информации применяется дискреционный или мандатный принцип разграничения доступа, но они применимы в чистом виде только для узкого класса задач. Поэтому существует потребность в создании универсальной методики по разграничению доступа информации (рис. 1).

Методика построения схем доступа к информации:

1. Согласно должностным инструкциям определить список сотрудников, которые могут работать с информацией.

2. Определить для каждого сотрудника перечень информационных ресурсов, с которыми он может работать.

3. Определить перечень программ, с помощью которых сотрудник может работать с информацией.

4. Для каждой программы определить список разрешенных протоколов, драйверов.

5. Определить, по каким каналам сотрудник может передавать информацию.

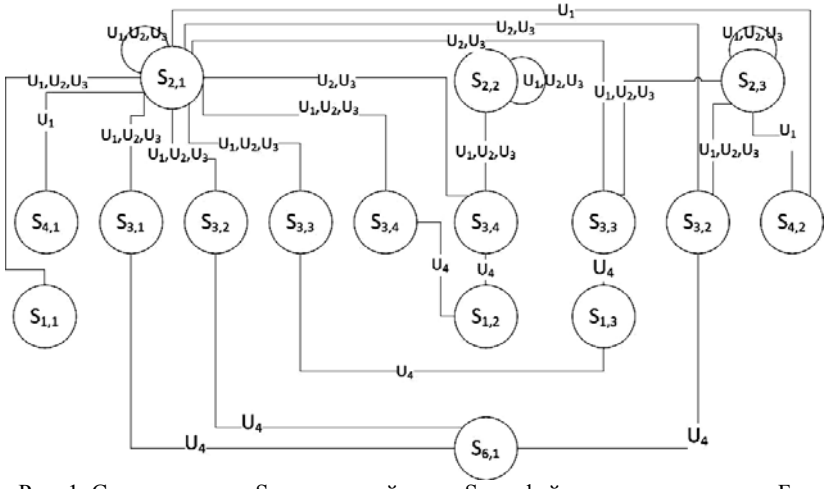


Рис. 1. Схема доступа: $S_{1,1}$ – жесткий диск; $S_{1,2}$ – файл на жестком диске «База.xml»; $S_{1,3}$ – файл на жестком диске «Работа.doc»; $S_{2,1}$ – пользователь Иванов А.С.; $S_{2,2}$ – пользователь Петров И.К.; $S_{2,3}$ – пользователь Сидоров Е.Г.; $S_{3,1}$ – программа Mozilla thunderbird; $S_{3,2}$ – браузер Chrome; $S_{3,3}$ – программа MS Word; $S_{3,4}$ – программа СКУД; $S_{4,1}$ – сейф 1; $S_{4,2}$ – шкаф 2; $S_{6,1}$ – firma.ru; U_1 – физический канал передачи информации; U_2 – видовой канал передачи информации; U_3 – акустический канал передачи информации; U_4 – виртуальный канал передачи информации

Под физическим каналом передачи информации понимается работа с физическим носителем информации, передача носителя другим лицам и перенос носителя из одного места в другое, работа с компьютерной техникой, на которой хранится информация и с помощью которой можно получить доступ к содержимому носителя.

Видовой канал передачи информации – это визуальное получение информации из документов или с монитора компьютера.

Акустический канал передачи информации – это передача информации при помощи устной речи, телефонного разговора и других акустических устройств.

Виртуальный канал передачи информации – передача информации между устройствами компьютера, программами, драйверами, по сети, работа с содержимым носителя информации.

После построения схемы доступа к информации в виртуальной среде необходимо разграничить доступ в физической среде к зонам, в которых находятся ценные информационные ресурсы. Для каждой зоны определить список санкционированных лиц и санкционированных каналов преодоления рубежа защиты.

ЛИТЕРАТУРА

1. Торокин А.А. Инженерно-техническая защита информации. М.: Гелиос АРВ, 2005. 960 с.

ИСТОРИЯ РАЗВИТИЯ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ И ЭЛЕКТРОННОЙ ПОДПИСИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

А.В. Котенко, Д.Р. Нурдавлетова, студенты каф. КИБЭВС
г. Томск, ТУСУР, kotandvla@gmail.com
Проект ГПО КИБЭВС-1210 – «Развитие удостоверяющих центров»

Историю развития электронной подписи и удостоверяющих центров в России фактически можно разделить на 3 этапа: до 2002 г., т.е. до принятия первого закона «Об электронной цифровой подписи (ЭЦП)», далее период с 2002 по 2011 г., когда шло активное обсуждение и внедрение ее в повседневную жизнь и деятельность государственных органов, а далее, в 2011 г. принятие нового закона «Об электронной подписи (ЭП)».

Первое упоминание ЭЦП в законодательстве Российской Федерации появилось только в 1995 г. в Гражданском кодексе РФ, где рассматривалась в качестве одного из аналогов собственноручной подписи (АСП) [1].

Постепенно ЭЦП внедрялась в работу банков, предприятий и организаций как эффективный способ обеспечения защиты конфиденциальной информации. По мере внедрения все острее вставала необходимость закона, который бы официально обозначил и закрепил область применения ЭЦП, позволил бы вести юридически значимый электронный документооборот, приравнивая его к бумажному.

Обсуждение законопроекта началось еще в конце 90-х годов, и его принятие предполагалось в 2000 г., но разработка, согласование и утверждение затянулись, и Закон «Об ЭЦП» вышел в свет только в январе 2002 г.

Федеральный закон № 1-ФЗ «Об электронной цифровой подписи» вступил в силу 10 января 2002 г., который вводил правовые условия для использования ЭЦП в Российской Федерации, определяя права и обязанности лиц, оказывающих услуги, связанные с использованием электронно-цифровой подписи. В этом законе впервые фигурировало первое полное определение электронно-цифровой подписи, а также определения открытого/закрытого ключа, сертификата и пр. Именно ЭЦП обеспечивала однозначное соответствие между электронным документом и лицом, поставившим под ним свою электронную подпись. Принципиальным нововведением стало появление понятия удостоверяющего центра (УЦ) – юридического лица, оказывающего услуги по выдаче сертификатов электронно-цифровой подписи, ведению реестров выданных сертификатов, их аннулированию и т.д. [1].

Стремительного распространения ЭЦП не произошло, несмотря на скорое появление первых удостоверяющих центров. На тот момент еще отсутствовали подзаконные акты, регулирующие обмен электронными документами с использованием ЭЦП между различными органами власти, ведомствами и юридическими и физическими лицами. На решение этих вопросов ушло около полутора лет. Так, было издано порядка тридцати законодательных, нормативных и ведомственных актов, в которых определялось применение ЭЦП [1].

В 2002 г. в Санкт-Петербурге стала проводиться ежегодная конференция под названием «PKI-форум Россия», в которой принимали участие различные эксперты и разработчики СКЗИ, в том числе из других стран [1].

К середине 2003 г. были созданы все необходимые условия для широкого применения электронно-цифровой подписи. Именно этот момент можно считать началом быстрого роста количества организаций, вовлеченных в юридически значимый электронный документооборот [2]. Примерно тогда ЭЦП начали широко применять в органах государственной власти, таких как Администрация Президента, Государственная дума ФС РФ и т.д. Многие коммерческие структуры также успешно пользовались ЭЦП.

На 2006 г. в юридически значимом электронном документообороте с использованием ЭЦП в России участвовало около 150 тыс. юридических лиц [4].

Однако оставались проблемы: в законе не оговаривались форматы представления данных в сертификате. Такая же ситуация возникла с шифровальными средствами ЭЦП, которые даже при реализации одного и того же алгоритма шифрования часто «не понимали» друг друга. То же самое наблюдалось с форматами криптографических сообщений. Для исправления сложившейся ситуации довольно остро стояла необходимость стандартизации на государственном уровне.

Поэтому 10 июня 2005 г. федеральным агентством по информационным технологиям «Росинформтехнологии» был открыт корневой (федеральный) УЦ на базе НИИ «Восход» (ФУЦ), который сначала год проходил подготовку и после этого перешел в штатный режим работы [3]. Задача корневого УЦ состояла в том, чтобы связать все удостоверяющие центры России с целью создания единой зоны доверия в части сертификатов.

На момент открытия корневого УЦ в России насчитывалось 150 локальных удостоверяющих центров [3]. К 2008 г. в России существовало уже 136 удостоверяющих центров в 52 субъектах РФ и 537 центров регистрации [5].

6 апреля 2011 г. вступил в силу Федеральный закон № 63-ФЗ «Об электронной подписи», изменяющий нормы и правила пользования электронной подписью (бывшая ранее электронно-цифровая подпись). Всеохватность является основным отличием нового Федерального закона [6].

Кроме того, вместе с расширением области применения Федерального закона увеличилось и количество видов электронной подписи: простая электронная подпись и усиленная электронная подпись, которая, в свою очередь, может быть квалифицированной и неквалифицированной. Так же, теперь владельцем электронной подписи может быть не только физическое лицо, но и юридическое.

В дополнение к новому закону вышли приказы ФСБ (№795 и № 796 от 27 декабря 2011 г.), стандартизирующие форму сертификата [6].

С 1 июля 2012 г. сам термин «электронно-цифровая подпись» (ЭЦП) заменен термином «электронная подпись» (ЭП) [7].

Только в системе госзаказа на июль 2012 г. было выдано порядка 1 млн ЭП, по сдаче отчетностей в налоговые органы – более 1,5 млн ЭП, еще приблизительно по 500 тыс. было выдано юридическим лицам для участия в коммерческих торгах и для отчетностей в пенсионные фонды. Совет Федерации предлагает унифицировать ЭП [7].

ЛИТЕРАТУРА

1. По материалам конференции PKI-Форум. СПб. 2002.
2. По материалам конференции PKI-Форум. СПб. 2003.
3. По материалам конференции PKI-Форум. СПб. 2005.
4. По материалам конференции PKI-Форум. СПб. 2006.
5. По материалам конференции PKI-Форум. СПб. 2008.
6. По материалам конференции PKI-Форум. СПб. 2011.
7. По материалам конференции PKI-Форум. СПб. 2012.

АВТОМАТИЧЕСКОЕ РАЗВЁРТЫВАНИЕ СИСТЕМЫ МОНИТОРИНГА С ПРОГНОЗИРОВАНИЕМ

А.С. Ковтун, аспирант
Научный руководитель А.А. Шелупанов, проректор по НР, зав. каф. КИБЭВС, д.т.н., проф.
г. Томск, ТУСУР, каф. КИБЭВС, kas@udcs.ru

Современные системы мониторинга сетевой инфраструктуры включают в себя большой функционал для контроля состояния сетевого оборудования. Однако лишь небольшая часть таких систем обладает функционалом по автоматическому обнаружению целей мониторинга. Использование автоматического обнаружения позволяет в значительной степени сократить затраты на развёртывание системы мониторинга.

Введём два понятия: хост и датчик. Хост – элемент сетевой инфраструктуры, относительно которого необходимо развернуть систему мониторинга. Примерами хоста может выступать сервер пользовательских приложений или аппаратный маршрутизатор. Датчик – источник информации о состоянии того или иного составного элемента хоста. В качестве примера типичного датчика можно привести среднюю и пиковую нагрузку на центральный процессор хоста или количество активных отслеживаемых соединений протокола TCP в оперативной памяти маршрутизатора.

Задачи системы мониторинга с прогнозированием заключаются в следующем:

- обнаружение хостов в сети;
- обнаружение датчиков в каждом найденном хосте;
- каталогизация хостов и датчиков хранилища;
- сбор первичной информации с датчиков;
- анализ первичной информации и настройка ядра прогнозирования в соответствии с результатами анализа;
- ведение мониторинга.

Задача обнаружения хостов в сети TCP/IP в наше время решается многими инструментами [1, 5]. Возможно применение ICMP-запросов с последовательным перебором IP-адресов, а также поиск хостов в ARP-таблицах маршрутизаторов. Основная проблема, с которой сталкиваются системы автоматического обнаружения хостов, это сетевые экраны, блокирующие доступ к ресурсам сети. Эта проблема, в основном, решается административными способами.

Обнаружение доступных датчиков в каждом хосте может выполняться различными способами. Самый распространённый способ передачи данных о производительности хоста – использование расширяемого протокола SNMP (Simple Network Management Protocol) [1]. Этот протокол реализован в большинстве операционных систем сете-

вого оборудования, в том числе и аппаратных и программно-аппаратных решений. Стандартизация предоставляемых протоколом данных позволяет упростить процедуру обнаружения основных датчиков хоста, таких как, к примеру, нагрузка на сетевые интерфейсы устройства. Однако ввиду специфичных для каждого производителя принципов работы хостов такая информация, как объём доступной оперативной памяти или нагрузка на центральный процессор хоста, передаётся в разных элементах OID, что усложняет автоматическое обнаружение датчиков. В этом случае имеет смысл применять стороннюю базу данных, содержащую в себе информацию о местонахождении того или иного датчика в дереве параметров. Такая база содержит в себе конечное число элементов, сопоставляющих семейство оборудования одного (или нескольких) производителя и дерево OID, в котором содержится вся необходимая информация. Таким образом, считывая модель устройства, можно определить, какие датчики доступны и их местонахождение.

Очевидно, что для доступа по протоколу SNMP к параметрам производительности оборудования необходимо, чтобы этот протокол поддерживался хостом, а также чтобы он был предварительно настроен. Настройка протокола SNMP специфична для каждого оборудования и выходит за рамки данной статьи.

Задача хранения и каталогизации данных заключается в организованном хранении адреса наблюдаемого хоста, а также значений OID, соответствующих найденным датчикам хоста. В качестве такой системы хранения может выступать реляционная СУБД, обеспечивающая быстрый доступ к значениям.

Система мониторинга с прогнозированием представляет собой математический аппарат, выполняющий анализ поступающих с датчиков данных с целью смоделировать поведение наблюдаемого хоста и предупредить обслуживающий персонал о возможных неполадках. Для автоматизированного построения модели хоста необходимо выполнить первичный сбор данных в течение определённого промежутка времени. Сбор и хранение производятся путём выборки адресов OID всех датчиков хоста, после чего выполняется SNMP-запрос на получение значений параметров соответствующих элементов. Полученные значения сохраняются в базу данных СУБД. Выборка производится периодически, с некоторым интервалом.

На основании полученной с датчиков информации появляется возможность построить статистическую модель хоста. Такая модель позволит обрабатывать поступающие данные в режиме реального времени, своевременно обнаруживая возникающие нестандартные ситуации.

Использование для построения статистической модели хоста статистического языка программирования R[2] позволяет решить ряд задач, исходящих из функциональных возможностей этого языка программирования:

- простота в реализации ввиду готовых оптимизированных статистических библиотек;
- интеграция с иными языками программирования;
- возможность использовать несколько моделей, а также динамические модели.

Статистическая модель строится на основании разрабатываемых в рамках данной работы алгоритмов, позволяющих оценивать корреляцию поступающих данных между собой, а также иные статистические характеристики.

После построения статистической модели хоста система может использоваться для формирования оценочной характеристики хоста с целью выявления всех нештатных ситуаций и генерации предупреждающих сигналов.

ЛИТЕРАТУРА

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии протоколы: учеб. для вузов. 4-е изд. СПб.: Питер, 2012. 944 с.

2. Norman Matloff. The art of R programming. San Frencisco: No Starch Press, Inc, 2011. 404 с.

3. Гмурман В.Е. Теория вероятностей и математическая статистика: учеб. пособие для вузов. 9-е изд., стер. М.: Высш. шк., 2003. 479 с.

4. Бельков Д.В., Едемская Е.Н., Незамова Л.В. Статистический анализ сетевого трафика. Донецкий национальный технический институт. Донецк, 10 с.

5. Документация на программный продукт NMap [Электронный ресурс]. Режим доступа: http://nmap.org/man/ru/

6. Шумский А.А. Основы системного анализа: учеб. пособие / А.А. Шумский, А.А. Шелупанов. Томск : ТМЦДО, 2005. 225 с.

7. Шелупанов А.А. Теория вероятности: учеб. пособие [Электронный ресурс]. Электрон. текстовые дан. Электрон. граф. дан. Электрон. прикладная прогр. Томск: ТУСУР, 2007.

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ЗАЩИТЫ .NET ПРИЛОЖЕНИЙ ОТ ИЗУЧЕНИЯ

К.А. Козловский, студент каф. КИБЭВС

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

г. Томск, ТУСУР, eatingpeopleisfun.da@gmail.com

В настоящее время актуальна проблема защиты исходного кода от изучения. Немодифицированное .NET приложение при помощи некоторых инструментов может быть с легкостью изучено конкурентами и

злоумышленниками. Подавляющее большинство методов защиты кода от изучения известны как разработчикам, так и злоумышленникам, существуют готовые решения для «обхода» многих методов защиты.

Для решения проблемы можно использовать методы обфускации.

Основной целью данного проекта является создание комплексного метода защиты исходного кода от изучения.

Сформулированная цель определяет следующие задачи:

1. Изучение существующих методов защиты.

3. Реализация приложения – защитника.

4. Разработка и практическая реализация криптора/лоадера.

5. Разработка и практическая реализация пяти методов обфускации.

Дизассемблер – транслятор, преобразующий машинный код, объектный файл или библиотечные модули в текст программы на языке Ассемблер.

По режиму работы с пользователем делятся:

- на автоматические;
- интерактивные.

Примером автоматических дизассемблеров может служить Ildasm. Такие дизассемблеры генерируют готовый листинг, который можно затем править в текстовом редакторе. Пример интерактивного – IDA. Он позволяет изменять правила дизассемблирования и является весьма удобным инструментом для исследования программ.

Чаще всего дизассемблер используют для анализа программы (или ее части), исходный текст которой неизвестен – с целью модификации, копирования или взлома. Реже – для поиска ошибок (багов) в программах и компиляторах, а также для анализа оптимизации создаваемого компилятором машинного кода.

Обычно однопроходный дизассемблер (как и построчный ассемблер) является составной частью отладчика.

Отладчик (дебáггер, англ. debugger) – компьютерная программа, предназначенная для поиска багов в других программах, ядрах операционных систем, SQL-запросах и других видах кода. Отладчик позволяет выполнять пошаговую трассировку, отслеживать, устанавливать или изменять значения переменных в процессе выполнения кода, устанавливать и удалять контрольные точки или условия остановки и т.д.

Проектирование схемы защиты приложения. Защита приложения будет состоять из трёх компонентов:

1. Обфускация исходного кода.

1.1. Переименование переменных/функций.

1.2. Шифрование строк.

1.3. Обфускация контрольного потока.

2. Грубая защита.

2.1. Внедрение дополнительных методов, обладающих некорректной семантикой для языка Ассемблер либо для компиляторов высокого уровня и соответственно вызывающих ошибки при восстановлении кода.

2.2. Внедрение недостижимых функций с некорректным кодом.

3. Криптор / лоадер.

3.1. Посредством криптора шифруется оригинальный программный файл и в его начало записывается код [лоадер], при запуске выполняющий расшифровку и выполнение зашифрованной программы.

Реализация криптора. Были реализованы криптор (модуль для шифрования) и загрузчик.

Алгоритм работы модуля для шифрования:

1. На вход подается исполнительный (.exe) файл приложения, созданного на базе .NET Framework'a.
2. Файл полностью шифруется, получается массив байт.
3. В новый файл записывается код загрузчика, а затем массив байт, полученный на предыдущем шаге.
4. Созданный на предыдущем шаге файл возвращается.

Алгоритм работы загрузчика:

1. При запуске загрузчика он считывает байты в массив из файла, в котором находится, начиная со смещения, равного длине загрузчика.
2. Полученные байты расшифровываются. Получается исходное приложение.
3. Приложение запускается.

Реализация обфускатора. Было реализовано пять методов обфускации исходного кода. Применяются эти методы после декомпиляции исходной сборки.

1. Переименование методов.
2. Клонирование методов.
3. Развертка циклов.
4. Создание методов-оберток.
5. Внедрение мертвого кода.

Шифрованный код приложения полностью игнорируется декомпиляторами. Применение ildasm также показало игнорирование шифрованного кода дизассемблером. Если злоумышленнику удастся распаковать приложение, то изучение исходного кода затруднит обфускация.

Вынесение полезной логики на сервер. Чтобы усложнить злоумышленнику процесс разгадывания реализованных методов защиты, программный комплекс будет работать на сервере, а пользователи смогут подключаться к нему через браузер. Таким образом, алгоритмы, защищающие код, будут выполняться на удаленной машине, а не на компьютере пользователя.

Удалённая работа с программным комплексом реализована через связку ASP.NET + WCF. WCF сервис располагается на IIS 8.0 сервере, под управлением операционной системы Windows Server 2012 и применяет алгоритмы методов защиты кода непосредственно на серверной стороне.

ЛИТЕРАТУРА

1. Erohin A. Синтаксис языка CIL // Сборки .NET [Электронный ресурс]. URL: http://professorweb.ru/my/csharp/assembly/level4/4_1.php (дата обращения: 21.01.2013).

2. Стандарт языка CIL // ECMA International [Электронный ресурс]. URL: http://www.ecma-international.org/ (дата обращения: 22.01.2013).

3. Инъекции MSIL кода в стороннюю сборку при помощи Mono.Cecil. Реализация принципов АОП в NET // Хабрахабр [Электронный ресурс]. URL: http://habrahabr.ru/post/108947/ (дата обращения: 29.01.2013).

4. Mono.Cecil и его использование // .NET RSDN [Электронный ресурс]. URL: http://www.rsdn.ru/forum/dotnet/2795517.hot (дата обращения: 29.01.2013).

5. Mono.Cecil: делаем свой «компилятор» // Хабрахабр [Электронный ресурс]. URL: http://habrahabr.ru/post/109167/ (дата обращения: 30.01.2013).

6. Обфускация и защита программных продуктов // CIT Forum [Электронный ресурс]. URL: http://citforum.ru/security/articles/obfus/ (дата обращения: 30.01.2013).

7. Обфускаторы (и деобфускаторы) для .NET // Хабрахабр [Электронный ресурс] URL: http://habrahabr.ru/post/74463/ (дата обращения: 1.02.2013).

8. MSIL Tutorial // Codeguru [Электронный ресурс]. URL: http://www.codeguru.com/csharp/.net/net_general/il/article.php/c4635/MSIL-Tutorial.htm (дата обращения: 1.02.2013).

9. Варновский Н.П., Захаров В.А., Кузюрин Н.Н., Чернов А.В., Шокуров А.В. Об особенностях применения методов обфускации программ для информационной защиты // Научная библиотека КиберЛенинка [Электронный ресурс] URL: http://cyberleninka.ru/article/n/ob-osobennostyah-primeneniya-metodov-obfuskatsii-programm-dlya-informatsionnoy-zaschity-mikroelektronnyh-shem#ixzz2LntsZKQ7 (дата обращения: 02.02.2013).

10. Mikalai Kalpinski. Обфускация. Взгляд изнутри // Персональный блог [Электронный ресурс]. URL: http://sharcus.blogspot.ru/2011/06/blog-post.html (дата обращения: 02.02.2013).

11. Mikalai Kalpinski. Как работают обфускаторы. Изменения внутренней логики // Персональный блог [Электронный ресурс]. URL: http://sharcus.blogspot.ru/2011/08/blog-post.html (дата обращения: 02.02.2013).

12. Common Intermediate Language // Википедия [Электронный ресурс]. URL: http://ru.wikipedia.org/wiki/MSIL (дата обращения: 02.02.2013).

13. Обфускация // Википедия [Электронный ресурс]. URL: http://ru.wikipedia.org/wiki/Обфускация (дата обращения: 02.02.2013).

УПРАВЛЕНИЕ РИСКАМИ, СВЯЗАННЫМИ С ВНЕДРЕНИЕМ DLP-СИСТЕМ В ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ ПРЕДПРИЯТИЯ

Н.С. Козыренко, студентка

Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.

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

Как показывает статистика, более 70% всех инцидентов безопасности связано с деятельностью легальных пользователей информационных систем [1]. В данном случае базовые механизмы защиты, направленные в основном на защиту от несанкционированного доступа к информации, оказываются недейственными. Поэтому в корпоративные информационные системы активно внедряются специализированные системы обнаружения и предотвращения утечек информации (DLP-системы).

Большинство DLP-систем предполагает защиту от утечек на трех уровнях [2]:

– локализация и отслеживание действий с конфиденциальной информацией в файловых хранилищах;

– мониторинг и управление перемещениями конфиденциальных данных по корпоративной сети предприятия (анализ трафика);

– мониторинг и управление данными на пользовательских рабочих станциях.

Как правило, разработчики предлагают отдельные решения по каждому из перечисленных уровней, но для полного контроля информационных потоков рекомендуется сочетание этих решений.

Системы данного класса являются сложными программными или программно-аппаратными комплексами, в связи с чем недолжное управление системой может породить ряд рисков для предприятия.

В данной статье рассмотрены некоторые ключевые риски, связанные с внедрением в инфраструктуру предприятия DLP-систем.

Управление рисками

Риски	Последствия	Управление рисками
1	2	3
Ошибки в определении точки установки модулей перехвата	Под контролем оказываются не все информационные потоки предприятия. Возможны утечки	Предпроектное исследование. Знание структуры сети и инфных потоков. Подключение сервера перехвата к пограничному роутеру
Продолжение таблицы Неправильная настройка модулей сетевого перехвата	Нарушение непрерывности бизнес-процессов; Временные и материальные потери; Урон репутации организации, потеря коммерческих связей	Детальная проработка и тестирование правил блокировки трафика. Более надежным является установка системы в режим мониторинга с настройкой проработанных правил политик безопасности и оповещением

Продолжение табл.

1	2	3
Сбои и отказы модулей DLP-системы	Отсутствие анализа проходящего трафика	Наличие модуля централизованного управления системой. Контроль работы системы
Недостаточно выделено дискового пространства для хранения перехваченного трафика	Удаление некоторых сетевых пакетов из хранилищ или исключение из перехвата (прохождение трафика без анализа контента)	Определение требований к аппаратному обеспечению сервера DLP-системы. Объем дискового пространства из расчета: «суточный объем трафика» × «кол-во дней хранения» + % (определяемый спецификацией разработчика)
Высокий процент ошибок первого рода	Лишнее время на обработку событий. Возможность упустить действительные угрозы	Настройка критериев поиска в политиках безопасности DLP-систем в соответствии со специфичными шаблонами критичных данных
Конфликты с программными решениями сторонних производителей	Снижение производительности. Отказы в работе информационных систем	Получение детальной информации от вендора о возможных конфликтах и о совместных решениях. Внедрение системы в тестовом режиме на выделенном сегменте ИТ-инфраструктуры
Изменения исполнения бизнес-процессов или ИТ-структуры, снижающие эффективность DLP-системы	Обход настроенных в DLP-системе политик безопасности. Утечки информации	Внедрение организационных мер: контроль и учет изменений в инфраструктуре и в информационных потоках предприятия. Непрерывный процесс менеджмента политик безопасности
Ошибки в интеграции со службой каталогов	Отсутствие или ошибки в идентификации нарушителей	Не является критической ошибкой, но затрудняет процесс определения каналов утечки. Необходимо развертывание и администрирование службы каталогов

DLP-системы являются эффективным средством предотвращения утечек информации, позволяющим минимизировать риски реализации угроз утечек информации от внутренних пользователей корпоративной сети. Однако следует учитывать, что внедрение таких систем требует значительных предварительных исследований, в том числе связанных с менеджментом рисков.

ЛИТЕРАТУРА

1. Астахов А. Как защищаться от инсайдера? [Электронный ресурс]. 2007. URL: http://www.iso27000.ru/chitalnyi-zai/zaschita-ot-insaiderov/kak-zaschischatsya-ot-insaidera (дата обращения: 21.01.2013).

2. Data Leak Prevention. An ISACA White Paper. ISACA, 2010, 24 с.

СПОСОБ БЕЗОПАСНОЙ ПЕРЕДАЧИ СВЕДЕНИЙ О СОСТОЯНИИ ЗДОРОВЬЯ ЧЕЛОВЕКА

Н.С. Козыренко, студентка
Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, nattyk@sibmail.com

Одним из приоритетных направлений развития информационных технологий является их внедрение в сферу медицины, так как медицинские информационные системы позволяют управлять одним из важнейших ресурсов – человеческим ресурсом.

Следует отметить, что в подобных информационных системах нельзя избежать обработки специальных категорий персональных данных, обозначенных в Федеральном законе №152-ФЗ «О персональных данных». Человек имеет конституционное право на защиту информации, обеспечивающей его личную безопасность [1], отсюда возникают особые требования по обеспечению информационной безопасности сведений о его здоровье.

Вопросы защиты данных специальных категорий особенно актуальны при необходимости их передачи по открытым каналам связи, например при реализации систем контроля за состоянием наблюдаемого вне стационара пациента (удаленный мониторинг пациента). Наиболее общая схема функционирования систем такого класса заключается в следующем (рис. 1):

1) пользователь (пациент) регистрирует события диагностики с помощью датчиков или отвечая на вопросы анкет;

2) средствами вычислительной техники производится обработка полученных данных;

3) реализация оповещения о требующих внимания случаях; отправка результатов обработки курирующему врачу.

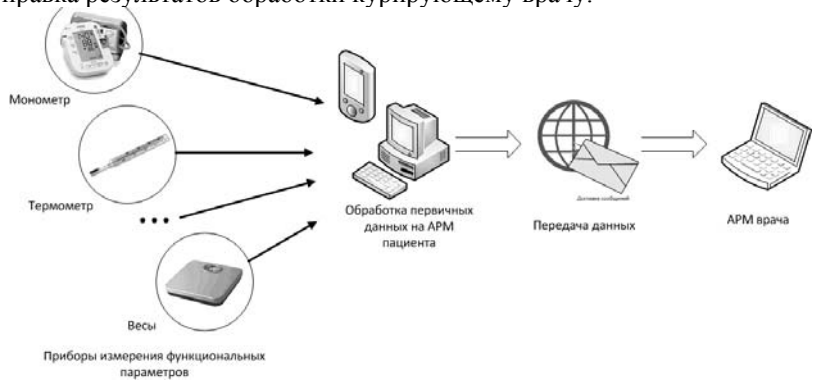


Рис. 1. Схема взаимодействия пациента и врача

Как правило, основой оценки состояния человека является субъективная оценка врача, даваемая им на основе анализа информации о состоянии подсистем организма по отточенным многолетним опытом методам диагностики. В таком случае специалисту необходимо предоставление ряда функциональных показателей и реализация схем их защищенной передачи.

Предлагается решение, позволяющее скрыть конкретные показатели здоровья человека, не снизив при этом информативности об общем состоянии пациента. С этой целью необходимо формализовать процесс принятия решения о состоянии здоровья автоматизированной системой на стороне клиента. Куратору наблюдаемого человека передается только результат обработки первичных данных.

Появляется задача построения математической модели оценки состояния здоровья и определение численных методов для ее реализации, которая позволила бы по набору разнородных получаемых системой на входе показателей (представленных вербальными описаниями, интервальными и точечными количественными значениями) определить интегральную оценку здоровья человека.

В данном случае необходимо рассматривать организм человека как некоторую техническую систему, состоящую из ряда взаимодействующих подсистем, а также подвергающуюся ряду внешних воздействий.

Поскольку любая математическая модель есть лишь некоторая аппроксимация исследуемой действительности, то в процессе ее построения выполняется последовательность шагов, позволяющая упростить модель, сохранив при этом отражение ею реальности [2]. Для обозначенной модели эта последовательность действий представлена ниже:

1) определение показателей, определяющих здоровье человека;
2) задание набора состояний здоровья человека;
3) формирование референтных групп пациентов;
4) измерение, фиксация множества показателей – сбор исходных данных;
5) построение математической модели, получение интегральной оценки;
6) сопоставление значений интегрального показателя с состоянием;
7) верификация модели.

Замена отношений между системами жизнеобеспечения человека (кардиологической, респираторной системами, состоянием зрения, слуха, речи) подходящими отношениями между математическими объектами формализует процесс оценки здоровья пациента, выдавая в качестве результата интегральный показатель.

Передача по открытым каналам связи интегральной оценки позволяет минимизировать вероятность реализации угроз информацион-

ной безопасности, связанных с передачей информации по сетевым каналам.

ЛИТЕРАТУРА

1. Панченко А.В. Личная безопасность человека и гражданина и конституционно-правовой механизм ее обеспечения в Российской Федерации: автореф. дис. ... канд. юрид. наук. Челябинск, 2010. 26 с.

2. Айвазян С.А. Прикладная статистика. Основы моделирования и первичная обработка данных / С.А. Айвазян, И.С. Енюков, Л.Д. Мешалкин. М.: Финансы и статистика, 1983. 471 с.

ПРИНЦИПЫ НАПОЛНЕНИЯ РЕЧЕВОГО КОРПУСА

Н.В. Кумушбаева, студентка

Научный руководитель А.А. Конев, доцент, к.т.н

г. Томск, ТУСУР, каф. КИБЭВС, madmasele@list.ru

Создание систем анализа и распознавания речи является одной из актуальных проблем развития современных технологий. Важная составляющая таких систем – это изучение звукового строя языка. Современный русский язык начал формироваться еще в XIX в., однако до сих пор ведется достаточное количество научных исследований, направленных на изучение параметров звукового строя.

На кафедре КИБЭВС был создан речевой корпус. Речевой корпус состоит из речевых сигналов и базы данных, содержащей их описание, также сюда входят и средства обработки для эффективной работы с речевым материалом.

Речевой материал, пожалуй, самая важная часть речевого корпуса.

При проектировании подобных систем нужно учитывать различные критерии [1], такие как наличие дикторов разного пола и возраста, дикторов с дефектами речи, различными заболеваниями речевого тракта, также немаловажно будет учитывать эмоциональную окраску говорящего, тип речи (диалог, спонтанная речь, чтение), скорость речи, тип речевого сигнала и его акустическое окружение. Существенным признаком системы также являются возможность пополнения базы новыми сигналами, внесение изменений в существующие данные, возможность ручной сегментации сигналов.

Основные критерии были учтены при создании программы SpeechSoft. Она не только содержит в себе базу сигналов с характеристиками, но и позволяет их дополнять и изменять.

Для дополнения данного речевого корпуса была выбрана речевая база СПбГУ. Она содержит записи разговора с 10 дикторами (5 женщин и 5 мужчин), а это в общей сложности более 800 различных фраз

разной длины и эмоциальной нагрузки. Для одного диктора женского пола для 30 фраз определена сегментация и транскрипция. Но внести эти данные в базу нельзя без дополнительной обработки. Звуковой алфавит, определенный в СПбГУ, не соответствует алфавиту, определенному на кафедре КИБЭВС, поэтому также будут отличаться границы звуков в сегментации. Стоит отметить, что у СПбГУ определено несколько вариантов транскрипции для всех фраз. Скорее всего, это связано с тем, что транскрипцию составляли разные эксперты, которые не смогли придти к согласию в определении звукового алфавита, что, безусловно, делает эти данные субъективными. Эти транскрипции были составлены заново для нашего звукового алфавита и добавлены в базу данных с кратким описанием, а также была добавлена информация о дикторе.

Работа по наполнению речевого корпуса продолжается. Планируется обработать и добавить оставшиеся сигналы базы СПбГУ. На данный момент речевой корпус содержит 113 речевых единиц, 156 речевых сигналов общей длительностью 16 минут и 46 секунды, результаты ручной сегментации для 132 сигналов.

ЛИТЕРАТУРА

а. Кривнова О.Ф. Области применения речевых корпусов и опыт их разработки // Тр. XVIII сессии Рос. акустического общества РАО. Таганрог, 2006.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПК «КВАРТА»

Ю.В. Кополовец, студент, А.И. Кураленко, аспирант
г. Томск, ТУСУР, каф. РЗИ, yurakop@mail.ru

Проведение аудита информационной безопасности сетевых и информационных ресурсов приобретает сегодня особую актуальность, так как результаты его проведения позволяют повысить эффективность системы информационной безопасности и снизить затраты на обеспечение безопасности информационных систем.

Аудит информационной безопасности (далее – ИБ) – системный процесс получения и оценки объективных данных о текучем состоянии системы обеспечения безопасности информации (далее – СОБИ) на объектах информатизации, действиях и событиях, происходящих на объекте, определяющих уровень их соответствия определенному критерию. Причем оценки могут быть как качественными, так и количественными. На базе оценок вырабатываются практические рекомендации по повышению эффективности, построению и управлению СОБИ в соответствии с поставленными задачами и изменением во времени.

Результатом аудита ИБ могут быть рекомендации по изменению инфраструктуры сети, по применению соответствующих средств защиты, организационно-административные решения, если они целесообразны по экономическим, техническим соображениям или не позволяют достичь необходимого уровня защищенности.

Аудит ИБ включает в себя следующие процедуры:

- инициирование процедуры аудита;
- сбор информации аудита;
- анализ данных аудита;
- выработку рекомендаций;
- подготовку аудиторского отчета [1].

Для проведения аудита была создана экспертная комиссия. Формирование экспертной группы состоит из [2]:

- определения численного состава экспертной группы;
- определения коэффициентов авторитета экспертов;
- подбора экспертов в соответствии с их компетентностью [2].

В ходе проведения работ применялись следующие методы обследования:

- интервьюирование сотрудников;
- проведение опроса сотрудников отделов, в которых обрабатываются ПДн;
- анализ организационно-распорядительных документов:
- внутренние организационно-распорядительные документы и инструктивно-методическая документация на предмет соответствия их требованиям законодательства РФ в области ПДн;
- технические документы, в которых отражены функциональные возможности средств защиты информации;
- расположение оборудования ИСПДн.

В качестве объекта аудита выступала информационная система (далее – ИС) персональных данных ПК «Кварта» ООО «РИЦ ЖКХ». ИС располагается в офисном здании на пятом этаже в двух кабинетах (офисное помещение и серверная). ИС ПК «Кварта» построена на основе технологий и оборудования компании Cisco Systems. На уровне ядра центральной ЛВС используются 2 сервера. В качестве граничного оборудования на стыке контролируемой зоны и общей сети предприятия используется S-Terra CSP VPN Gate 1000 (рис. 1).

Помещение, где располагается ИС, оборудовано охранной и пожарной сигнализацией. Доступ в офисное помещение бесконтрольный в присутствии сотрудников организации. В отсутствии сотрудников двери запираются. Ключ от помещения находится у ответственного сотрудника. Доступ в серверное помещение регламентирован для конкретных лиц организации. Посторонние лица имеют доступ только в

присутствии допущенных лиц. Двери оборудованы запорным механизмом. В отсутствие допущенных лиц помещение серверной закрывается.

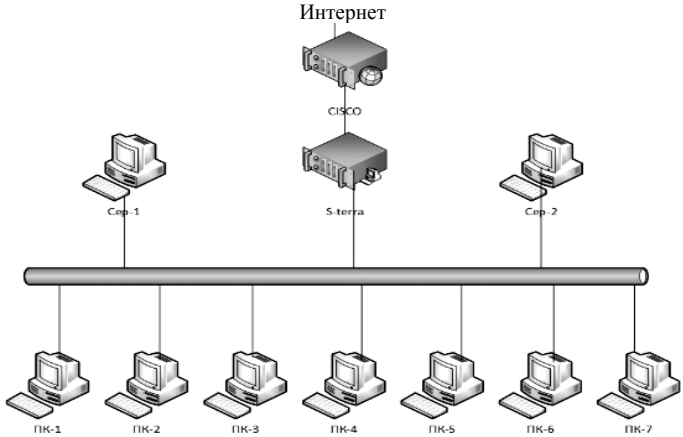


Рис. 1. Топология ИС ПК «Кварта»

Техническая защита осуществляется следующими средствами защиты информации:

- Средство межсетевого экранирования – S-Terra CSP VPN Gate 1000 3.1.
- Средства защиты информации от несанкционированного доступа – Secret Net 6 (автономный режим).
- Средства доверенной загрузки – Secret Net Card PCI.
- Средства криптографической защиты – КриптоПро CSP 3.6 R2.
- Средства антивирусной защиты – Eset NOD32 Platinum Pack 4.0.

Аудит ИБ ИС ПК «Кварта» проведен методами, которые описывались ранее, составлены модели угроз и нарушителя. На основе полученных данных установлен набор требований в соответствии с «1-м уровнем защищенности» [3].

Проведено сравнение организационных и технических мер защиты информации с требованиями ФСТЭК России по защите ПДн [3, 4]. После сравнения был сделан вывод, что система полностью соответствует требованиям по техническим мерам защиты информации, а организационные меры защиты информации нуждаются в доработке организационно-распорядительной документации.

В результате проведения аудита ИБ ИС ПК «Кварта» разработан аудиторский отчет, который содержит цели проведения аудита ИБ, характеристики обследуемой ИС, указание используемых методов ау-

дита, результаты анализа данных аудита, выводы, обобщающие эти результаты и содержащие соответствие требованиям нормативно-методических документов в области защиты персональных данных, рекомендации по устранению существующих недостатков в системе защиты ИС ПК «Кварта».

ЛИТЕРАТУРА

1. Курило А.П. Аудит информационной безопасности. М.: БДЦ-пресс, 2006. 304 с.

2. Домарев В.В. Защита информации и безопасность компьютерных систем. М.: ДиаСофт, 1999. 189 с.

3. Постановление Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

ПОСТРОЕНИЕ СТРАТЕГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.И. Кураленко, аспирант, М.С. Саблин, инженер

г. Томск, ТУСУР, каф. РЗИ, TheOriginal_6a@sibmail.com

ООО «Комплексные услуги безопасности»

В настоящее время стабильная работа организации зависит от множества факторов и составляющих, одной из таких составляющих является информационная безопасность. Для разработки эффективной стратегии обеспечения информационной безопасности НО «Фонд развития малого и среднего предпринимательства Томской области», а именно информационной системы (далее ИС) «Сотрудники и контрагенты» будем использовать SWOT-анализ.

Методология проведения SWOT-анализа состоит в следующем:

- производится подбор экспертов и формирование экспертных групп для проведения SWOT-анализа [1];
- экспертами формируются критерии для оценки внешней и внутренней структуры организации [2];
- оценка экспертами внешней и внутренней структуры организации [3];
- обработка полученных оценок [3];
- анализ полученных результатов и формирование рекомендаций.

Внутренняя среда – это та часть, которая находится в рамках организации, включающая в себя сильные и слабые стороны организа-

ции. Оценка данных сторон производится экспертной группой по набору ключевых процессов и элементов организации. К данным процессам относятся:

- кадровые процессы;
- организационные процессы;
- производственные процессы;
- финансовые процессы.

SWOT-анализ внешней среды направлен на выявление угроз и возможностей, которые могут возникнуть во внешней или внутренней среде, а также сильных и слабых сторон [2]. Анализ внешней среды предполагает изучение экспертной группой следующих факторов:

- сильные стороны – свойства организации, дающие преимущества;
- слабые стороны – свойства, ослабляющие организацию;
- возможности – факторы внешней среды, использование которых создаст преимущества этой деятельности;
- угрозы – факторы, которые могут потенциально затруднить деятельность.

В результате анализа внешней и внутренней среды строится список категорий (табл. 1) SWOT-анализа, содержащий в себе сами категории и критерии оценки.

Таблица 1

Списки категорий SWOT-анализа

Сильные стороны (S): • организационные процессы; • производственные процессы	Слабые стороны (W): • кадровые процессы; • финансовые процессы
Возможности (O): • разработка нормативной документации	Угрозы (T): • угрозы несанкционированного доступа

В результате построения списка перечисленных категорий и критериев оценки формируется матрица SWOT (табл. 2).

Таблица 2

Матрица SWOT

Критерии		Возможности (O)	Угрозы (T)
		O1	T1
Сильные стороны (S)	S1	(S1, O1)	(S1, T1)
	S2		
Слабые стороны (W)	W1	(W1, O1)	(W1, T1)
	W2		

Оценка критериев «возможности» и «угрозы» производится в соответствии с [3]. После расчета критериев экспертной группой составляется расширенная матрица SWOT (табл. 3).

Таблица 3

Расширенная матрица SWOT

Критерии		Возможности (O)	Угрозы (T)
		O1	T1
Вероятность появления (Pj)			
Коэффициент влияния (Kj)			
Сильные стороны (S)	S1	(S1, O1)	(S1, T1)
	S2		
Слабые стороны (W)	W1	(W1, O1)	(W1, T1)
	W2		

В результате построения итоговой матрицы экспертной группой производится анализ полученных результатов и формирование рекомендаций.

Проведение SWOT-анализа ИС «Сотрудники и контрагенты» показывает следующие положительные стороны данного метода:

- простота концепции SWOT-анализа;
- возможности обобщить и сопоставить информацию совершенно разного характера;
- четкая классификация по определенным критериям;
- свободный выбор анализируемых элементов в зависимости от поставленных целей;
- концепцию можно адаптировать к объекту исследования любого уровня и на любом этапе обследования объекта;
- интеграция результатов SWOT-анализа в соответствии с текущим законодательством.

И следующие отрицательные:

- оценка возможностей и угроз – это всего лишь оценка с определенной долей вероятности;
- SWOT-анализ не учитывает возможные риски;
- процесс получения оценок в существующих методиках расчетов важности требует от экспертов больших затрат времени, психологических и профессиональных навыков, хорошего знания методик.

В результате SWOT-анализа ИС «Сотрудники и контрагенты» был сформирован перечень критериев оценки с дальнейшей оценкой экспертами внешней и внутренней структуры организации, сформирован список категорий SWOT-анализа, на основании которого строилась матрица SWOT и расширенная матрица SWOT. Оценка полученных результатов SWOT-анализа ИС «Сотрудники и контрагенты» послужит для дальнейшей разработки стратегии обеспечения информационной безопасности.

ЛИТЕРАТУРА

1. Домарев В.В. Безопасность информационных технологий. Системный подход. К.: ООО «ТИД ДС», 2004. 992 с.

2. Виханский О.С. Стратегическое управление: учебник. 2-е изд. М.: Гадарики, 2000.

3. Гольдштейн Г.Я. Стратегический менеджмент [Электронный ресурс]. М.: 2003. Режим доступа: http://planovik.ru/management/20/6_4

ЛАБОРАТОРНЫЙ СТЕНД ПОЖАРНО-ОХРАННОЙ СИГНАЛИЗАЦИИ

Е.И. Кузнецов, студент ФВС

Научный руководитель А.С. Ковтун, инженер ЦТБ ТУСУРа

г. Томск, ТУСУР, nootmen131@mail.ru

Пожарно-охранные сигнализационные системы в современном обществе являются неотъемлемой частью электронных систем различного рода предприятий, начиная от небольших частных фирм и домов и заканчивая огромными технологическими предприятиями. В данном проекте будут рассмотрены два комплекса охранно-пожарных сигнализаций: «Мираж» класса «Приват» А4-03 и «Профессионал» М8-03. Контроллер «Приват» предназначается для охраны небольших помещений, таких как малые офисы или квартиры, гаражи. Этот контроллер имеет 4 шлейфа сигнализации, первично конфигурируется с помощью компьютера и работает только посредством GSM-канала передачи извещений, т.е. посредством SMS-сообщений и голосовых сообщений Voice. В зависимости от предпочтений пользователя – получать извещения в виде сообщений или звонков – следует выбирать оператора сотовой связи и определенного рода услуги, направленные на экономию средств абонента. Конкретные тактики реагирования и типы шлейфов (пожарный или охранный) настраиваются с помощью программы-конфигуратора, поставляемой на компакт-диске вместе с контроллером. После конфигурирования контроллер в ЭВМ не нуждается и имеет возможность конфигурирования с помощью запросов мобильного телефона [1].

Контроллер «Профессионал» имеет более продвинутый функционал, чем у контроллера «Приват», имеет возможность расширения посредством интерфейса RS-485 (стандарт физического уровня модели OSI, для асинхронного интерфейса, т.е. интерфейс для связи с другими цифровыми устройствами, обычно по витой паре) [2]. В качестве модуля расширения используется сетевая контрольная панель Мираж-СКП-08-02. «Профессионал» имеет восемь шлейфов пожарно-охран-

ной сигнализации, сетевая контрольная панель так же имеет дополнительно восемь шлейфов сигнализации. Количество панелей определяется возможностями контроллера и составляет до 15 устройств. Помимо GSM-канала оповещения, «Профессионал» имеет возможность передавать извещения по дополнительным каналам передачи извещений, и теперь составляет в общей сумме четыре канала: GPRS (TCP/IP), DATA, SMS, VOICE [3].

Контроллер «Профессионал» работает в совокупности со станцией мониторинга, являющейся сердцем охранно-пожарной сигнализации. Станцией мониторинга является ЭВМ общего назначения с установленными драйверами и конфигуратором. Большинство устройств, такие как GSM-модемы и собственно сам контроллер, конфигурируются с помощью Web-конфигураторов, загружаемых в любой установленный на компьютере браузер. Также в качестве резервного канала через специальный модем станция мониторинга может передавать извещения по телефонным линиям ГТС.

Извещатели, или датчики, делятся на охранные и пожарные. По принципу формирования информационного сигнала охранные и пожарные извещатели делятся на активные и пассивные. Активные извещатели генерируют в охраняемой зоне сигнал и реагируют на изменение его параметров, пассивные реагируют на изменение параметров окружающей среды, вызванное вторжением нарушителя или возгоранием [4].

Охранные извещатели – это устройства, которые в зависимости от принципа действия и условий эксплуатации сообщают о любых нарушениях безопасности. Различают охранные извещатели: движения (инфракрасные активные и пассивные, радиоволновые линейные и объемные, ультразвуковые), открытия (различного рода магнитоконтактные датчики); разбития стекла (акустические и удароконтактные); приближения или прикосновения (емкостные); тряски (вибрационные); преступного нападения (тревожные кнопки); совмещенные или комбинированные [5].

Пожарные извещатели – устройства для формирования сигнала о пожаре. Обычно для извещения о возгорании применяются: тепловые, дымовые, световые (пламени) ионизационные, комбинированные, ручные извещатели. Пожарные извещатели по способу электропитания бывают с питанием по шлейфу, с питанием по отдельной линии и с автономным питанием [6].

В качестве примера была разработана простейшая лабораторная работа на базе контроллера «Приват» (рис. 1). Контроллер «Приват», который имеет 4 шины сигнала (ШС) для подключения шлейфов охранно-пожарной сигнализации, а также вывод +12 В благодаря нали-

чию интегрированного блока питания. К ШС1 по данной схеме подключается пожарный шлейф, состоящий из пожарного дымового оптико-электронного извещателя ИПД-3.1М и ручного пожарного извещателя ИПР-ЗСУ. К ШС2 подключается охранный шлейф сигнализации, состоящий из акустического извещателя разбития стекла «Астра-С» и инфракрасного пассивного датчика движения «Рапид» исполнения 1. К ШС 3 подключается охранный шлейф датчиков открытия, состоящий из двух магнитоконтактных накладных охранных извещателей. ИО «102-2» является более большим по размерам и предназначается для установки на двери, ИО «102-4», в силу своей компактности, обычно монтируется на окна. В конце каждой линии обязательно ставится оконечный резистор, необходимый для согласования линии. В случае его отсутствия контроллер не сможет «взять» на охрану данный шлейф.

В рамках дипломного проекта для стенда разрабатывается курс лабораторных работ.

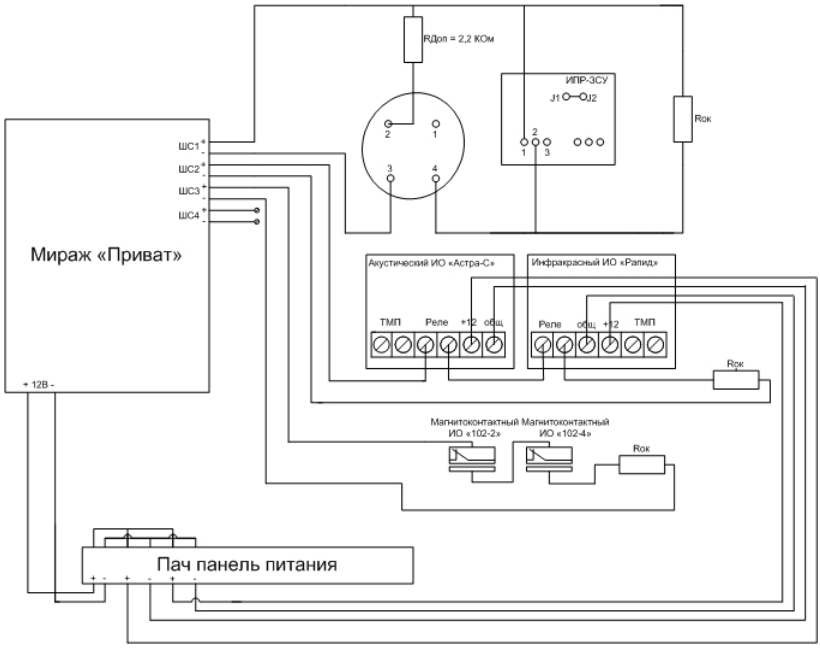


Рис. 1. Структурная электрическая схема подключения шлейфов к контроллеру

Также был спроектирован стенд пожарно-охранной сигнализации (рис 2).

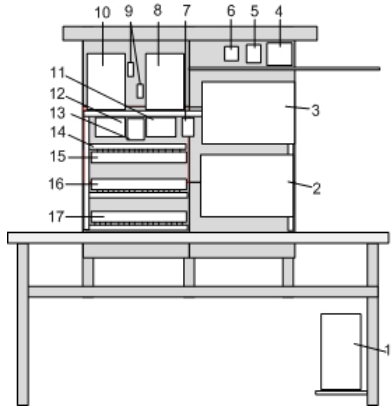


Рис. 2. Проект лабораторного стенда: *1* – системный блок пульта централизованного наблюдения и мониторинга; *2* – основной монитор, предназначенный для выполнения лабораторных работ; *3* – дополнительный монитор, предназначенный для поиска информации в Интернете и вспомогательных целей; *4* – звуковая сирена ООПЗ-12; *5* – звуковая сирена «Гром-12М»; *6* – звуковая сирена «Маяк-12-3М»; *7* – кодовая панель КД-02; *8* – контроллер «Мираж» («Профессионал»); *9* – световые извещатели «Астра-10»; *10* – контроллер «Мираж» («Приват»); *11* – сетевая контрольная панель; *12* – блок-реле БР 3; *13* – контактная площадка touch memory; *14* – кабель-канал; *15* – патч-панель контроллеров; *16* – патч-панель извещателей; *17* – патч-панель питания

ЛИТЕРАТУРА

1. Объектовый контроллер «Мираж-GSM-A4-03». Сер. «Приват»: руководство по эксплуатации АГНС.425644.015 РЭ.

2. Бель Е.А. RS-485 для чайников: электрон. учебник [Электронный ресурс]. Режим доступа: http://www.mayak-bit.narod.ru/rs485.html, free access

3. Объектовый контроллер интегрированной системы мониторинга «Мираж-GSM-M8-03». Сер. «Профессионал»: руководство по эксплуатации АГНС.425644.016 РЭ.

4. Типы и виды охранных извещателей [Электронный ресурс]. Режим доступа: http://www.estateline.ru/articles/885/, free access

5. Принципы работы датчика движения [Электронный ресурс]. Режим доступа: http://lempert.ru/2012/11/23/printsip-rabotyi-datchika-dvizheniya/, free access

6. Пожарный извещатель [Электронный ресурс]. Режим доступа: http://www.polyset.ru/glossary/Пожарный извещатель.php, free access

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПРОВЕРКИ ТЕКСТА НА ОДНОРОДНОСТЬ И ВЫЯВЛЕНИЯ ПЛАГИАТА

Ч.А. Ламожапов, студент, А.С. Романов, доцент, к.т.н.

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

Развитие технологий и сети Интернет предоставило массам пользователей доступ к огромным массивам информации. В настоящее время всё чаще встречаются тексты, содержащие плагиат и неоднородные включения. Это студенческие и псевдонаучные работы, ском-

пилированные из разных источников, а также тексты, подвергшиеся изменению.

Существует много способов обнаружения плагиата: стилометрия; метод шинглов; метод, построенный на классических принципах информационного поиска, и др. [1].

В данной работе в качестве возможного плагиата будем рассматривать фрагменты текста (группы предложений), явно отличающиеся по стилю от основного авторского текста.

Цель данной работы заключается в разработке методики определения неоднородных по стилю фрагментов в тексте, на основе которых можно определить, был ли дополнен изначальный текст.

В качестве математического аппарата будем использовать контрольные карты кумулятивных сумм (КУСУМ-карты) – графическое представление данных, отображающее отклонения от некоторого опорного значения:

$$c_i = \sum_{r=1}^{i} (y_r - T),$$

где y_r – значение наблюдаемой переменной; T – опорное значение, обычно принимают среднее значение выборки; i – номер выборки.

КУСУМ-карты применяются во многих сферах, таких как контроль качества для выявления отклонений от критических значений показателей продукции и процессов, контроль за изменением данных и их отклонения от опорного значения, для анализа текста на однородность и др.

Рассмотрев некоторые работы по анализу текста на однородность с использованием КУСУМ-карт [2–5], можно сделать вывод, что характеристики у каждой из групп исследователей были выбраны свои. Например, в работе [2] используются такие характеристики, как слова, начинающиеся с гласной, короткие слова длиной 2 или 3 буквы и комбинации обеих характеристик. Это указывает на то, что правильный выбор признаков является наиболее важным этапом исследования. КУСУМ-карты дают достаточно высокую точность при определении неоднородных вставок, однако решение принимается человеком «на глаз» – критериев для определения близости графиков не предлагается.

В ходе работы была разработана программная система с веб-интерфейсом для определения неоднородностей в тексте.

Входными данными является текст, который в процессе анализа разбивается на предложения. Для каждого предложения подсчитываются его длина, количество служебных слов и коротких слов, начинающихся с гласной. Также ведутся работы по добавлению других значимых характеристик.

Выходными данными является КУСУМ-карта. Если два графика практически совпадают, можно сделать вывод об однородности текста (рис. 1). Точки расхождения графиков показывают начало неоднородного фрагмента (рис. 2).

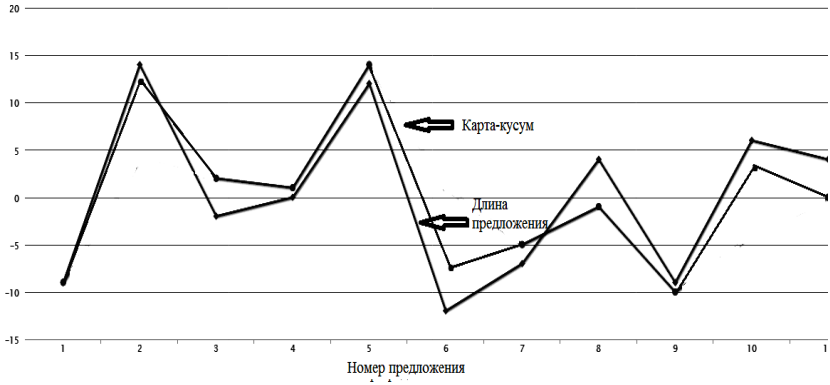


Рис. 1. Пример КУСУМ-карты однородного текста

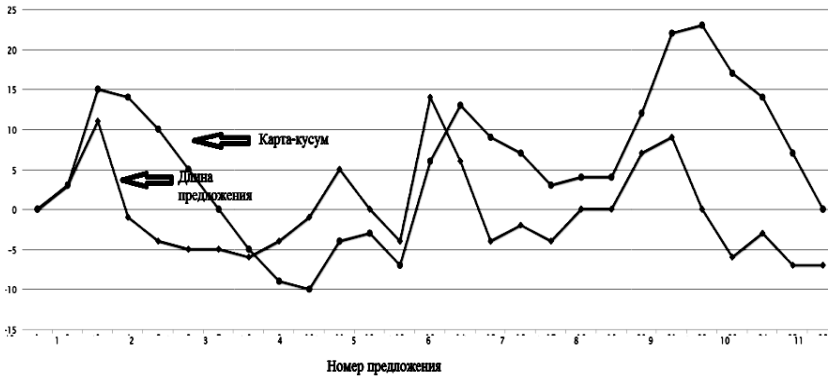


Рис. 2. Пример КУСУМ-карты неоднородного текста

В настоящее время ведется автоматизация метода взвешенных кумулятивных сумм, впервые предложенного Хилтоном и Холмсом [6]. В этой модификации метода отклонения вычисляются с учетом пропорции использования характеристики, что даст более точные результаты:

$$s_i = \sum_{r}^{i} (x_r - pw_r),$$

где $x_г$ – значение наблюдаемой переменной; w_r – длина предложения r; p – доля признаков с интересующими параметрами по отношению к общему количеству признаков.

Далее будут представлены полные результаты исследования.

ЛИТЕРАТУРА

1. Шарапов Р.С., Шарапова Е.В. Система проверки текстов на заимствование из других источников. М.: Айрис-пресс, 2011. 5 с.

2. Authorship Attribution [Электронный ресурс]. Режим доступа: http://www.geoinformatics.org/publications/ABlendedAppro-ach.pdf, свободный.

3. A blended text mining method for authorship authentication analysis [Электронный ресурс]. Режим доступа: http://www.geo-informatics.org/publications/ABlendedApproach.pdf, свободный.

4. Analysing E-mail Text Authorship for Forensic Purposes [Электронный ресурс]. Режим доступа: http://www.academia.edu /721360/Multi-topic_e-mail_authorship_attribution_forensics, свободный.

5. Farringdon J.M. Analyzing for Authorship / J.M. Farringdon with contributions by Morton A.Q., Farringdon M.G., Baker M.D. Cardiff: University of Wales Press, 1996. 324 p.

6. Hilton M.L., Holmes D.I. An assessment of cumulative sum charts for authorship attribution. Literary and Lingllistic Compllting, 1993.

ПОДХОД К ОБФУСКАЦИИ ПРОГРАММНОГО КОДА ПРИ ИСПОЛЬЗОВАНИИ ДИСПЕТЧЕРА УПРАВЛЕНИЯ

С.А. Лапин, студент магистратуры каф. ПФЭиБ

Научный руководитель В.В. Поляков, проф., д.ф.-м.н.

г. Барнаул, АлтГУ, lapinsa567@gmail.com

Одним из способов реализации угроз, связанных с несанкционированным доступом к корпоративным ресурсам и персональным данным, является поиск и эксплуатация критических, с точки зрения информационной безопасности, ошибок в используемом программном обеспечении. Для поиска таких уязвимостей применяются различные техники и методики, среди которых присутствует анализ программного кода с помощью отладчиков, анализаторов кода, интерактивных дизассемблеров. Поэтому задача защиты программ от статического и динамического анализа ее кода на сегодняшний день является актуальной [1]. Частично решить обозначенную проблему позволяет обфускация. В работе [2, 3] показано, что эффективных алгоритмов обфускации в моделях «черного ящика» и «серого ящика» не существует. Однако существует смысл в создании алгоритмов обфускации, обходящих приемы автоматического анализа кода, что влечет за собой повышение требований к уровню квалификации круга лиц, занимаю-

щихся подобным анализом, что в целом положительно влияет на уровень защиты кода приложения [1].

Целью данной работы является создание нового алгоритма для полиморфного изменения программного кода, позволяющего затруднить анализ кода приложения.

Поставленная цель достигается путем использования диспетчера, управляющего потоком выполнения программы. Исходный код на языке assembler, полученный, например, с помощью системы дизассемблирования, делится на N блоков $B=\{B_1,B_2,...,B_n\}$. Каждому полученному блоку ставится в соответствие уникальный, случайно выбранный из множества натуральных чисел идентификатор $ID=\{id_1,id_2,...,id_n\}$, после чего блоки случайным образом перемешиваются. Зная порядок следования идентификаторов до применения такой операции, можно восстановить изначальный алгоритм. Сформируем ключевую последовательность натуральных чисел $K=\{k_1,k_2,...,k_n\}$. Если в соответствие каждому $k_i \in K$ поставить $id_j \in ID$, то можно найти такую функцию $f(k)$, что для любого $k_i \in K$ существует $id_j \in ID$ такая, что $f(k_i)=id_j$. Получение такой функции возможно путем применения одного из существующих методов интерполяции.

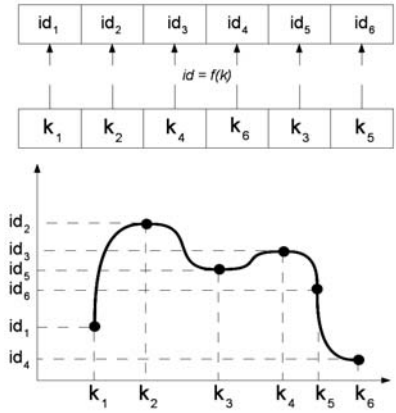


Рис. 1. Зависимость идентификаторов от ключевых значений

При нахождении функции $f(k_i)=id_j$ генерируется код, реализующий вычисление ее значений. В зависимости от полученного результата вызывается тот или иной блок из сформированного ранее множества $B=\{B_1,B_2,...,B_n\}$. Значения ключевых последовательностей для внесения большей неопределенности $K=\{k_1,k_2,...,k_n\}$ при анализе вычисляются в процессе выполнения данного алгоритма перед непосредственным вычислением функции $f(k_i)=id_j$. Как показано в работе [4], такой алгоритм подвержен инструментам динамического анализа, которые позволяют эмулировать выполнение алгоритма. Для предотвращения подобного рода действий в различные участки исходного

кода помещаются антиэмуляционные приемы, позволяющие определить процесс эмуляции кода. Такие методы основаны на недостатках средств эмуляции, на их неспособности корректно получать результаты некоторых операций. После прохождения последнего этапа защиты полученный код должен быть откомпилирован.

Предлагаемый метод не влияет на результат выполнения исходного алгоритма, при этом программа полностью теряет свой первоначальный вид, а использование случайных величин гарантирует получение уникального защищенного кода при выдаче результатов работы. Уровень сложности анализа полученного программного кода не поддается строгой формализации, т.к. зависит от свойств человеческой психики, квалификации, умений, навыков и других субъективных факторов.

Заключение. Предложенный в данной работе метод может найти применение в качестве механизма защиты программного обеспечения, позволяющего усложнить анализ алгоритма работы. При совместном использовании рассмотренной в работе техники защиты с другими существующими методами и алгоритмами обфускации возможно достижение высокого уровня «размытости» кода. Также достоинством представленного метода является то, что статистика использования команд в защищенной программе будет мало отличаться от подобной статистики в исходной программе, что позволяет убрать некоторые проблемы, связанные с определением защищенного кода как вредоносного антивирусными системами, подсчитывающие, например, энтропию секций исполняемого модуля. Кроме того, если принять во внимание факт выполнения условия об уникальности полученного результата работы предложенного алгоритма, то разработчикам программного обеспечения предоставляется возможность генерировать уникальные копии одной и той же программы, по которым можно, например, идентифицировать правообладателя той или иной копии продукта.

ЛИТЕРАТУРА

1. Курмангалеев Ш.Ф. Описание подхода к разработке обфуцирующего компилятора / Ш.Ф. Курмангалеев, В.П. Корчагин, Р.А. Матевосян // Труды Института системного программирования РАН. 2012. Т. 23. С. 67–76.

2. Варновский Н.П. Об особенностях применения методов обфускации программ для информационной защиты микроэлектронных схем / Н.П. Варновский, В.А. Захаров, Н.Н. Кузюрин и др. // Труды Института системного программирования РАН. 2006. Т. 11. С. 27–26.

3. Варновский Н.П. О стойкой обфускации компьютерных программ / Н.П. Варновский, В.А. Захаров, Н.Н. Кузюрин, А.В. Шокуров // Научные ве-

домости БелГУ. Сер. История. Политология. Экономика. Информатика. 2009. № 12-1. С. 97–104.

4. Бакулин М.Г. Динамический анализ обфусцированных приложений с диспетчеризацией или виртуализацией кода / М.Г. Бакулин, С.С. Гайсарян, Ш.Ф. Курмангалеев и др. // Труды Института системного программирования РАН. 2012. Т. 23. С. 49–65.

ЭКРАНИРОВАНИЕ ЭЛЕКТРОМАГНИТНЫХ ВОЛН КАК ОДНО ИЗ СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

А.С. Лукьянов, к.т.н., преп. каф. инфокоммуникационных систем и технологий,
А.О. Авсентьев, адъюнкт каф. информационной безопасности
г. Воронеж, Воронежский институт МВД России, las92@yandex.ru

Сохраняя информацию, на каком-либо носителе, мы подвергаем себя опасности вероятного доступа третьих лиц. Поэтому информационная безопасность не только становится обязательной, но и выступает как одна из важнейших характеристик информационной системы. В деятельности многих учреждений, предприятий отведена первостепенная роль фактору безопасности информации, в том числе в деятельности органов внутренних дел. Большинство современных предприятий, работающих в любом направлении, не могут вести нормальную деятельность без уверенности в обеспечении безопасности своей информации. Нельзя забывать и про персональные компьютерные системы, связанные между собой сетью Интернет, на которых и тренируются взломщики.

Человека, пытающегося нарушить работу информационной системы или получить неразрешенный доступ к информации, называют взломщиком, а иногда «компьютерным пиратом» (хакером).

В общем смысле информация содержит сведения об окружающем нас мире, являющиеся объектом хранения, передачи, преобразования и использования их для определенных целей. Исходя из этого, человек размещается в постоянно изменяющемся информационном поле, влияющем на его действия и образ жизни. Информация по своему характеру может быть экономической, военной, политической, научно-технической, производственной или коммерческой. По степени секретности можно разделить информацию на секретную – конфиденциальную и несекретную.

К *секретной информации* относится информация, содержащая сведения, отнесенные к государственной тайне. А также отметим следующее, что *государственная тайна* – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации [1].

С современным развитием информационного общества очень большое значение приобретают проблемы, связанные с защитой конфиденциальной информации. Информация как категория, имеющая стоимость, защищается ее собственником от лиц и организаций, пытающихся завладеть ею любыми способами. В связи с этим складывается тенденция, что чем выше уровень секретности информации, тем выше и уровень ее защиты, а значит, тем больше средств затрачивается на ее защиту.

Высокую эффективность защиты информации можно определить как совокупность следующих факторов: своевременность, активность, непрерывность и комплексность. Очень важно проводить профилактические защитные мероприятия комплексно, т.е. гарантировать нейтрализацию всех опасных каналов утечки информации. Нельзя забывать, что один открытый канал утечки информации может свести на нет эффективность всей системы защиты.

Для защиты информации от утечки и снижения паразитных связей по техническим каналам используется ряд средств, представляющих собой комплекс проработанных мероприятий: экранирование электромагнитных волн, безопасность оптоволоконных кабельных систем, особенности слаботочных линий и сетей как каналов утечки информации [2]. Рассмотрим одно из основных – экранирование электромагнитных волн.

Экранирование электромагнитных волн является одним из самых действенных средств защиты объекта от утечки информации по техническим каналам и основой экологической безопасности.

Но для более эффективной защиты мало просто применить экранирование и развязывающие фильтры на каналы связи, но также в первую очередь необходимо устранять или ослаблять до допустимых значений паразитные связи путем следующих мероприятий:

– размещение вероятных источников и приемников наводок на максимально допустимом расстоянии друг от друга;

– сведение к минимуму общих сопротивлений;

– уменьшение сечения габаритов токонесущих элементов, обеспечивающих минимум паразитной связи (для получения минимальной

взаимоиндуктивности катушек индуктивности их оси должны быть взаимно перпендикулярны);

– изъятие посторонних проводов, проходящих через несколько узлов или блоков, которые могут связать элементы, расположенные на удаленном расстоянии друг от друга;

– при невозможности исключения посторонних проводов, создающих паразитную связь, необходимо позаботиться о том, чтобы при емкостной паразитной связи сопротивление постороннего провода относительно корпуса было минимальным, при индуктивной паразитной связи необходимо увеличивать внутреннее сопротивление посторонней линии связи;

– это локализация электромагнитной энергии в пределах определенного пространства путем преграждения ее распространения.

Развязывающий фильтр – это устройство, ограничивающее распространение помехи по проводам, являющимся общими для источника и приемника наводки.

В настоящее время все актуальней становится проблема формирования электромагнитной обстановки, обеспечивающей нормальное функционирование электронных устройств и экологическую безопасность.

Для создания благоприятной электромагнитной обстановки и обеспечения требований по электромагнитной безопасности объекта, которая включает в себя и предотвращение несанкционированного доступа к информации с использованием специальных технических средств, производится экранирование электромагнитных волн.

Применение качественных экранов позволяет решить многие задачи, в которые входит защита информации в помещениях и технических каналах, электромагнитную совместимость оборудования и приборов при совместном использовании, защиту персонала от повышенного уровня электромагнитных полей и обеспечение безопасной экологической обстановки вокруг работающих электроустановок и СВЧ-устройств.

ЛИТЕРАТУРА

1. ГОСТ Р 51624-2000. Автоматизированные системы в защищенном исполнении. Система стандартов. Основные положения. Введ. от 30.06.2000.

2. Зайцев А.П. Технические средства и методы защиты информации: учеб. для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. М.: Горячая линия – Телеком, 2009. 616 с.

БЕЗОПАСНАЯ СИСТЕМА ДЕЦЕНТРАЛИЗОВАННОГО ХРАНЕНИЯ ДАННЫХ

А.Е. Максимов, студент магистратуры, каф. ПФЭиИБ
Научный руководитель В.В. Поляков, проф., д.ф.-м.н.
г. Барнаул, АлтГУ, 10btik@gmail.com

Стремительно возрастающий объем обрабатываемой информации, среди которой есть и конфиденциальные данные, требует новых подходов с точки зрения ее хранения [1, 2]. Системы, в которых обрабатываемая информация не сосредоточена в одном месте (на одном сервере), а распределяется по различным узлам, применяются в системах электронной коммерции, мультимедийных системах и др. Задачей распределенного файлового хранилища является хранение программ и данных и предоставление к ним доступа по мере необходимости [3]. Условиями, которым должны удовлетворять системы распределенного хранения данных, являются [3]: открытая архитектура, прозрачность размещения файлов, независимость размещения файлов, мобильность клиента, мобильность файлов, устойчивость к сбоям, расширяемость. При этом необходимо обеспечивать конфиденциальность хранимых данных узлами распределенной системы от несанкционированного доступа при компрометации узла, а также их целостность.

Целью данной работы является создание модели безопасной системы распределенного хранения данных, удовлетворяющей обозначенным условиям.

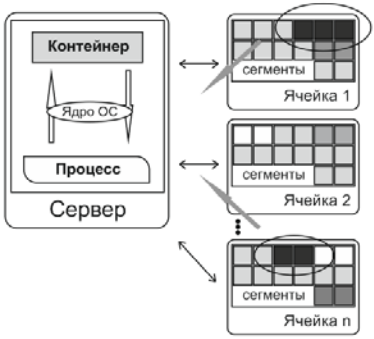


Рис. 1. Принцип работы системы

Система, предлагаемая в данной статье, работает следующим образом (рис. 1): на автоматизированном рабочем месте, которое в дальнейшем называется сервер, создается специальная логическая область хранения данных, называемая контейнером. Каждый файл в контейнере хранится частями, называемыми сегментами файла, распределенными по другим специально выделенным автоматизированным системам, называемым ячейками хранения данных. При обращении к файлу из контейнера неким процессом ядро ОС сервера перехватывает такой запрос, получает запрашиваемые сегменты файла с ячеек и отдает его процессу.

Сервер имеет базу данных, в которой содержится вся информация о хранящихся в распределенной области файлах. Такая база данных содержит имя файла, размер файла, путь к файлу, идентификатор фай-

ла, контрольную сумму, количество сегментов, на которое разбит файл, имена ячеек, на которых хранятся сегменты, а также дополнительную информацию, например права доступа к файлу.

Каждая ячейка хранения также содержит базу данных, содержащую информацию об имеющихся в ячейке сегментах. Такая база данных состоит из двух таблиц: сегментной и файловой. Сегментная таблица полностью описывает свойства каждого сегмента. Вторая таблица (файловая) содержит информацию о файле, части которого содержатся в ячейке. Фактически это таблица дублирует таблицу, хранящуюся на сервере, с тем лишь отличием, что в ней хранится информация о файлах, сегменты которых хранит данная ячейка. Она предназначена для того, чтобы восстановить все данные, которые должен был хранить сервер, в случае выхода его из строя.

Процесс добавления файла происходит следующим образом: сервер делит файл на сегменты, опрашивает и выбирает дополнительные серверы (ячейки) в зависимости от свободного пространства и загруженности. Далее делает соответствующую запись в своей базе данных и передает каждый сегмент файла на выбранные ячейки. При получении сегмента ячейка, в свою очередь, делает соответствующую запись в сегментной и, при необходимости, если в ней не хранится ни один сегмент передаваемого файла, запись в файловой таблице.

При чтении некоторой части файла из контейнера процессом сервер получает список ячеек, на которых распределен запрашиваемый файл, после чего определяет, в какой ячейке хранится нужный сегмент, далее происходит его передача на сервер и предоставление запрашиваемых данных процессу (рис. 2).

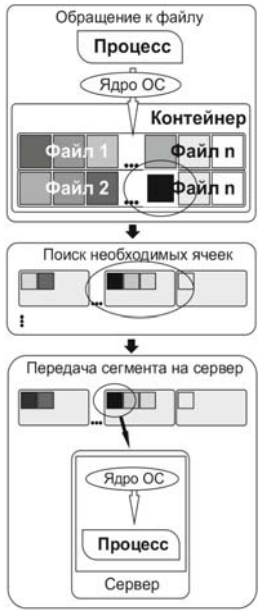


Рис. 2. Процесс чтения файла из контейнера

При запросе на изменение файла главный сервер извлекает информацию об изменяемом файле и обращается к тем ячейкам, которые хранят изменяемые сегменты. Каждая из таких ячеек перезаписывает изменяемый сегмент новым.

В соответствующих таблицах баз данных на ячейках и сервере информация о файле обновляется (размер файла, контрольная сумма, количество сегментов). Стоит отметить, что перезаписываются только те сегменты в ячейках, которые были подвержены изменению, остальные же сегменты остаются неизменными.

Заключение. Предлагаемая система удовлетворяет обозначенным в начале статьи условиям. В соответствии с архитектурой, механизм размещения файлов в системе является прозрачным и независимым. Данная система обладает свойством расширяемости: добавление новой ячейки хранения не вызывает дополнительных трудозатрат. В отличие от аналогичных существующих решений, например от проекта Hadoop, рассматриваемая система обладает устойчивостью к сбоям или к полному выходу из строя сервера. В таком случае всю информацию, которой он оперировал, возможно восстановить благодаря существующим БД на ячейках, в которых зафиксирована вся информация, связанная с исходными файлами, сегменты которых на них хранятся. При этом необходимо отметить, что обеспечение целостности данных, находящихся на самих ячейках, не обеспечивается, что является недостатком, требующим дополнительной проработки. Конфиденциальность данных, находящихся в ячейках, обеспечивает тот факт, что при компрометации ячейки злоумышленник не сможет извлечь из хранящихся сегментов какую-либо полезную информацию.

Предложенная система может найти применение в организациях, обрабатывающих большой объем информации, требующей большого дискового пространства и обеспечения ее безопасного хранения.

ЛИТЕРАТУРА

1. Клеменков П.А. Большие данные: современные подходы к хранению и обработке / П.А. Клеменков, С.Д. Кузнецов // Труды Института системного программирования РАН. 2012. Т. 23. С. 143–154.

2. Посконин А. Web-приложения и данные: проблемы абстракции и масштабируемости // Труды Института системного программирования РАН. 2012. Т. 23. С. 159–169.

3. Лукьянов Н.М. Анализ факторов, влияющих на качественные и количественные показатели функционирования систем распределенного хранилища данных / Н.М. Лукьянов, В.В. Кирилов // Науч.-техн. вестник информационных технологий, механики и оптики. 2008. № 56. С. 9–17.

АНАЛИЗ ЗАЩИЩЕННОСТИ ОБЪЕКТА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ В РАМКАХ АТТЕСТАЦИИ

А.А. Межевалов, студент

г. Томск, ТУСУР, каф. КИБЭВС, sk665@mail.ru

Научно-техническая революция в последнее время приняла огромные масштабы в области информатизации общества на базе современных средств вычислительной техники, связи, а также современных

методов автоматизированной обработки информации. Владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха в любом виде деятельности. Государственные структуры также нуждаются в этом. Однако нередко бывает так, что они обрабатывают информацию для ограниченного круга лиц, то есть имеющую определенную степень секретности. Для такой информации необходимо иметь объект обработки, который обладает степенью защищенности соответствующей степени секретности обрабатываемой информации. Присвоение объекту информатизации степени защищенности называется аттестацией объекта.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «аттестата соответствия» – подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК (Гостехкомиссией) России. Наличие на объекте информатизации действующего «аттестата соответствия» дает право обработки информации с уровнем секретности и на период времени, установленными в «аттестате соответствия».

Начальная стадия работ по подготовке помещения к аттестации включает в себя общее исследование структуры организации и составление основных документов, относительно которых будет строиться дальнейшая работа по обеспечению информационной безопасности (составляться модель угроз, рассматриваться определенный тип нарушителей, технический канал утечки информации и многое другое). Первоначальный список документов следующий:

– перечень сведений конфиденциального характера;

– распоряжение о назначении администратора безопасности АС и пользователей АС;

– акт категорирования объекта информатизации;

– акт классификации объекта информатизации;

– распоряжение об утверждении контролируемой зоны (далее – КЗ);

– матрица доступа;

– модель угроз и вероятностного нарушителя;

– технический паспорт объекта информатизации.

После составления этих документов можно делать выводы относительно того, какие каналы утечки конфиденциальной информации представляют наибольшую опасность, и работать над защитой от утечек по этим каналам.

Дальше происходит анализ защищенности объекта ВТ, который происходит в результате непосредственного обследования объекта информатизации и проведения измерений и инструментально-расчет-

ных оценок защищенности помещения. Результаты этих измерений дают реальную оценку того, есть ли необходимость в установке средств защиты или нет.

Оценочные мероприятия играют огромную роль при аттестации помещений. По их результатам делается анализ для определения подходящих методов защиты (активные, пассивные) и экономическое обоснование выбора методов и средств.

СТЕГАНОГРАФИЧЕСКОЕ СОКРЫТИЕ ИНФОРМАЦИИ С ПОМОЩЬЮ КЛЕТОЧНЫХ АВТОМАТОВ

Е.В. Негачева, студентка
Научный руководитель О.О. Евсютин, преподаватель
г. Томск, ТУСУР, каф. КИБЭВС

В настоящее время актуальна проблема передачи секретной информации по незащищенным каналам сети Internet. При этом необходимо, чтобы такая информация не стала доступной третьему лицу. Кроме того, недостаточно сделать информацию недоступной для нарушителя, зачастую требуется скрыть сам факт ее передачи.

Стеганография – набор средств и методов передачи информации с сокрытием факта передачи сообщения. Первоочередной задачей стеганографических методов является сокрытие самого существования канала связи.

В настоящее время стеганографические методы защиты информации являются одним из современных способов обеспечения информационной безопасности. В данной работе была поставлена задача разработки подходов к стеганографическому сокрытию информации, основанных на использовании математического аппарата теории клеточных автоматов.

Усиление метода LSB посредством применения обратимого клеточного автомата. Известный стеганографический метод сокрытия информации в цифровых изображениях, называемый методом наименьших значащих бит (LSB), был усилен путем применения обратимого клеточного автомата.

Недостаток метода состоит в том, статистические характеристики сокрытого сообщения будут отличаться от характеристик случайной последовательности, которую должны представлять собой младшие биты RGB-изображения, собранные вместе.

Обратимый клеточный автомат – это клеточный автомат, история развития которого является детерминированной в обоих направлениях

времени. Обратимость клеточных автоматов достигается применением специальных обратимых правил.

Перед тем как информация встраивается в изображение, она проходит предварительную обработку по следующему алгоритму.

Шаг 1: Задается правило, по которому будет работать клеточный автомат. Оно определяется одномерным массивом из 512 элементов, значения которых образуют некоторую перестановку всех чисел от 0 до 511.

Шаг 2: Определяется число шагов развития клеточного автомата. На этапе сокрытия информации данное значение указывается пользователем. Во время обратного преобразования клеточный автомат сам определяет это значение.

Шаг 3: Текст, уже переведенный в двоичное представление, представляется в виде решетки клеточного автомата, после чего разбивается на блоки в соответствии с заданными схемами разбиения.

Шаг 4: Состояние каждого блока представляется в виде десятичного числа. Исходное состояние блока определяет номер элемента в правиле, а значение этого элемента будет новым состоянием блока. Данное десятичное число переводится в двоичный код и представляется в виде блока решетки.

Шаг 5: Шаг 4 повторяется для всех блоков.

Шаг 6: К решетке клеточного автомата применяется правило Марголуса, заключающееся в том, что в каждом блоке (размером 2x2 клетки) содержимое каждой клетки меняется местами с содержимым диагонально противоположной клетки. Разбиение происходит по двум схемам разбиения: четной и нечетной [1].

Извлечение данных проходит аналогичным образом только в обратном порядке. Но здесь клеточный автомат должен определить, сколько ему нужно сделать шагов для возвращения в исходное состояние. Для этого на каждом шаге клеточный автомат сравнивает начало и конец решетки, и как только они стали одинаковыми, прекращает работу.

Стеганографическое кодирование информации с помощью метода сжатия цифровых изображений на основе блочных клеточных автоматов. Метод сжатия цифровых изображений на основе блочных клеточных автоматов, рассматриваемый в [2, 3], может быть описан следующей последовательностью этапов.

1. Предварительная обработка цифрового изображения (перевод в цветовую модель YCbCr).

2. Декоррелирующее клеточное преобразование.

3. Квантование преобразованных элементов данных.

4. Формирование массива серий квантованных элементов данных.

5. Удаление дубликатов из получившегося массива.

6. Арифметическое кодирование.

Обратное преобразование происходит аналогичным образом в обратном порядке.

В результате анализа метода сжатия цифровых изображений на основе блочных клеточных автоматов был выбран следующий способ последующего встраивания информации в изображение.

После того как прошел этап квантования с последующим округлением, среди квантовых значений высокочастотных составляющих появляется большое количество малых целочисленных значений, а именно: 0, ±1,±2 и т.д.

Значения, получившиеся после преобразований, равные 0 и 1, являются наименее значимыми, т.е. если их заменить на обратные значения (например, 0 на 1 или наоборот), это не сильно повредит изображению. Эти значения и будем использовать для встраивания секретной информации в преобразованный элемент данных. Предполагается, что в каждом из элементов может быть закодирован 1 бит информации.

ЛИТЕРАТУРА

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

2. Евсютин О.О. Метод сжатия цифровых изображений на основе блочных клеточных автоматов: автореф. дис. ... канд. техн. наук: 05.13.11. Томск, 2012. 16 с.

3. Евсютин О.О. Сжатие цифровых изображений, используемых в геоинформационной системе электронного генерального плана промышленного предприятия / О.О. Евсютин, М.М. Милихин // Доклады ТУСУРа. 2012. № 2 (26), ч. 1. С. 224–229.

ОРГАНИЗАЦИЯ АКТИВНОГО МОНИТОРИНГА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

К.С. Нестеров, студент каф. ИБ

Научный руководитель А.А. Лисс

г. Новосибирск, НГУЭУ, pardusurbanus@yandex.ru

В настоящее время большинство существующего в корпоративных локальных сетях программного и программно-аппаратного обеспечения обладает собственными журналами регистрации событий. Каждый такой журнал, как правило, использует собственный уникальный набор фиксируемых параметров. Учитывая, что распределённые информационные системы, состоящие из разнородных элементов, могут производить гигабайты журналов ежедневно, анализ всей совокупности сохра-

ненных в них событий становится задачей, не сопоставимой с понятием оперативности. Своевременное реагирование на события всего перечня журналов с целью предотвращения нарушений безопасности информации в условиях высокой динамики локальных сетей является актуальной и вместе с тем трудоёмкой задачей. В настоящей работе, в качестве решения обозначенной проблемы предлагается к рассмотрению модель системы активного мониторинга безопасности информации и её реализация на прикладном уровне.

На первом этапе – этапе поиска решения – были изучены существующие методы и средства защиты от информационных атак и мониторинга безопасности информации.

По спектру решаемых задач мониторинга безопасности информации были выбраны для дальнейшего рассмотрения СОА [1, с. 84] и SIEM-системы [2] (как более частное решение СОА).

Выявлено место проектируемой системы в классификации систем обнаружения атак [1, с. 86]. Проектируемую систему было решено отнести по типу используемых датчиков к системам обнаружения атак на уровне узла; по типу методов обработки данных – к централизованным системам обнаружения атак; по типу методов реагирования – к активным системам обнаружения атак; по назначению системы – к системам общего назначения. Данный выбор характеризует проектируемую систему как клиент-серверную, с централизованной обработкой данных, с опосредованным сбором информации через журналы безопасности операционных систем и приложений.

На втором этапе на основании проведённого анализа была разработана концептуальная схема системы активного мониторинга безопасности информации (далее – АМБИ), представленная на рис. 1.

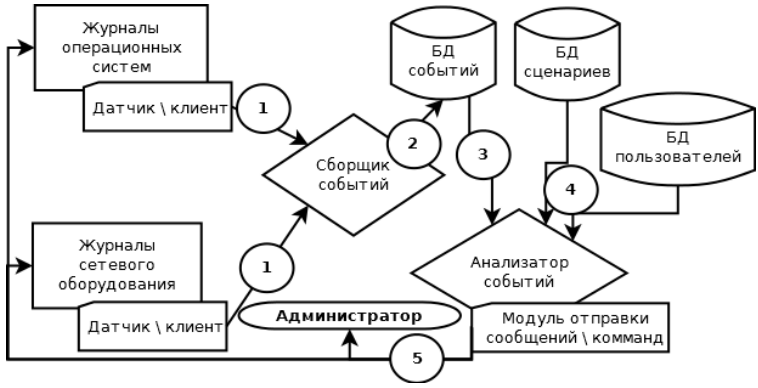


Рис. 1. Концептуальная схема АМБИ

Схема взаимодействия элементов системы следующая:

1. На первом этапе работы системы предварительно устанавливаемые на контролируемые рабочие места и настроенные на сетевом оборудовании датчики считывают журнальную запись. Датчики принимают решение об отнесении записи к категории рассматриваемых и отсылают запись на сервер.

2. На сервере входящие записи принимает сборщик событий, записывающий их в базу данных.

3. На следующем этапе анализатор событий считывает записи из базы данных для дальнейшей обработки.

4. Далее анализатор событий сравнивает полученные записи базы данных с заранее подготовленными сценариями инцидентов информационной безопасности. Сценарии описывают код события, тип системы, для которой событие характерно, краткое сообщение для отправки оповещения конкретному пользователю или администратору безопасности, код команды управления (воздействия) на удалённую систему.

5. При принятии решения об отнесении события или группы событий к опасным или потенциально опасным анализатор событий, при помощи модуля отправки сообщений и команд производит оповещение уполномоченного лица (администратора) и в отдельных случаях воздействие на удалённую систему. Виды воздействия соответствуют заранее определённым функциям прикладного программного интерфейса удалённой системы.

На третьем этапе решения были выдвинуты функциональные требования к системе, сформирована технологическая основа реализуемого прототипа системы (рис. 2).

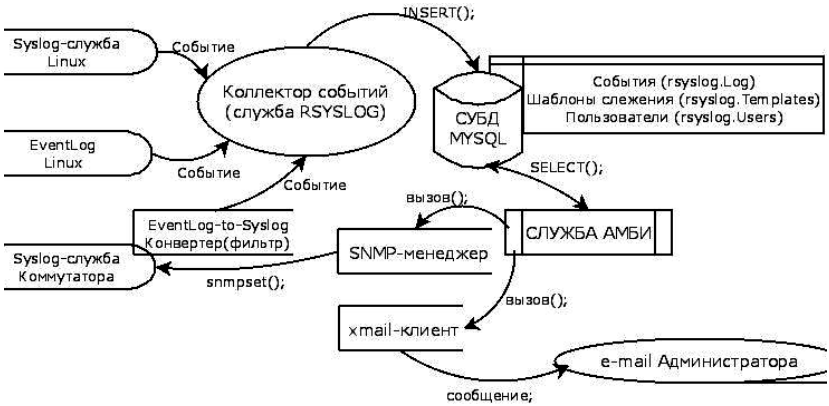


Рис. 2. Прототип АМБИ

Предложенное решение позволяет выполнять требования по анализу информации журналов регистрации событий в распределённой и неоднородной по используемому программному обеспечению корпоративной локальной сети. Фактором кроссплатформенности решения является использование общепринятых технологий и средств. Выбранная технологическая основа реализации не зависит от единого производителя и технологий, выбранные средства являются программным обеспечением с открытым кодом, что позволяет производить необходимую корректировку функциональных возможностей. Выполнимы требования по ежедневному анализу журнальной информации с прикладных систем за счёт непрерывного процесса анализа и сбора.

Система является легко расширяемой за счёт отсутствия привязки к числу наблюдаемых в системе объектов. Все полученные записи, приведённые к единому синтаксису, хранятся на серверной стороне. Система имеет возможность расширения поля анализа инцидентов безопасности за счёт добавления новых сценариев в базу данных сценариев инцидентов безопасности.

Система имеет возможность автоматизированного управления конечными устройствами за счёт использования SNMP-протокола. Также имеется возможность контроля работоспособности устройств в сети за счёт журналирования действий SNMP-протокола.

ЛИТЕРАТУРА

1. Сердюк В.А. Новое в защите от взлома корпоративных систем. М.: Техносфера, 2007. 360 с.

2. Magic Quadrant for Security Information and Event Management [Электронный ресурс]: Gartner RAS Core Research Note G00212454, Mark Nicolett, Kelly M. Kavanagh, 12 May 2011, RV4A105172012. Режим доступа: http://www.arcsight.com/collateral/whitepapers/Gartner_Magic_Quadrant_2011.pdf

СПОСОБ АЛГОРИТМИЧЕСКОЙ ОПТИМИЗАЦИИ ВЫЧИСЛЕНИЙ ЗНАЧЕНИЙ ОДНОСТОРОННЕЙ ХЭШ-ФУНКЦИИ MD4 НА ГРАФИЧЕСКИХ УСКОРИТЕЛЯХ

В.А. Новосядлый, зав. лаб., к. ф.-м. н., К.Д. Майзаков, науч. сотр., Д.А. Эдель, науч. сотр.

г. Ростов-на-Дону, ФГАНУ НИИ «Спецвузавтоматика», v.novosiadliy@niisva.org

Однонаправленные хэш-функции применяются тогда, когда необходимо вычислить от исходного прообраза некоторое значение, которое трудно получить, используя другой прообраз. Примерами являются обеспечение конфиденциальности хранимой информации в базе

данных (пользовательские пароли) или обеспечение проверки подлинности сообщения. Понижение фактической стойкости хэш-функ-ции может произойти благодаря существованию уязвимости, позволяющей снизить количество вычислений, необходимых для получения образа.

В данной работе рассмотрена практическая реализация алгоритмической уязвимости хэш-функции MD4 [1] на графических вычислителях с поддержкой технологии nVidia CUDA, позволяющая ускорить процесс восстановления прообраза. Проведено сравнение скорости реализованного алгоритма восстановления прообразов с существующими реализациями, а именно, с программным обеспечением (далее – ПО) восстановления прообразов «Extreme GPU Bruteforcer» и «oclHashcat-plus». В результате вычислительных экспериментов было установлено, что рассмотренное ПО восстановления прообразов односторонних хэш-функций не использует известные уязвимости хэш-функции MD4 для ускорения процесса восстановления.

Постановка задачи. Пусть однонаправленная хэш-функция H(M) применяется к прообразу M и возвращает значение h фиксированной длины m. Функция H(M) называется криптографической, если она является криптостойкой, а именно, удовлетворяет трем основным требованиям:

– устойчивость к нахождению прообраза. Для заданного h должно быть трудно найти такое M, что H(M) = h;

– устойчивость к нахождению второго прообраза. Для заданного M^1 должно быть сложно найти такое M^2, чтобы $H(M^1) = H(M^2)$;

– устойчивость к коллизиям. Должно быть сложно найти такую пару M^1 и M^2, чтобы $H(M^1) = H(M^2)$.

В данной работе сосредоточимся на задаче восстановления прообраза. Несмотря на то, что хэш-фунция MD4 не является криптостойкой и считается устаревшей, она продолжает использоваться для обеспечения конфиденциальности паролей пользователей ОС семейства Windows (алгоритмы NT [2] и MS-CACHE [3]). В работах [4–6] описаны уязвимости, позволяющие ускорять восстановление прообразов длиной 512 байт. В данном случае эти результаты использовать не представляется возможным из-за ограничений на длину пароля.

Описание уязвимости. Алгоритм вычисления хэш-функции MD4 состоит из 48 шагов, разделенных на три раунда. Оказывается, что, начиная с шага 34, хэширующие преобразования не затрагивают первые четыре байта входного массива данных. Назовем предхэшем значение, полученное из заданного h путем применения к нему преобразований, обратных к шагам 34–48 хэширующих преобразований MD4. Тогда для проверки того, что последовательность входных байт не является искомым прообразом, в подавляющем большинстве случаев достаточно произвести не 48, а 33 шага, таким образом, получая алго-

ритмическое ускорение вычислений приблизительно в 1,455 раза. Описанная алгоритмическая уязвимость аналогична уязвимости хэш-функции MD5 [7, 8], которая впервые была использована в ПО «BarsWF».

Результаты экспериментальных вычислений. Приведенные результаты использованы при разработке ПО восстановления прообразов на графических вычислителях с поддержкой технологии nVidia CUDA. Разработанное ПО было использовано для получения экспериментальных результатов по скорости восстановления прообразов. Лабораторный стенд имел следующую конфигурацию: Intel Core i7 2,8 GHz, nVidia GTX 680, 8GB RAM. Проводилось восстановление прообразов длиной 9 символов с алфавитом, состоящим из прописных и строчных латинских символов и цифр (a-z, A-Z, 0-9). Получены следующие результаты по скорости функционирования ПО:

– ПО «Extreme GPU Bruteforcer» – 1270 млн/с;

– ПО «oclHashcat-plus» – 2345 млн/с;

– разработанное ПО – 3241 млн/с.

Таким образом, можно сделать вывод о том, что использование алгоритмической уязвимости односторонней хэш-функции MD4 позволяет существенно ускорить процесс восстановления прообразов по сравнению с существующим ПО.

ЛИТЕРАТУРА

1. Rivest R. MD4 Algorithm. Network Working Group, Request for Comments: 1320 // MIT Laboratory for Computer Science and RSA Data Security. Inc., 1992.

2. Passwords Technical Overview // MSDN. http://technet.microsoft.com/en-us/library/hh994558%28v=ws.10%29.aspx. 2012.

3. MSCash Algorithm // Openwall Community Wiki. http://openwall.info/wiki/john/MSCash. 2010.

4. Dobbertin H. The First Two Rounds of MD4 are Not One-Way // Fast Software Encryption – FSE'98, LNCS 1372. 1998. С. 284–292.

5. Kuwakado H., Tanaka H. New Algorithm for Finding Preimages in a Reduced Version of the MD4 Compression Function // IEICE Trans. Fundamentals. 2000. Vol. E83–A. № 1. С. 97–100.

6. Aoki K., Sasaki Y. Preimage attacks on one-block MD4, 63-step MD5 and more // Selected Areas in Cryptography. Lecture Notes in Computer Science. 2009. Vol. 5381. С. 103–119.

7. Rivest R. MD5 Algorithm. Network Working Group, Request for Comments: 1321 // MIT Laboratory for Computer Science and RSA Data Security, Inc., 1992.

8. Майзаков К.Д., Эдель Д.А., Новосядлый В.А. Способ эффективного вычисления прообразов хэш-функции MD5 // Матер. 7-й Всерос. науч.-практ. конф. «Перспективные системы и задачи управления». Таганрог: Изд-во ТТИ ЮФУ, 2012. 327 с.

АНАЛИЗ ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЯ В РАМКАХ АТТЕСТАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

А.А. Поляков, студент
г. Томск, ТУСУР, каф. КИБЭВС, koshachy@gmail.com

В настоящее время огромное количество информации обрабатывается на специализированных средствах вычислительной техники. Естественно, что информация, представляющая какой-либо коммерческий интерес или тайну, защищается различными программными или программно-аппаратными средствами и комплексами, которые обеспечивают безопасность информации, являющейся конфиденциальной. Но также довольно часто источниками информации являются непосредственно люди, владеющие этой информацией, и обрабатывается она также людьми, без помощи каких-либо технических средств.

Под акустической информацией обычно понимается информация, носителями которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой. Первичными источниками акустических сигналов являются механические колебательные системы, например органы речи человека, а вторичными – преобразователи различного типа, например громкоговорители.

Для обеспечения безопасности речевой информации обмен этой информацией происходит в специализированных помещениях, в которые не имеют допуск посторонние люди, не участвующие в обработке информации. Такие помещения проходят специальную аттестацию, процесс которой заключается в изучении всех возможных каналов утечки информации и проведении специальных мер для предотвращения утечки конфиденциальной информации. Аттестация защищаемого помещения представляет собой доказательство соответствия этого помещения определенным критериям, которые утверждаются уполномоченными на то организациями. Документация, составляемая для прохождения аттестации, имеет общий тип и структуру, но в каждом конкретном случае она зависит от организации, которой принадлежит аттестуемое помещение. Именно поэтому существует много компаний, осуществляющих помощь в аттестации объектов информатизации [1].

Начальная стадия работ по подготовке помещения к аттестации включает в себя общее исследование структуры организации и составление основных документов, относительно которых будет строиться дальнейшая работа по обеспечению информационной безопасности (составляться модель угроз, рассматриваться определенный тип нару-

шителей, технический канал утечки информации и многое другое). Первоначальный список документов следующий:

– перечень сведений конфиденциального характера;

– список лиц, имеющих доступ к сведениям конфиденциального характера;

– распоряжение о назначении ответственного за защищаемое помещение (далее – ЗП);

– акт категорирования (классификации) объекта информатизации;

– распоряжение об утверждении контролируемой зоны (далее – КЗ);

– модель угроз и вероятностного нарушителя;

– технический паспорт объекта информатизации.

После составления этих документов можно делать выводы относительно того, какие каналы утечки конфиденциальной информации представляют наибольшую опасность, и работать над защитой от утечек по этим каналам, ведь на руках имеется вся необходимая информация о ЗП.

Под утечкой информации по техническому каналу понимается неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации [2].

Анализ защищенности помещения происходит в результате непосредственного обследования помещения и проведения измерений и инструментально-расчетных оценок защищенности помещения. Результаты этих измерений дают реальную оценку того, есть ли необходимость в установке средств защиты или нет.

Задача перед подготовкой помещения к аттестации – не допустить утечки информации. Поэтому проводятся различные мероприятия по оценке защищенности помещения.

Оценочные мероприятия играют огромную роль при аттестации помещений. По их результатам делается анализ для определение подходящих методов защиты (активные, пассивные) и экономическое обоснование выбора методов и средств.

ЛИТЕРАТУРА

1. Аттестация объектов информатизации [Электронный ресурс]. Электрон. текст. дан. [Б.м.], 2012. URL: http://samlib.ru/l/loclay/woprosypotemeattestacijaobxektowinformatizacii.shtml

2. Хорев А.А. Защита информации от утечки по техническим каналам. Ч. 1. Технические каналы утечки информации. М., 1997, 250 с.

КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАВИСИМОСТИ ОТ УГРОЗ

Д.В. Поляков, студент каф. КИБЭВС
Научный руководитель А.А. Конев, доцент каф. КИБЭВС
г. Томск, ТУСУР, dmitriy.polyakov.mailbox@gmail.com

Важным аспектом в вопросе защиты информации является определение полного перечня угроз для самой информации, чтобы в будущем использовать перечень выявленных угроз для конкретной системы. Большую важность имеют полнота и актуальность перечня угроз, так как при отсутствии какого-либо элемента вероятность реализации угрозы резко возрастает, и владелец информации может понести ущерб.

Для выявления угроз безопасности информации потребуется модель документооборота для различных типов состояний информации и сред обработки, представленная в виде мультиграфа (рис. 1). Документооборот – движение документов в организации с момента их создания или получения до завершения исполнения или отправления [1].

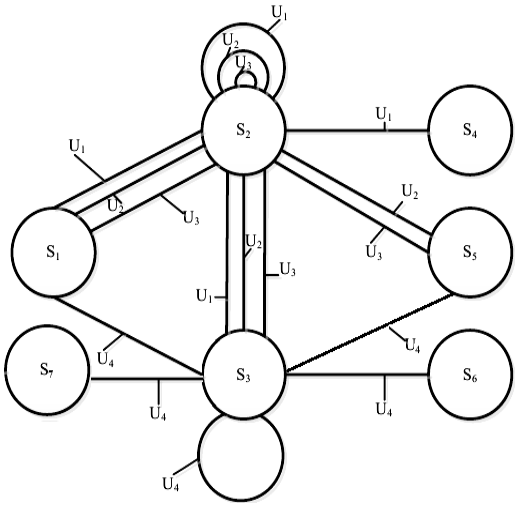


Рис. 1. Модель документооборота

Множество документопотоков G={S, U}, множество состояний S={s1, s2, s3, s4, s5, s6}. Элементы множества состояний S: s1 – место хранения информации (жесткий диск, flash-накопитель, документ, аудиокассета, видеокассета); s2 – человек; s3 – процесс; s4 – почтовый пакет; s5 – радиограмма/телефонное сообщение; s6 – сетевой пакет.

Множество каналов передачи информации U={u1, u2, u3, u4};

u1 – физический канал передачи информации; u2 – видовой канал передачи информации; u3 – акустический канал передачи информации; u4 – виртуальный канал передачи информации.

Для удобства определения средств защиты информации потребуется разделение данных средств на типы и подтипы (рис. 2).

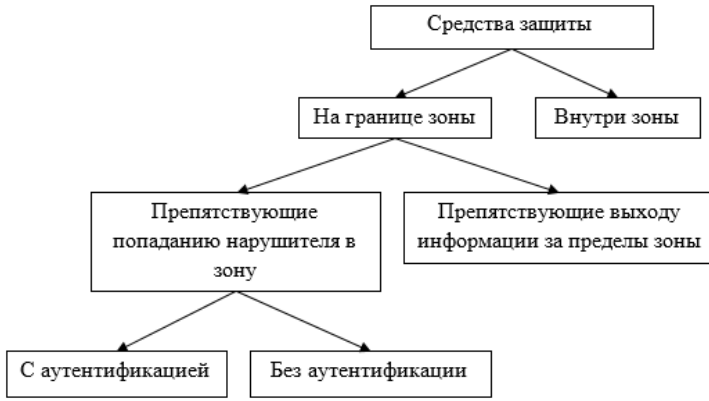


Рис. 2. Классификация средств защиты информации

Выявленные угрозы информации для каждой среды обработки сопоставляются со средствами защиты, определенными в соответствии с классификацией, указанной выше. Таким образом, получается полный перечень угроз информации и средств, обеспечивающих защиту от данных угроз.

ЛИТЕРАТУРА

1. ГОСТ Р 51141–98, [Электронный ресурс]. Режим доступа: http://vsegost.com/Catalog/35/3595.shtml, свободный. Загл. с экрана.

ОСНОВНЫЕ МЕТОДЫ И ПРОБЛЕМЫ В ОБЛАСТИ ИДЕНТИФИКАЦИИ ДИКТОРА ПО ГОЛОСУ

И.А. Рахманенко, аспирант
Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, ria@keva.tusur.ru

Актуальность проблемы идентификации диктора по голосу в настоящее время не поддается сомнению. В связи с большим распространением мобильных устройств, обладающих микрофоном приемлемого качества, систем голосовой коммуникации в сети Internet, телефонных систем автоматического обслуживания, появляется потребность в идентификации конкретных пользователей систем. Также имеется необходимость в использовании систем идентификации диктора в таких областях, как криминалистическая экспертиза, антитеррористическая деятельность, в системах разграничения доступа, в банковском деле, для разметки звуковых стенограмм.

Системы, распознающие диктора по голосу, можно разделить на 2 вида: системы, позволяющие идентифицировать конкретного человека, и системы, подтверждающие (верифицирующие) личность. Кроме того, существуют схожие по цели системы, позволяющие отделить одного диктора от другого в потоке слитной речи [1].

Известно использование голосовой аутентификации совместно с распознаванием личной подписи [2]. Данная система была протестирована на базе данных из 50 пользователей, для каждого из которых имеется 10 образцов речевой информации и 10 образцов подписей. Итоговый коэффициент Equal Error Rate (EER) составил 0,86%. Данный показатель используется для сравнения различных методов распознавания диктора. Он определяет ошибку распознавания при условии равенства вероятности пропуска самозванца и отказа законному пользователю [3].

С момента появления первых систем распознавания диктора был поставлен вопрос о возможности подделки голоса целевого диктора. Как описано в [4], вероятность имитации голоса достаточно мала, т.к. у имитатора нет возможности подделать глубинные факторы, определяющие индивидуальные свойства речи. Однако в настоящее время разрабатываются системы трансформации одного голоса в другой. Ошибка ложного распознавания при использовании таких систем повышается до 50% [5].

Отдельной проблемой при использовании фиксированных фраз для идентификации диктора является возможность их записи злоумышленником. Одним из способов решения данной проблемы является проверка записи на полную идентичность. Кроме того, на качество распознавания влияет отличие расположения и характеристик микрофона злоумышленника. Изменяются также и частотные характеристики речевого сигнала за счет влияния звукового тракта (микрофона и звуковоспроизводящей системы) злоумышленника.

В работах по распознаванию диктора доминирует метод кепстрального преобразования спектра речевых сигналов (метод впервые предложен в [6]). Схема этого метода такова: на интервале времени в 10–20 мс вычисляется текущий спектр мощности, а затем применяется обратное преобразование Фурье от логарифма этого спектра (кепстр), и находятся коэффициенты кепстра [3].

Коэффициенты кепстрального преобразования формируют пространство, в котором и производится распознавание диктора. Эти коэффициенты сокращенно обозначаются как MFCC – Mel Frequiency Cepstral Coefficients. Число используемых коэффициентов от 10 до 30. Часто используются первые и вторые разности по времени кепстральных коэффициентов, что втрое увеличивает размерность пространства

принятия решений, но улучшает эффективность распознавания диктора [7].

В силу того, что в подавляющем большинстве систем распознавания диктора используется одно и то же пространство признаков в идее кепстральных коэффициентов, их первых и вторых разностей, основное внимание уделяется построению решающих правил. Наиболее популярны метод аппроксимации плотности вероятности в пространстве признаков взвешенной смесью нормальных распределений (GMM – Gauss Mixture Models), метод опорных векторов (SVM – Support Vector Machines), метод скрытых Марковских моделей (HMM – Hidden Markov Models), искусственные нейронные сети, а также модификации факторного анализа [3].

ЛИТЕРАТУРА

1. Campbell J. Speaker recognition: a tutorial / Proc. IEEE,. 1997. Vol. 85, №9. P. 1437–1462.

2. Krawczyk S. Securing Electronic Medical Records using Biometric Authentication / S. Krawczyk, Anil K. Jain. AVBPA'05 Proceedings of the 5th international conference on Audio- and Video-Based Biometric Person Authentication. P. 1110–1119.

3. Сорокин В.Н., Вьюгин В.В., Тананыкин А.А. Распознавание личности по голосу: аналит. обзор / Информационные процессы. Т. 12, №1. С. 1–30.

4. Rosenberg A. Automatic speaker recognition / Proc. IEEE. 1976. Vol. 64, №4. P. 475–478.

5. Bonastre J.-F., Matrouf D., Fredouille C. Artificial impostor voice transformation effects on false acceptance rates / In: Proc. Interspeech 2007 (ICSLP). Antwerp, Belgium. August 2007. P. 2053–2056.

6. Davis S., Mermelstein P. Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences / IEEE Trans. Acoustics, Speech, Signal Process. 1980. Vol. 28, №4. P. 357–366.

7. Zhang Sh.-X, Mak M.-W. A new adaptation approach to high-level speaker-model creation in speaker verification // Speech Communication. 2009. Vol. 51. P. 534–550.

НОСИТЕЛИ С НЕИЗВЛЕКАЕМЫМ ЗАКРЫТЫМ КЛЮЧОМ – НОВЫЙ ПОДХОД К БЕЗОПАСНОСТИ

Д.С. Ризванов, студент, Н.С. Михайлов, аспирант

г. Томск, ТУСУР, каф. КИБЭВС, dinar-sama@yandex.ru

Проект ГПО КИБЭВС 1213 – «Криптоменеджер»

Замки, как гласит известная поговорка, предназначены для защиты собственности от честных людей. Ибо человек способен взломать любой код, придуманный человеком, – весь вопрос в том, сколько

времени и усилий для этого потребуется. Именно из такого принципа исходят разработчики всех алгоритмов и устройств шифрования. Зачастую данные необходимо оградить от любопытных глаз, это может быть бухгалтерия, компромат, личная переписка и т.п. Государственные секреты, военные тайны принято доверять более солидным системам, использующим хранилища с неизвлекаемыми закрытыми ключами а для ежедневного использования может подойти портативное устройство – электронный токен.

Уже несколько лет на рынке средств защиты информации присутствуют так называемые аппаратные ключи защиты – токены, которые бывают двух видов: с извлекаемым и неизвлекаемым закрытым ключом. Они являются ярким примером двухфакторной аутентификации: pin-код и токен. Не зная пароля, никто не воспользуется ключом. Pin-код же становится простым набором цифр, если нет токена, к которому он принадлежит. В наше время наиболее широкое распространение получили ключи, выполненные в виде USB-брелоков и смарт-карт. Эти защищенные аппаратно-программные устройства предназначены для использования в инфраструктуре открытых ключей, платежных системах, системах доступа, в сетевой безопасности, в качестве электронного идентификатора, носителя ключевой информации, а также средства формирования электронной цифровой подписи. Их разработкой и продвижением в России занимаются такие компании, как «Мультисофт», «Актив», «Аладдин».

Решение eToken ГОСТ компании «Аладдин» представляет собой персональное средство формирования электронно-цифровой подписи с неизвлекаемым закрытым ключом. Он предназначен для использования в качестве интеллектуального ключевого носителя в защищенных системах, поддерживающих российские криптографические стандарты, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной цифровой подписи.

Большинство токенов выполнены на базе нового поколения электронных ключей с использованием языка Java, они имеют открытую архитектуру и возможность добавления требуемой функциональности путем загрузки в ключ Java-апплета (например, реализующего функции «электронного кошелька» и пр.).

Взаимодействие компьютера с USB-брелоком производится с помощью штатного CCID-драйвера, входящего в состав современных ОС. Благодаря этому обеспечивается возможность работы без установки дополнительных драйверов и ПО на разных платформах (Windows, Mac OS X, Linux).

Для использования носителей с извлекаемым закрытым ключом требуется персональный компьютер (ПК), с установленным средством криптографической защиты информации (СКЗИ), например: КриптоПро CSP, ЛИССИ-CSP, ViPNet CSP. СКЗИ, получив закрытый ключ, реализует формирование и проверку электронно-цифровой подписи согласно ГОСТ Р 34.10-2001, вычисление хэш-функции в соответствии с ГОСТ Р 34.11-94, выработку ключа парной связи по алгоритму Диффи–Хеллмана в соответствии с RFC 4357 и генерацию последовательности случайных чисел, используя вычислительные мощности компьютера. При этом электронный документооборот подвержен некоторой опасности со стороны злоумышленников, в частности, есть риск кражи закрытого ключа на стадии его передачи из токена в оперативную память ПК (рис. 1).

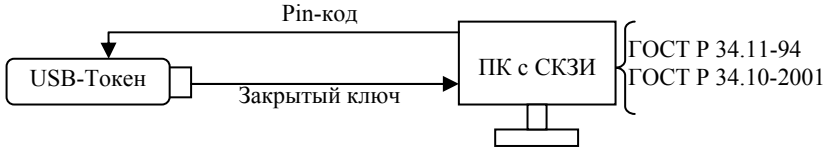


Рис. 1. Обмен информацией между ПК и токеном с извлекаемым закрытым ключом

Риск кражи отсутствует в носителях с неизвлекаемым закрытым ключом. Например, eToken ГОСТ реализует формирование и проверку электронно-цифровой подписи, вычисление хэш-функции, выработку ключа парной связи и генерацию последовательности случайных чисел, используя вычислительные мощности самого носителя, а не ПК, как в первом случае (рис. 2), что повышает сохранность закрытого ключа.

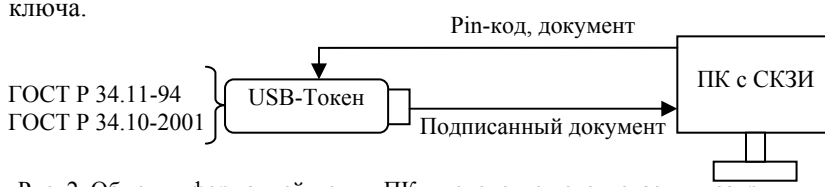


Рис. 2. Обмен информацией между ПК и токеном с неизвлекаемым закрытым ключом

Целевыми сферами применения таких устройств являются:

– Удаленный банковский клиент (система клиент–банк). С помощью ключа клиент подписывает электронно-цифровой подписью платежные поручения на аппаратном уровне.

– Защищенный документооборот. eToken используется для аутентификации пользователей системы.

– Системы сбора налоговой отчетности (предоставление налоговой отчетности в электронном виде). Ключи могут использоваться в системе ФНС и на клиентской стороне (организация, сдающая отчет).

– Системы сбора статистической отчетности (предоставление статистической отчетности в электронном виде). Ключи могут использоваться в системе Госкомстата России и на клиентской стороне (организация, сдающая статистический отчет).

– Органы власти и управления. Использование ЭЦП в органах государственной власти на федеральном и региональном уровнях.

Уже сейчас USB-ключи и смарт-карты являются неотъемлемой частью инфраструктуры информационной безопасности. Они поддерживаются всеми ведущими производителями информационных систем и бизнес-приложений, соответствуют требованиям российских регулирующих органов. В дальнейшем доля носителей с неизвлекаемым закрытым ключом будет только расти.

ЛИТЕРАТУРА

1. Скляров Д.В. Искусство защиты и взлома информации. М.: Изд. дом «Питер», 2004. 288 с.

2. Сигнал-КОМ – криптографическая защита информации. USB-ключи eToken компании «Аладдин» [Электронный ресурс]. URL: http://www.signal-com.ru (дата посещения: 10. 03. 2013).

ОЦЕНКА НАДЕЖНОСТИ СИСТЕМЫ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ

К.С. Рошкован, студент

Научный руководитель М.А. Сопов, ст. преподаватель

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

В связи с широким развитием информационных систем ключевой становится проблема обеспечения надежности их функционирования. Проработка вопросов, связанных с надежностью, должна осуществляться уже на этапе проектирования системы. 27 апреля 2012 г. вступил в силу приказ Федеральной службы безопасности №796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра», в котором сказано, что должны быть определены требования по надежности и устойчивости функционирования средств удостоверяющего центра (УЦ) [1]. Вместе с этим данный приказ не предлагает каких-либо указаний по расчету надежности, поэтому открытой остается проблема разработки методики, которая описывает процесс расчета надежности для системы УЦ.

Расчет надежности основывается на определении основных характеристик работоспособности УЦ. Из всех его функций, указанных в Федеральном законе №63 «Об электронной подписи», критичными для системы УЦ являются функции по формированию и публикации списков отозванных сертификатов (СОС). Исходя из этого, работоспособное состояние системы УЦ можно описать следующими условиями:

− в работоспособном состоянии должен находиться Центр сертификации (ЦС) каждого УЦ;

− возможен информационный обмен между всеми УЦ, входящими в систему.

Системы УЦ можно классифицировать в зависимости от реализуемой модели доверия. Самыми жизнеспособными оказались мостовая, иерархическая и сетевая модели. Наибольший интерес представляют такие показатели надежности, как вероятность безотказной работы (1) и коэффициент готовности (2) [2].

$$P(t) = \int_0^{\infty} a(t)dt \,, \tag{1}$$

где $a(t)$ – частота отказов, то есть плотность распределения времени работы до первого отказа.

$$K_{\Gamma} = \frac{T_{\text{о}}}{T_{\text{о}} + T_{\text{в}} + T_{\text{ож}}} \,, \tag{2}$$

где $T_{\text{о}}$ – полезное время работы системы; $T_{\text{в}}$ – время восстановления работоспособности системы; $T_{\text{ож}}$ – время ожидания начала восстановления.

Для того чтобы оценить надежности системы УЦ, необходимо определить порядок расчета надежности для каждой модели доверия. В данном отношении иерархическое и мостовое соединение ничем не отличаются, их надежность рассчитывается по (3) для последовательного включения элементов в систему [2]:

$$P(t) = \prod_{i=1}^{n} P_i(t) \,, \tag{3}$$

где $P_i(t)$ – вероятность безотказной работы i-го элемента структуры (УЦ и линии связи между ними), n – количество элементов.

Гораздо большую сложность представляет расчет надежности для сети УЦ, так как в ней возможно несколько вариантов маршрута информационного обмена, что существенно повышает его надежность. Существует несколько методов расчета надежности сети, но часть из них требует полного перебора всех состояний сети, другие же – при-

менимы для определенных сетевых структур и в общем случае не работают. Поэтому оценку надежности сети целесообразно осуществлять с помощью статистического моделирования методом Монте-Карло.

Суть метода Монте-Карло для оценки надежности сети состоит в проведении ряда статистических испытаний. Для примера рассмотрим схему сети в виде графа, изображенного на рис. 1.

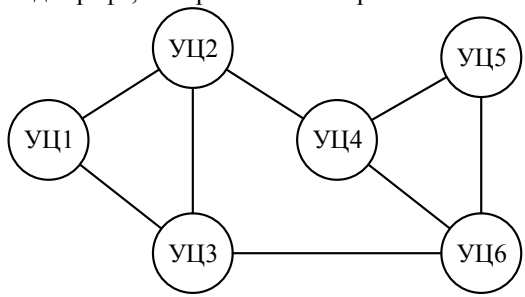


Рис. 1. Граф, описывающий пример сети УЦ

Для простоты условимся, что вершины графа абсолютно надежны. Каждое ребро характеризуется показателем надежности p_{ij}. Ребро может быть либо работоспособным, либо отказавшим, согласно закону распределения:

X 0 1;

P $1-p_{ij}$ p_{ij}.

Генерируется столько псевдослучайных чисел x_i, сколько ребер в графе, и затем сравниваются с p_{ij} [3]:

$x_i \le p_{ij}$ – элемент работает,

$x_i > p_{ij}$ – элемент отказал.

В результате испытания некоторые из ребер будут отказавшими, на рис. 2 они представлены пунктирными линиями.

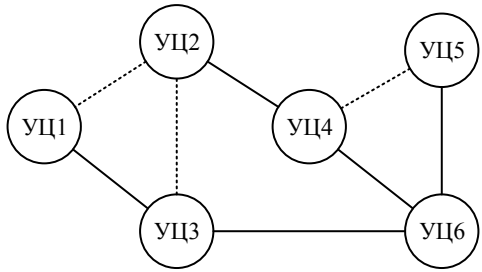


Рис. 2. Граф после испытания

Далее проверяется структурная целостность сети. В сети, изображенной на рис. 2, возможен информационный обмен между всем УЦ. В этом случае испытание считается успешным. Если остается хотя бы один УЦ, не связанный с другими (более одной компоненты связности графа), то испытание не засчитывается. Проводится достаточное количество статистических испытаний, после чего можно оценить надежность всей сети по формуле (4).

$$P = \frac{M}{N}, \tag{4}$$

где M – количество успешных испытаний; N – общее количество испытаний.

ЛИТЕРАТУРА

1. Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра: приказ Федеральной службы безопасности №796 от 27.12.2011.

2. Шелупанов А.А. Обеспечение надежности функционирования удостоверяющих центров: НИР / А.А. Шелупанов, Р.В. Мещеряков, Е.М. Давыдова и др. М., 2007. 65 с.

3. Гмурман В.Е. Теория вероятностей и математическая статистика: учеб. пособие для вузов. 9-е изд., стер. М.: Высш. шк., 2003. 479 с.

РЕАЛИЗАЦИЯ БАЗОВОЙ АРХИТЕКТУРЫ КРИПТОГРАФИЧЕСКОГО ПРОВАЙДЕРА В ЯЗЫКЕ JAVA

Р.В. Сёмин, студент каф. ИВЭ ЮФУ

г. Ростов-на-Дону, ФГАНУ НИИ «Спецвузавтоматика»,
r.semin@niisva.org

Комплект разработчика приложений Java Development Kit содержит стандартную библиотеку Java Cryptography Architecture [1] для работы с криптографией. Основной чертой данной библиотеки является независимость реализации, что достигается посредством использования провайдеров криптографических служб (Cryptographic Service Provider, CSP), далее именуемых как провайдеры. Провайдеры представляют собой своеобразные контейнеры, содержащие набор служб для работы с криптографией в среде Java. Вызов конкретной службы производится с использованием так называемой трансформации – строки, описывающей схему, по которой над входными данными будут произведены некие действия [1]. Трансформация всегда включает имя криптографического алгоритма, за которым могут следовать название режима и тип выравнивания. Например, для использования алгоритма AES [1] в режиме Cipher Block Chaining [2] с выравниванием

по стандарту PKCS5 [2] необходимо задать трансформацию вида «AES/CBC/PKCS5Padding».

Стандартная процедура включения новых компонентов шифрования в программную среду Java подразумевает создание собственной комплексной архитектуры, что не всегда удобно, особенно при реализации небольших приложений, требующих использования шифрования. Таким образом, создание базовой архитектуры криптографического провайдера обеспечит быстрое и удобное подключение собственных разработок и реализаций блочных шифров. При этом были проанализированы и использованы принципы и примеры, описанные в [3].

Реализация базовой архитектуры. При разработке архитектуры провайдера необходимо учитывать, что для удобства дальнейшего использования требуется создать набор классов и интерфейсов, позволяющих независимо друг от друга производить над входными данными различные преобразования, такие как выравнивание, применение режима шифрования блоков и др. [4]. Для этого следует использовать принцип вложенности, когда результат преобразования передаётся с нижних уровней архитектуры на верхние, и принцип модульности, позволяющий легко расширять и дополнять существующую архитектуру. Схема реализованной архитектуры представлена на рис. 1.

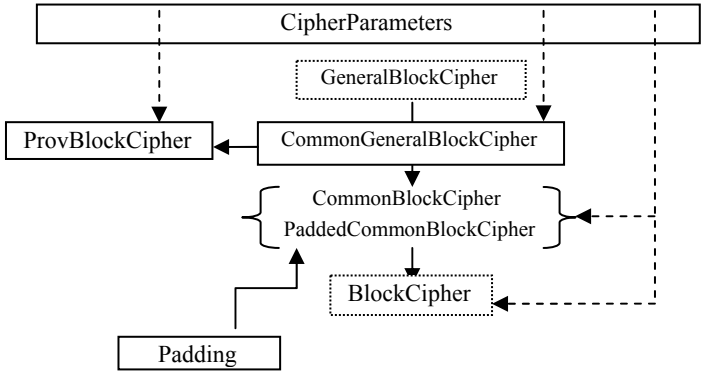


Рис. 1. Базовая архитектура криптографического провайдера

Разбор трансформации производится средой Java автоматически в абстрактном классе CipherSpi, который является ключевым для реализации блочных шифров, поэтому остаётся только включить информацию о преобразованиях, используемых в архитектуре, в необходимые методы выбора параметров трансформации.

На базе выбранных принципов была создана архитектура криптографического провайдера блочных шифров. В её основе лежит класс

ProvBlockCipher, который является одним из связующих звеньев между системой шифрования и конкретным алгоритмом шифрования. Основным интерфейсом для алгоритмов шифрования является интерфейс BlockCipher, задающий вид блочных шифров. Метод processBlock является ключевым, так как в нём проходит процесс преобразования массива байт.

Интерфейс GeneralBlockCipher определяет спецификацию всех классов-оболочек для объектов BlockCipher. Методы данного интерфейса вызываются непосредственно объектом ProvBlockCipher. Основной задачей классов, реализующих интерфейс, являются обработка и передача параметров дальнейшим компонентам архитектуры. Класс CommonGeneralBlockCipher, основанный на данном интерфейсе, позволяет задать выравнивание для системы шифрования.

Класс CommonBlockCipher представляет собой самый простой блочный шифр без выравнивания. Класс PaddedCommonBlockCipher, являющийся расширением данного класса, представляет собой блочный шифр с использованием выравнивания.

Интерфейс Padding обобщает структуру классов, отвечающих за выравнивание блоков.

В качестве примеров реализации режимов шифрования созданы классы CBCCipher и CFBCipher, отвечающие за режимы Cipher Block Chaining и Cipher Feedback [2] соответственно и реализующие базовый интерфейс BlockCipher.

Параметры криптосистемы реализуют интерфейс CipherParameters. Параметры представляют собой объекты, содержащие в себе объекты того же типа, по принципу шаблона «компоновщик» [5]. Передача параметров ведётся сверху вниз. Часть параметров используется на верхнем уровне, остальные передаются на более низкие уровни архитектуры.

Для создания ключей используется класс CommonKeyGenerator, наследующий абстрактный класс KeyGeneratorSpi. Генерация ключей производится путём использования стандартного класса SecureRandom, создающего псевдослучайное число криптографического качества.

Заключение. Преимуществом реализованной базовой архитектуры криптографического провайдера является возможность добавления новых компонентов шифрования в программную среду Java при помощи одного собственного класса, реализующего непосредственно процесс шифрования/расшифрования массива байт. Реализация уже содержит базовые режимы шифрования ECB, CBC, CFB и режимы выравнивания NIST800-38a и PKCS7, а также набор инструментов для добавления своих компонентов.

ЛИТЕРАТУРА

1. Knudsen J.. Java Cryptography // O'Reilly & Associates. 1998. 364 с.
2. Weiss J.. Java Cryptography Extensions: Practical Guide for Programmers // Morgan Kaufmann. 2004. 176 с.
3. Flanagan D. Java In A Nutshell, 5th Edition // O'Reilly Media. 2005. 1256 с.
4. Garms J., Somerfield D. Professional Java Security (Programmer to Programmer) // Wrox Press. 2001. 521 с.
5. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Д. Приемы объектно-ориентированного проектирования. Паттерны проектирования. СПб.: Питер, 2006. 368 с.

ПРИМЕНЕНИЕ ТЕОРИИ ПРОИЗВОДЯЩИХ ФУНКЦИЙ ДЛЯ ПРОВЕРКИ ПРОСТОТЫ ЧИСЛА

Ю.В. Шабля, С.А. Черепанов, студенты

Научный руководитель Д.В. Кручинин, аспирант

г. Томск, ТУСУР, каф. КИБЭВС, shablya-yv@mail.ru

Проект ГПО КИБЭВС-1205 – «Математические основы защиты информации»

С развитием общества и переходом от индустриального типа к постиндустриальному (информационному) ценность такого ресурса, как информация, выходит на первый план. Как следствие, защита информации становится неотъемлемой частью информационных процессов. Существует целый раздел математики, занимающийся данной проблемой, – криптография.

Математической основой современной криптографии является теория чисел. Основным понятием теории чисел, применяющимся в области защиты информации, является простое число. К сожалению, на сегодняшний день вопрос простых чисел является основным нерешенным вопросом целочисленной арифметики, и исследования в данной области имеют высокую научную ценность. Проблема заключается в определении, является ли заданное натуральное число простым.

На практике различные методы проверки на простоту натурального числа применяются, например, в криптографической системе с открытым ключом RSA [1]. Данный криптографический алгоритм основан на том, что факторизация больших натуральных чисел – очень трудная вычислительная операция. Благодаря этому данный алгоритм до сих пор остается наиболее эффективным и часто применяемым при шифровании для защиты информации. Но скорость выполнения данного алгоритма шифрования и его криптографическая устойчивость целиком и полностью зависят от выбора пары достаточно больших

простых чисел, на основе которых собственно и будет осуществляться процесс шифрования данных.

Актуальность рассматриваемой темы заключается в потребности разработки более эффективных и точных методов проверки натуральных чисел на простоту с целью снижения потребляемых временных ресурсов и повышения качества криптографических систем при шифровании.

В работе [2] предлагается новый метод генерации алгоритмов проверки на простоту натурального числа, основанный на теории производящих функций. В данной работе рассмотрена композиция с использованием логарифмической производящей функции, но применение такого метода возможно и с применением композиции других производящих функций. Приведем пример получения критерия на простоту.

Пример:

В качестве производящих функций берем:

$$R(x)=\ln\left(\frac{1}{1-x}\right),\ F(x)=ax=bx^2.$$

Композита функции $F(x)$:

$$F^{\Delta}(n,k,a,b)=a^{2k-n}b^{n-k}\binom{k}{n-k}.$$

Функция коэффициентов $g(n)$ для суперпозиции $G(x)=R\left(F(x)\right)$:

$$g(n)=\sum_{k=1}^{n}\frac{a^{2k-n}b^{n-k}}{k}\binom{k}{n-k}.$$

При $a=2,b=1$:

$$ng(x)=\left[2,6,14,34,82,198,478,1154,2786,6726,\ldots\right],$$

откуда

$$ng(n)=\left(1+\sqrt{2}\right)^n+\left(1-\sqrt{2}\right)^n.$$

Получаем критерий простоты.

Значение выражения

$$\frac{\left(1+\sqrt{2}\right)^n+\left(1-\sqrt{2}\right)^n-2^n}{n}$$

является целым для простых чисел n.

Основной задачей является построение критериев простоты натурального числа, используя эту методику генерации критериев на основе различных производящих функций, и проведение анализа получен-

ных критериев (определение вычислительной сложности, оценка вероятности ошибки).

Следовательно, появляется возможность разработки более эффективных и точных методов проверки натуральных чисел на простоту за счет нахождения подходящих критериев простоты числа.

ЛИТЕРАТУРА

1. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and publickey cryptosystems // Communications of the ACM. 1978. Vol. 21, №2. P. 120–126.

2. Кручинин Д.В., Кручинин В.В. Метод построения алгоритмов проверки простоты натуральных чисел для защиты информации // Доклады ТУСУРа. 2011. №2(24), ч. 2. С. 247–251.

О МЕТОДИЧЕСКОЙ ПОГРЕШНОСТИ ИЗМЕРЕНИЯ РАССТОЯНИЯ ВОЗМОЖНОГО ПЕРЕХВАТА ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Г.В. Шатров, студент каф. защиты информации

Научный руководитель В.А. Трушин, с.н.с., к.т.н.

г. Новосибирск, НГТУ, killer_gr@mail.ru

Работу всех технических средств, содержащих в своем составе электронные компоненты, сопровождают электромагнитные излучения, вызванные протеканием токов по различным токоведущим элементам. Для основных технических средств и систем (ОТСС) такие излучения называются побочными (ПЭМИ).

Если данные ПЭМИ имеют достаточный уровень, позволяющий производить их прием за границей контролируемой зоны защищаемого помещения, то потенциальный противник, используя соответствующую аппаратуру, может проводить перехват соответствующей информации. Поэтому такие ПЭМИ могут создавать опасные технические каналы утечки информации.

Критерием оценки защищенности информации за счет утечки по каналу ПЭМИ является расстояние (радиус), в пределах которого возможен перехват этих излучений с последующей расшифровкой содержащейся в них информации ($R_{\text{ПЭМИ}}$).

Нахождение расстояния возможного перехвата осуществляется для каждой излучаемой устройством частоты ПЭМИ отдельно по электрической и магнитной составляющей поля для ближней, промежуточной и дальней зоны [1] по формулам, вытекающим из уравнений Максвелла.

То есть, на основании прямых измерений уровней шума и смеси сигнала и шума (в дальнейшем – смесь) на каждой информативной частоте по известной функциональной зависимости находят искомую величину – расстояние возможного перехвата ПЭМИ (косвенное измерение величины $R_{\text{ПЭМИ}}$).

В РФ существует Федеральный закон №102 от 26.06.2008 – «Об обеспечении единства измерений». Согласно ему в рассматриваемом случае необходима обязательная оценка погрешностей измерения, что и является целью настоящей работы.

Для нахождения абсолютной погрешности ($\Delta R_{\text{ПЭМИ}}$) косвенных измерений величины $R_{\text{ПЭМИ}} = R_{\text{ПЭМИ}}(x_1,x_2...x_n)$, где x_i – непосредственно измеряемые независимые величины, имеющие абсолютную погрешность Δx_i [2]:

$$\Delta R_{\text{ПЭМИ}} = \sqrt{\sum_{i=1}^{n}(\Delta x_i \frac{\partial R_{\text{ПЭМИ}}}{\partial x_i})^2} \ . \qquad (1)$$

В нашем случае величины прямого измерения x_i есть величины, измеряемые специальным оборудованием (смесь, шум, частота, расстояние между проверяемым оборудованием и антенной измерительного оборудования).

Ниже приводится формула расчета абсолютной погрешности расстояния возможного перехвата ПЭМИ, где $E_{\text{ш}}$– уровень шума ($\Delta E_{\text{ш}}$ – абсолютная инструментальная погрешность измерения $E_{\text{ш}}$); $\Delta E_{\text{с+ш}}$ – уровень смеси ($\Delta E_{\text{с+ш}}$ – абсолютная инструментальная погрешность измерения $E_{\text{с+ш}}$); R_0 – расстояние между проверяемым оборудованием и антенной измерительного оборудования (ΔR_0 – абсолютная погрешность R_0); f – частоты (Δf – абсолютная инструментальная погрешность измерения f).

$$\Delta R_{\text{ПЭМИ}}(\Delta E_{\text{с+ш}},\Delta E_{\text{ш}},\Delta R_0,\Delta f) =$$

$$= \sqrt{[\frac{\partial}{\partial E_{\text{с+ш}}}(R_{\text{ПЭМИ}})\Delta E_{\text{с+ш}}]^2 + [\frac{\partial}{\partial E_{\text{ш}}}(R_{\text{ПЭМИ}})\Delta E_{\text{ш}}]^2 + [\frac{\partial}{\partial R_0}(R_{\text{ПЭМИ}})\Delta R_0]^2 + [\frac{\partial}{\partial f}(R_{\text{ПЭМИ}})\Delta f]^2} . \qquad (2)$$

Для нахождения относительной погрешности ($\delta R_{\text{ПЭМИ}}$) вычисляется отношение абсолютной погрешности расстояния возможного перехвата ПЭМИ к самому расстоянию.

Для получения результата потребуется знать абсолютные погрешности независимых величин, описанных выше. Используемым измерительным оборудованием являются анализаторы спектра компании Agilent серии ESA-E E4402B, серии PSA E444xA, серии ESA E4403B,

компании Rohde&Schwarz серии FSU, серии FSP с погрешностями измерения уровня 0,4; 0,62; 1,1; 0,3; 0,5 дБ соответственно, погрешностью частоты 101 Гц [3, 4]. Анализаторы спектра входят в состав сертифицированных ФСТЭК программно-аппаратных комплексов (ПАК). А погрешность измерения расстояния между проверяемым оборудованием и антенной составляет половину цены деления рулетки $5 \cdot 10^{-4}$ м.

Рассматриваемый уровень шумов ($E_{ш}$) 40, 60 дБ (мкВ/м), уровень смеси ($E_{с+ш}$) 80 дБ, расстояние между проверяемым оборудованием и антенной измерительного оборудования (R_0) 1 м. Взяты частоты (f) 54 МГц (видеоконтроллер-монитор), 240 МГц (большинство USB-устройств).

Для расчета погрешностей $\Delta R_{ПЭМИ}$ разработана программа на математическом пакете Maple, вычисляющая абсолютные и относительные погрешности $\Delta R_{ПЭМИ}$ для заданных начальных условий.

В ходе программы сначала вычисляется радиус возможного перехвата ПЭМИ, а затем его абсолютная погрешность.

Все расчеты велись для электрической составляющей электромагнитного поля; для магнитной составляющей расчеты аналогичны.

На основе программы, в частности, рассчитаны абсолютные и относительные погрешности расстояния возможного перехвата ПЭМИ для разных сертифицированных анализаторов спектра при уровне шума 40, 60 дБ, смесь 80 дБ, $R_0 = 1$ м, $f = 240$ МГц (табл. 1), 54 МГц (табл. 2).

Также выявлена закономерность: при одинаковой разности смеси и шума в дБ (например: 40 и 20, 60 и 40 и т.д.; разность составляет 20 дБ), а также при фиксированных остальных начальных условиях, в частности, фиксированной частоте, в ближней зоне набор $R_{ПЭМИ}$, $\Delta R_{ПЭМИ}$, $\delta R_{ПЭМИ}$ имеет одинаковые значения. Это же присуще промежуточной и дальней зоне соответственно.

Например:

- при $f = 240$ МГц $\Delta E_{ш} = 0{,}4$ дБ, $\Delta E_{с+ш} - \Delta E_{ш} = 20$ дБ, $R_0 = 1$ м, $\Delta f = 101$ Гц;
- $R_{ПЭМИ} = 4{,}07$ м, $\Delta R_{ПЭМИ} = 0{,}13$ м, $\delta R_{ПЭМИ} = 3{,}29\%$;
- как при $E_{с+ш} = 40$ дБ, $E_{ш} = 20$ дБ, так при $E_{с+ш} = 50$ дБ, $E_{ш} = 30$ дБ, так при $E_{с+ш} = 60$ дБ, $E_{ш} = 40$ дБ и т.д.

Результаты показали, что для наиболее часто встречающихся значений частот, уровней смеси, шума относительные погрешности расстояния (радиуса) возможного перехвата ПЭМИ лежат в диапазоне 2…17%.

Проведены расчеты погрешности оценки радиуса возможного перехвата ПЭМИ для наиболее часто используемых средств измерения (см. табл. 1, 2).

Таблица 1

Абсолютные и относительные погрешности расстояния возможного перехвата ПЭМИ для разных анализаторов спектра при f = 240 МГц

Название анализатора спектра, абсолютная погрешность измерения уровня	Радиус возможного перехвата ПЭМИ, м		Абсолютная погрешность радиуса возможного перехвата ПЭМИ, м		Относительная погрешность радиуса возможного перехвата ПЭМИ, %	
	При уровне шума, дБ					
	40	60	40	60	40	60
Agilent серии ESA-E E4402B, 0,4 дБ	22,22	4,07	1,45	0,13	6,51	3,29
Agilent серии PSA E444xA, 0,62 дБ	22,22	4,07	2,24	0,21	10,1	5,1
Agilent серии ESA E4403B, 1,1 дБ	22,22	4,07	3,98	0,37	17,91	9,04
Rohde&Schwarz серии FSU, 0,3 дБ	22,22	4,07	1,08	0,1	4,89	2,47
Rohde&Schwarz серии FSP, 0,5 дБ	22,22	4,07	1,81	0,17	8,14	4,11

Таблица 2

Абсолютные и относительные погрешности расстояния возможного перехвата ПЭМИ для разных анализаторов спектра при f = 54 МГц

Название анализатора спектра, абсолютная погрешность измерения уровня	Радиус возможного перехвата ПЭМИ, м		Абсолютная погрешность радиуса возможного перехвата ПЭМИ, м		Относительная погрешность радиуса возможного перехвата ПЭМИ, %	
	При уровне шума, дБ					
	40	60	40	60	40	60
Agilent серии ESA-E E4402B, 0,4 дБ	12,91	4,07	0,42	0,13	3,29	3,26
Agilent серии PSA E444xA, 0,62 дБ	12,91	4,07	0,65	0,21	5,05	5,1
Agilent серии ESA E4403B, 1,1 дБ	12,91	4,07	1,16	0,37	8,96	9,05
Rohde&Schwarz серии FSU, 0,3 дБ	12,91	4,07	0,32	0,1	2,44	2,47
Rohde&Schwarz серии FSP, 0,5 дБ	12,91	4,07	0,53	0,17	4,07	4,11

ЛИТЕРАТУРА

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. для вузов. М.: ООО «Издательство машиностроение», 2009. 508 с.

2. Гольдин Л.Л., Игошин Ф.Ф., Козел С.М. и др. Руководство к лабораторным занятиям по физике. М.: Наука, 1973. 688 с.

3. Agilent Technologies [Электронный ресурс]. 2013. Режим доступа: http://www.home.agilent.com/agilent/home.jspx?cc=RU&lc=rus. Загл. с экрана.

4. ROHDE&SCHWARZ [Электронный ресурс]. 2013. Режим доступа: http://www.rohde-schwarz.com/en/home_48230.html. Загл. с экрана.

АНАЛИЗ ТЕКСТОВЫХ ПРИЗНАКОВ ИСКУССТВЕННЫХ ТЕКСТОВ, СОЗДАННЫХ НА ОСНОВЕ СИНОНИМИЗАЦИИ

А.О. Шумская, студентка

Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.

г. Томск, ТУСУР, каф. КИБЭВС, shumskaya.ao@gmail.com

Задачи идентификации авторства могут возникать в разных отраслях. Проблема анализа и выявления искусственных текстов, сгенерированных автоматически с помощью специальных программ или роботов, на данной момент является активно исследуемой. Это связано с тем, что все большее место в общественных отношениях и взаимодействиях стал занимать Интернет и сопутствующие ему технологии. В последнее время появилось много новых возможностей, связанных с электронным представлением документов, обработка которых из-за увеличения объема требует все больших ресурсов [1].

Синонимизация позволяет качественно изменить текст любой статьи, то есть произвести так называемый «рерайтинг». Для создания текстов с помощью синонимизации необходим словарь синонимов и их склонений, от объема и качества которого зависит и качество текста-результата [2].

В ходе исследования были использованы следующие статистические характеристики случайной величины:

Математическое ожидание $M(X)$ случайной величины X. Так как принимается, что в данном случае величина распределена нормальна, то математическое ожидание приравнено к арифметическому среднему значению величины в выборке (1):

$$M(X)=\frac{\sum_{i=1}^{n} x_i}{n}, \quad (1)$$

где x_i – значение элемента выборки, n – объем выборки.

Среднеквадратичное отклонение s случайной величины X (2):

$$s^2(X)=M[X-M(X)]^2. \quad (2)$$

Для исследования характеристик текстов каждого из авторов в работе бралось 10 его текстов. Для тестирования автоматически сгенери-

рованных текстов брались 10 текстов, которые были созданы на основе текстов одного автора.

Для девяти из текстов высчитывается один и тот же показатель, затем рассчитываются математическое ожидание и среднеквадратическое отклонение. На десятом тексте идет проверка попадания рассчитанного для этого текста параметра в интервал $(M(X) - s;\ M(X) + s)$. В случае если проверка показывала, что величина находится вне этого интервала, выдается сообщение о данном событии и рекомендуется изменить выборку, чтобы выполнилось описанное условие.

Этот алгоритм использовался одновременно как для проверки, так и для основных вычислений текстовых параметров. Высчитанное значение математического ожидания для одного автора и одного численного параметра является выходным результатом расчетов.

Для определения характеристик, которые могли бы помочь отличить искусственный текст от естественного произведения были произведены расчеты как для специально сгенерированных текстов, так и для работ, автор которых заведомо известен.

Генерация искусственных текстов проводилась с помощью свободно распространяемого программного продукта SyMonym.

SyMonym – программный продукт для уникализации текста и статей, основанный на синонимизации исходного текста; содержит закрытую базу синонимов из 68272 словоформ, а также имеет дополнительный словарь синонимов более 1000000 просклоненных слов и словоформ, а также возможность добавлять собственные базы данных. Для исследований использовалась свободно распространяемая демоверсия продукта [3].

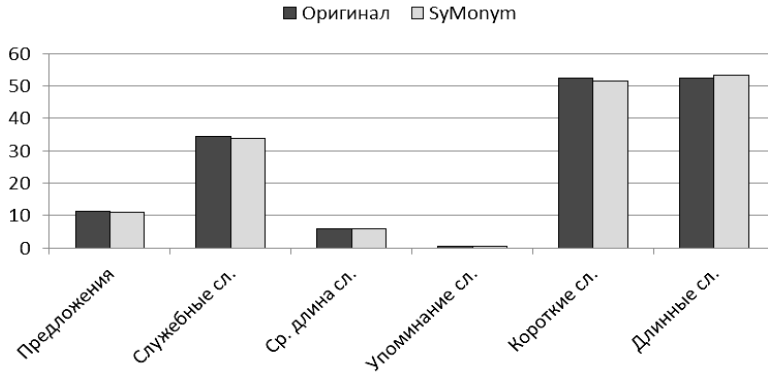


Рис. 1. Гистограмма изменения значений при синонимизации

Для проведения расчетов с помощью программы SyMonym, использующей в своей основе синонимизацию на базе встроенных сло-

варей синонимов, были созданы искусственные тексты из оригинальных текстов одного известного автора.

Графическая интерпретация результатов расчетов в виде гистограммы представлена на рис. 1.

Из гистограммы видно, что после преобразования в тексте увеличилось количество длинных слов и увеличилась средняя длина слова. Количество предложений и упоминаний искомых слов незначительно уменьшилось за счет того, что были добавлены новые слова в процессе преобразования текста и показатель количества на 100 знаков уменьшился на сотые доли единицы, хотя сам метод не вносит изменений в грамматическую структуру текста.

ЛИТЕРАТУРА

1. Романов А.С. Разработка и исследование математических моделей, методик и программных средств информационных процессов при идентификации автора текста / А.С. Романов, А.А. Шелупанов, Р.В. Мещеряков. Томск : В-Спектр, 2011. 188 с.

2. Автоматическое порождение текста [Электронный ресурс] // Tpl-it: проект студентов специальности «теоретическая и прикладная лингвистика» и магистрантов ФГБОУ ВПО ИГЛУ. Электрон. текст. дан. [Б.м.], 2013. URL: http://tpl-it.wikispaces.com/Автоматическое+порождение+текста. (дата обращения: 25.01.2013).

3. Качественная программа для уникализации текста и статей SyMonym [Электронный ресурс] // Автоматический рерайт, копирайт статей и текста. Электрон. дан. [Б.м.], 2012. URL: http://www.seosin.ru/page/6/ (дата обращения: 14.02.2013).

4. Интернет-библиотека Алексея Комарова [Электронный ресурс]. Электрон. текст. дан. [Б.м.], 1996–2013. URL: www.ilibrary.ru (дата обращения: 29.01.2013).

ЗАДАЧИ ИДЕНТИФИКАЦИИ ИСКУССТВЕННЫХ ТЕКСТОВ

А.О. Шумская, студентка

Научный руководитель Р.В. Мещеряков, зам. нач. НУ, проф., д.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, shumskaya.ao@gmail.com

Учитывая повсеместное внедрение и использование электронной документации, электронных версий произведений, повышение популярности электронного формирования запросов на различных ресурсах и подобного, уникальность создаваемых текстовых форм ставится под сомнение. В сети злоумышленник легко может скопировать какой-либо текст и использовать его в своих целях: для генерации спам-страниц, отправки ложных заявок и прочего. Также существуют мето-

ды создания искусственных текстов без необходимости иметь какое-либо начальное произведение.

Анализ особенностей искусственной речи и механизмов ее распознавания может использоваться для того, чтобы оградить себя или некоторый ресурс от работы с искусственными текстами (ложными обращениями, спамом и прочим), для исключение из результатов поисковых запросов страницы с автоматически сгенерированным контентом, используемым для продвижения веб-страниц в Интернете и др.

В процессе обработки текстов могут попадаться результаты различных методов генерации, однако немаловажно знать основные тенденции и особенности их работы, так как это может обусловить подход к исследованию. В настоящий момент описано несколько десятков методов автоматического порождения текстов, также существуют методики, основанные на них, но имеющих те или иные особенности для решения узких задач. Ниже перечислены основные такие методы и их особенности.

В практике автоматической генерации текстов самым распространенным и наиболее простым в реализации методом являются различные варианты цепей Маркова. Для его реализации требуются программа-генератор и большой объем исходного текста. Для создания текстов на практике это можно интерпретировать следующим образом: выбирается начальное слово и помещается в текст-результат, затем оно ищется в исходном тексте, когда находится, то в текст-результат переносится следующее за ним слово, и уже его ищут в исходном тексте. Опытные исследования показывают, что максимально человекоподобный текст получается из больших объемов исходного текста. Также отмечается, что текст должен быть определенного содержания и не содержать в себе разные предметные области. Например, исходный текст с упоминанием медицинских терминов и подробностей устройства автомобиля повлечет некорректный с точки зрения восприятия текст-результат [1].

Другой метод, часто используемый в качестве вспомогательного при использовании совместно с другими методами, – SIMP-таблицы (английский (США) Simplified Integrated Modular Prose – упрощённая интегрированная модульная проза) – таблицы с некоторыми фрагментами предложений, например таблицы *A*, *B*, *C*, *D*, в которых записаны начала предложений, внутренние части и завершения. Из каждой такой таблицы выбирается случайное значение и таким образом формируется законченное предложение. Возможны варианты изменения порядка таблиц, например *A, C, B, D*, а также добавление механизмов для коррекции окончаний слов при необходимости [2]. Данный метод позволяет генерировать общеупотребительные псевдонаучные фразы. Его работа

основана на генерации случайного четырёхзначного числа и выборке из четырёх SIMP-таблиц соответствующих частей предложения.

Метод с использованием словарей наиболее трудоемкий, но перспективный в плане соблюдения всех норм языка. Он требует специально подготовленных словарей с подробным перечислением характеристик слова и его форм, а также изучения порядка слов в предложении. Данный метод использует шаблоны известных ему форм языка – грамматических форм предложений и наличие зависимостей между словами. Чтобы метод работал корректно и создавал требуемые предложения, требуется очень подробное описание каждого слова, включая в том числе тематику [2].

Популярным методом на сегодняшний день является синонимизация – изменение исходного текста путем замены слов похожими по смыслу. Качество сгенерированного текста-результата зависит в большей степени от объема и качества словаря синонимов и их склонений [2].

На сегодняшний день не существует полной теории, описывающей законы порождения текстов, не отличимых от созданных человеком. Тем не менее, известны многие закономерности, характерные естественным текстам, такие как единство стиля, следование законам жанра, лингвистические особенности использования слов русского языка и словообразования, семантическая нагрузка используемых речевых оборотов, локальная связность, глобальная тематическая связность и т.п. [3].

Если принять во внимание особенности используемых методов и математическое обоснование, можно построить на их основе модель, позволяющую идентифицировать текст как искусственный.

Автором предлагаются следующие подходы к решению задач определения текстовых форм, сгенерированных автоматически:

– выделение параметра или набора параметров, присущих конкретным методам автоматического порождения текста на основе модели их работы и исследования сгенерированных текстов;

– выявление искусственного текста на основе выявленных характерных для того или иного метода параметров;

– исследование нескольких частей одного текста и сравнение показателей контрольных характеристик с целью выявления изменения авторского стиля или оценки связности текста между частями.

Данные подходы могут применяться как по отдельности, так и в совокупности. При комплексном подходе предполагается достижение более корректных и эффективных результатов. Следует отметить, что для подобного рода исследований объем текстовой формы играет важную роль: в коротком сообщении трудно выделить логические части и

корректно рассчитать показатели текста, что может повлечь ошибки в идентификации.

Таким образом, для решения вышеобозначенных задач и проведения исследований необходим комплексный подход к проблеме – со стороны математического аппарата генераторов искусственных текстов и со стороны лингвистических особенностей языка (предполагается работа с русским языком).

ЛИТЕРАТУРА

1. Павлов А.С. Метод обнаружения поискового спама, порожденного с помощью цепей Маркова [Электронный ресурс] / А.С. Павлов, Б.В. Добров // Университетская информационная система Россия. Электрон. текст. дан. М., 2009. URL: http://www.cir.ru/docs/ips/publications/2009_rcdl_markov.pdf (дата обращения: 05.02.2013).

2. Автоматическое порождение текста [Электронный ресурс] // Tpl-it: проект студентов специальности «Теоретическая и прикладная лингвистика» и магистрантов ФГБОУ ВПО ИГЛУ. Электрон. текст. дан. [Б.м.], 2013. URL: http://tpl-it.wikispaces.com/ Автоматическое+порождение+текста (дата обращения: 25.01.2013).

3. Романов А.С. Разработа и исследование математических моделей, методик и программных средств информационных процессов при идентификации автора текста / А.С. Романов, А.А. Шелупанов, Р.В. Мещеряков. Томск: В-Спектр, 2011. 188 с.

НЕ-ФАКТОР ПРИ ПОДБОРЕ ПЕРСОНАЛА В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

А.А. Сметанин, аспирант каф. ВТ

Научный руководитель Е.Ф. Стукалина, доцент, к.т.н.

г. Ижевск, ИжГТУ им. М.Т. Калашникова, smtnin@gmail.com

Задача обеспечения информационной безопасности приобрела особую важность в настоящее время в связи с бурным ростом корпоративных и государственных информационных систем, увеличением объемов хранения и обработки информации, в том числе конфиденциальной.

Проблема подбора персонала в условиях информационного противоборства приобрела особую актуальность в связи с повсеместной автоматизацей информационной инфраструктуры, глобализацией информационного пространства, подключением систем обработки информации к локальным и глобальным сетям, что существенно расширяет возможность нарушения конфиденциальности, целостности, доступности информации [1].

Существуют различные системы подбора персонала типа программа E-staff, Резюмакс, модули 1с, босс-кадровик, а также обширный функционал различных сайтов по подбору персонала hh.ru, superjob.ru. Однако, ни в одной из этих систем не уделено внимание благонадежности персонала, важнейшего элемента информационной безопасности, в то время как вопрос защиты информации требует системного подхода и, следовательно, анализа информации и о персонале как об основном составляющем звене любой информационной системы.

Всех кандидатов на любую должность можно разделить на три группы благонадежности в автоматическом режиме на основе формальных тестов и математических вычислений. Несмотря на то, что многие относятся к экспертным системам весьма скептически, это самый развитый и надежный на сегодняшний день способ построения символьных систем для решения слабоформализованных задач [3].

На входе автоматизированной системы будем использовать данные о кандидатах, получаемые из различных источников, а на выходе, на основе рассчитанных характеристик, – рекомендации по отнесению персонала к той или иной группе благонадежности. Задача является классической для использования аппарата нечеткой логики и вычислений в условиях неопределенности.

В общем случае нечетким отношением или, более точно, нечетким k-арным отношением, заданным на множествах (универсумах) X_1, X_2,…, X_k, называется некоторое фиксированное нечеткое подмножество декартова произведения этих универсумов. Другими словами, если обозначить произвольное нечеткое отношение через Q, то по определению [2]

$$Q=\{<x_1,x_2,...,x_k>,\mu_Q(<x_1,x_2,...,x_k>)\},$$

где $\mu_Q(<x_1, x_2, ..., x_k>)$ – функция принадлежности данного нечеткого отношения, которая определяется как отображение μ_Q: $X_1\times X_2\times\ldots\times X_k\rightarrow$ $\rightarrow[0, 1]$. Здесь через $<x_1, x_2,. .., x_k>$ обозначен кортеж из k элементов, каждый из которых выбирается из своего универсума: $x_1 \in X_1$, $x_2 \in X_2$, …, $x_k \in X_k$.

В общем случае бинарное нечеткое отношение задается на базисных множествах X_1, X_2 и определяется как нечеткое отношение

$$Q=\{<x_i,x_j>,\mu_Q(<x_i,x_j>)\},$$

где $\mu_Q(<x_i, x_j>)$ – функция принадлежности бинарного нечеткого отношения, которая определяется как отображение μ_Q: $X_1\times X_2 \rightarrow[0, 1]$, а через $<x_i, x_j>$ обозначен кортеж из двух элементов, при этом $x_1 \in X_1$, $x_2 \in X_2$.

Пусть Q и R – конечные или бесконечные бинарные нечеткие отношения. Причем нечеткое отношение $Q=\{<x_i, x_j>, \mu_Q(<x_i, x_j>)\}$ задано

на декартовом произведении универсумов $X_1 \times X_2$, а нечеткое отношение $R=\{<x_j, x_k>, \mu_R(<x_j, x_k>)\}$ – на декартовом произведении универсумов $X_2 \times X_3$. Нечеткое бинарное отношение, заданное на декартовом произведении $X_1 \times X_3$ и обозначаемое через $Q \times R$, называется композицией бинарных нечетких отношений Q и R, а его функция принадлежности определяется следующим выражением:

$$\mu_{Q \otimes R}(<x_i, x_k>) = \max_{x_j \in X_2} \{\min\{\mu_Q(<x_i, x_j>), \mu_R(<x_j, x_k>)\}\}, \quad (\forall <x_i, x_k> \in X_1 \times X_3).$$

Определенную таким образом композицию бинарных нечетких отношений называют иногда (max-min)-композицией или максиминной сверткой нечетких отношений.

Нечеткое бинарное отношение, заданное на декартовом произведении $X_1 \times X_3$ и обозначаемое через $Q \times R$, называется (max-*)-композицией бинарных нечетких отношений Q и R, если его функция принадлежности определяется следующим выражением:

$$\mu_{Q \otimes R}(<x_i, x_k>) = \max_{x_j \in X_2} \{\mu_Q(<x_i, x_j>) \times \mu_Q(<x_j, x_k>)\}, \quad (\forall <x_i, x_k> \in X_1 \times X_3).$$

В частности, если в этом выражении вместо операции «*» использовать операцию алгебраического умножения, то получим определение (max-prod)-композиции.

Так, рассмотренные нами ранее (max-min)- и (max-prod)-композиции дают информацию о степени благонадежности кандидата.

Следовательно, можно применить две модели нечеткой логики – max-min и max-prod.

Заключение. Здесь изложен основной подход к выбору персонала в нечетких условиях, когда у нас есть множество должностей, множество кандидатов и множество характеристик благонадежности каждого кандидата, что позволяет автоматизировать процесс оценки рисков информационной безопасности и выбрать оптимальное решение.

ЛИТЕРАТУРА

1. Сметанин А.А., Стукалина Е.Ф. Минимизация внутренних угроз информационной безопасности // Информационная безопасность в государственных и негосударственных структурах «Информтех–2012». 2012. С. 170–173.

2. Сметанин А.А., Сметанин А.М., Стукалина Е.Ф., Харин Ю.Л., Опыт работы по подбору и контролю персонала с использованием полиграфа // Информационная безопасность в государственных и негосударственных структурах «Информтех–2012». 2012. С. 165–169.

3. Душкин Р.В. Методы получения, представления и обработки знаний с НЕ-факторами. 2011. 115 с. [Электронный ресурс]. URL:http://www.labrate.ru/discus/messages/33870/dushkin_nefactors_2011-36925.pdf

ПРОГРАММНЫЕ СПОСОБЫ ВОССТАНОВЛЕНИЯ УДАЛЕННОЙ ИНФОРМАЦИИ ПРИ РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

А.Р. Смолина, аспирант каф. КИБЭВС

Научный руководитель А.А. Шелупанов, проректор по НР, зав. каф. КИБЭВС, д.т.н., проф.

г. Томск, ТУСУР, atoj@rambler.ru

Расследование компьютерных преступлений практически невозможно без производства компьютерно-технической экспертизы (КТЭ). Достаточно часто, в ходе КТЭ решаются вопросы по анализу информационного содержимого (файлового содержимого) каких-либо носителей информации (жестких дисков, USB-flash накопителей и т.д.).

К моменту предоставления объектов исследования на экспертизу значительная часть информации может оказаться удаленной. Но в большинстве случаев, удаленной эта информация лишь кажется и она может быть легко восстановлена программными способами, что и осуществляется в рамках КТЭ.

При обычном удалении информации она (информация) фактически не удаляется. Пространство, занимаемое ею, лишь помечается средствами операционной системы (ОС) как свободное, ссылки на удаленные файлы продолжают храниться ОС. Информация может быть прочитана и восстановлена до тех пор, пока соответствующее пространство не будет перезаписано другой информацией. В данном случае информацию можно восстановить практически любым программным обеспечением (ПО) для восстановления данных (например, «Recuva», «Handy Recovery», «Recover My Files»).

При восстановлении информации после форматирования, вирусной атаки, повреждения таблицы расположения файлов или сбоев ОС необходимо использование ПО, использующего более детальный метод. Данный метод заключается в выполнении посекторного сканирования носителя информации, последующем анализе обнаруженной информации по определенным структурным элементам, выделении из нее записанных файлов и их восстановлении. К данному ПО можно отнести ПО «Ontrack EasyRecovery Pro», в котором для вышеописанных случаев реализованы режимы «FormatRecovery» (восстановление после форматирования) и «RawRecovery» (восстановление без учета файловой системы), ПО «R-Studio» и «UFS Explorer».

Иногда возникает ситуация, что программным обеспечением при восстановлении без учета файловой системы происходит неверное выделение файлов из обнаруженного массива информации. Неверно может быть определено расширение файла (в данном случае достаточно

изменить расширение файла на подходящее) или границы информационного содержимого самого файла (некорректное определение начала и конца файла). Во втором случае необходимо воспользоваться шестнадцатеричным редактором с целью поиска по заголовку файла его фактического начала. Для данной цели весьма удобен шестнадцатеричный редактор «010 Editor».

Вышеописанные способы широко используются при производстве КТЭ при анализе информационного содержимого носителей информации с достаточно большим перечнем файловых систем.

ЛИТЕРАТУРА

1. Федотов Н.Н. Форензика – компьютерная криминалистика. М.: Юридический мир, 2007. 360 с.

2. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: учеб. пособие / А.И. Усов / Под ред. Е.Р. Россинской. М.: Экзамен. Право и закон, 2003. 368 с.

3. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. 416 с.

4. Петруй М.В., Давыдов И.В. Компьютерная судебно-техническая экспертиза. Существующие автоматизированные системы ее проведения: тезисы доклада // Матер. науч.-техн. конф. «Научная сессия ТУСУР–2006». Томск, 2006. Ч. 3. С. 47–51.

5. Свердлова В.Н., Романов А.С. Судебная компьютерная экспертиза // Матер. науч.-техн. конф. «Научная сессия ТУСУР–2007». Томск: В-Спектр, 2007. Ч. 2. С. 221–223.

ИНФОРМАЦИОННАЯ СИСТЕМА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

А.К. Новохрестов, И.А. Сологуб, студенты каф. КИБЭВС

Научный руководитель М.А. Сопов, ст. преподаватель

г. Томск, ТУСУР, ФВС, каф. КИБЭВС, AlexBigGluk@gmail.com

Проект ГПО КИБЭВС-1103 – «Инженерия баз данных»

В настоящее время организациям приходится хранить все большие и большие количества информации. В большинстве случаев хранение информации «на бумаге» не рассматривается как возможный вариант, и в дело вступают базы данных. Существуют различные базы данных и их классификации, однако требования к ним универсальны.

В данной работе рассматривается база данных Удостоверяющего центра Сибири, предназначенная для хранения договоров и сопутствующей информации: об организациях-клиентах, услугах и пользователях БД. Существующая программа не только хранит информацию о договорах, но и формирует сами файлы договоров на основе шаблонов.

Информационная система, рассматриваемая в данной работе, уже существует и функционирует, однако любая организация развивается, и от используемых приложений требуется выполнение новых функций. Удостоверяющей центр Сибири не является исключением.

При изучении существующей программы были выявлены не только недостающие функции, но и проблемы в уже реализованных. Например: шаблоны договоров (хранятся в формате RTF, который сам по себе уже устарел) можно редактировать только в Microsoft Word 98, после редактирования в более новых версиях программа перестает видеть эти шаблоны.

Таким образом, было принято решение о реализации нового приложения, выполняющего все требуемые функции. Далее перечислены наиболее важные функции, которые должны быть реализованы в первую очередь:

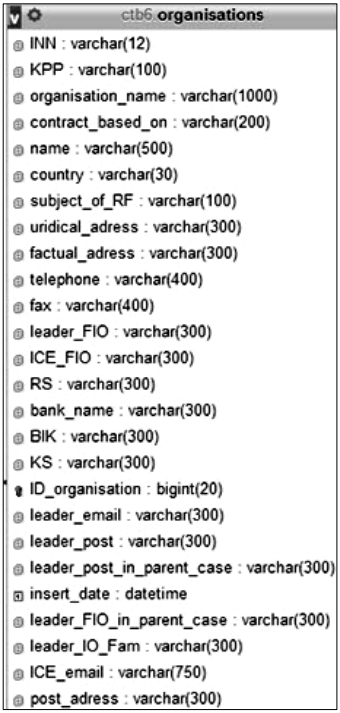


Рис. 1. Таблица «Организации»

– хранение информации (об услугах, предоставляемых удостоверяющим центром; организациях-клиентах; договорах, пользователях базы данных);

– поиск информации по базе данных;

– формирование файлов договоров по заготовленным шаблонам и информации о договоре.

В ходе работы над информационной системой в первую очередь исправлены ошибки в реализации структуры базы данных (неиспользуемые таблицы, отсутствующие связи, проблемы с нормализацией). Далее приведен пример проделанной работы по модификации базы данных.

Таблицу с информацией об организациях (рис. 1) можно преобразовать в три таблицы: «Организации», «Руководители» и «Контактные лица». Между новыми таблицами необходимо реализовать связи «многие ко многим». Структура измененного фрагмента базы данных приведена на рис. 2.

Параллельно велась работа над приложением, в ходе которой было принято решение о разработке нового приложения на языке программирования C# (используемое приложение реализовано на PHP).

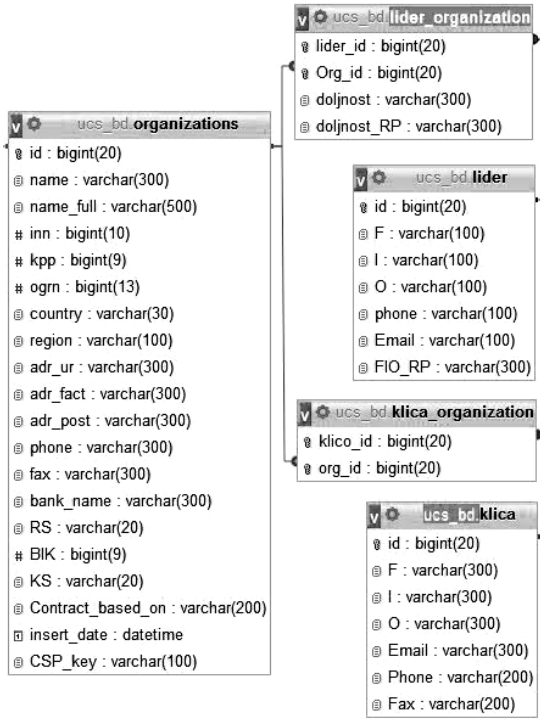


Рис. 2. Измененный фрагмент базы данных

В данный момент происходит согласование требований с заказчиком и разработка первой версии, реализующей основные функции.

СОЗДАНИЕ СКАНЕРА УЯЗВИМОСТЕЙ ИСХОДНЫХ КОДОВ НА ЯЗЫКЕ C++

И.С. Созинова, студентка каф. КИБЭВС

Научный руководитель Е.М. Давыдова, доцент, к.т.н.

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

Проект ГПО КИБЭВС-1104 – «Анализ уязвимостей кода»

В настоящее время остро встает проблема проверки исходного кода на всевозможные уязвимости, обнаруженные на сегодняшний день и разделенные по классам [1]. Основной же причиной возникновения уязвимостей по-прежнему является сжатость сроков создания программного обеспечения [2].

Одним из вариантов решения данной проблемы может являться сканер уязвимостей исходного кода. Говоря об исходных кодах, сразу примем за необходимое условие использование статических методов в применяемом сканере [2].

Статический анализ может проводиться двумя способами: сравнение с шаблонами и проверка правил корректности (проверка формализованных правил корректного построения исходного кода: синтаксический и семантический анализ [5]). Условимся, что если при проверке обнаружены синтаксические ошибки, дальнейший анализ не проводится [4].

Проблемы статического сканера. Недостатки статического анализа: ложные срабатывания, пропуск уязвимостей и недостаточная интеллектуальность, которая приводит к тому, что результаты статического анализа по сложности интерпретации сопоставимы с исходными текстами [2–4].

На рынке сканеров существует достаточно много аналогов. В ходе их исследования, наряду с недостатками самой используемой методики, был выявлен ряд дополнительных недостатков:

– скудность шаблонов;

– отсутствие периодических обновлений базы шаблонов;

– отсутствие защиты от некомпетентного изменения набора шаблонов;

– отсутствие защиты от фальсификации получаемых в ходе тестирования отчетов.

Следует взять во внимание такой фактор, который в некоторых случаях может стать серьезнейшим недостатком анализатора, – быстродействие. Хотя в большинстве сканеров процедура проверки занимает доли секунды, это связано лишь с предельной упрощенностью или сжатостью алгоритмов проверки.

Предлагаемые решения проблем статических сканеров уязвимостей. Разрабатываемый сканер уязвимостей создается для решения всех вышеперечисленных проблем тем или иным способом, будучи при этом максимально простой и доступной в использовании утилитой. В таблице приведены варианты проблем сканеров с предлагаемыми решениями.

Основную нагрузку при решении большинства обозначенных проблем несет база данных шаблонов уязвимостей, являющаяся неотъемлемой частью всей системы сканирования.

Проблема ложных срабатываний решена в сканере лишь частично за счет более детальной проработки шаблонов. Для каждой из найденных уязвимостей проставляется определенный уровень важности, исходя из которого, можно предположить, является ли найденная уязвимость ложной, с некоторой долей вероятности.

Устранение недостатков в разрабатываемом сканере

Недостаток	Решение
Ложные срабатывания	Детальная проработка шаблонов, указание важности уязвимости на основе частоты ложного срабатывания шаблона
Пропуск уязвимостей	Периодическое пополнения базы новыми примерами
Недостаточная интеллектуальность	Понятные пользователю описания шаблонов
Скудность шаблонов	Расширение базы, функция периодического обновления
Отсутствие периодических обновлений базы шаблонов	Установка напоминания об обновлении
Отсутствие защиты от некомпетентного изменения базы шаблонов	Разграничение прав доступа
Отсутствие обеспечения целостности отчетов о найденных уязвимостях	Разграничение прав доступа
Недостаточное быстродействие	Параллельные вычисления: сети Петри, модель акторов

Быстродействие данного сканера обусловлено тщательным подбором методики обхода большого объема текста и принятия решений о наличии уязвимостей: сети Петри, модель акторов [4, 6].

Заключение. В целом разработанный с учетом всех вышеперечисленных проблем сканер является удобной и полезной утилитой для поиска уязвимостей исходных кодов. Хотя нужно принять во внимание, что максимальной эффективности можно достигнуть только при использовании сканера опытным программистом.

ЛИТЕРАТУРА

1. Созинова И.С. Классификация уязвимостей программного обеспечения / И.С. Созинова, С.Е. Черепанов // Современные тенденции в науке: новый взгляд: сб. науч. тр. по матер. междунар. заоч. науч.-практ. конф. 29 ноября 2011 г. Тамбов, 2011. Ч. 7. С. 151–154.

2. Созинова И.С. Методы поиска уязвимостей программного кода / И.С. Созинова, С.Е. Черепанов // Вопросы образования и науки: теоретический и методический аспекты: сб. науч. тр. по мат-лам Междунар. заоч. науч.-практ. конф. 30 апреля 2012 г. Тамбов, 2012. Ч. 6. С. 124–126.

3. Марков А. Выявление уязвимостей в программном коде [Электронный ресурс] / А. Марков, С. Миронов, В. Цирлов. Электронные данные. Открытые системы. 2005. №12. Режим доступа: http://www.osp.ru/os/2005/12/380655, свободный.

4. Созинова И.С. Сканер уязвимостей на основе статического анализа исходного кода на языке программирования С++ / И.С. Созинова, С.Е. Черепанов // Перспективы развития науки и образования: сб. науч. тр. по матер. Междунар. заоч. науч.-практ. конф. 28 сентября 2012 г. Тамбов, 2012. Ч. 13. С. 150–152.

5. Кулямин В.В. Методы верификации программного обеспечения [Электронный ресурс] / В.В. Кулямин. Электронные данные. Информационно-телекоммуникационные системы, 2008. Режим доступа: http://www.ict.edu.ru/lib/index.php?id_res=5645, свободный.

6. Даньшин Е.А. Выявление уязвимостей в исходном коде программного обеспечения: дипломная работа: ФВС ДР.70401-01 81 01: Томск, 2011. 124 с.

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

Э.Р. Старухина, студентка каф. КИБЭВС

Научный руководитель М.А. Горбунов

Ведение современного бизнеса невозможно без активных коммуникаций внутри компании, с бизнес-партнерами или клиентами, средой для передачи важной информации все чаше и чаше становятся публичные сети и Интернет. При этом становится важным организация защиты передаваемой информации, хранящейся информации или ресурсов, обеспечивающих ее обработку от атак из неконтролируемых сегментов сети. Опираясь на данные крупнейших аналитических агентств, занимающихся вопросами информационной безопасности, (таких, как InfoWatch, Microsoft, McAfee Labs и Cisco Systems) можно судить о постоянным росте угроз сетевой безопасности, которые и без того составляют большую часть всех угроз. В связи с этим представляется актуальной разработка системы защиты корпоративной сети предприятия. В результате данной работы была спроектирована основная структура системы защиты корпоративной сети предприятия с применением программно-аппаратных средств обеспечения информационной безопасности.

При проектировании архитектуры используется подход к защите сети SNF (Cisco Secure Network Foundation). Этот подход предполагает внедрение разнообразных мер безопасности, реализованных в виде многоуровневой системы и управляемых в рамках единой стратегии. При этом многочисленные технологии и функции, обеспечивающие безопасность, развертываются в масштабе всей сети, дополняют друг друга и взаимодействуют между собой. Реализуемые в рамках единой стратегии меры безопасности призваны обеспечить максимальный уровень контроля и управления сетью.

Ключевые области, которые рассматриваются при обеспечении безопасности сети: доступ к устройствам, формирующим инфраструктуру; инфраструктура маршрутизации; устойчивость и безотказная работа устройств; сетевая телеметрия; обеспечение выполнения сетевой политики; инфраструктура коммутации. Для каждой области выделяются присущие ей угрозы и соответственные рекомендации по обеспечению безопасности. Чтобы гарантировать полноту решения, технологии и функции выбираются в соответствии с концепцией Cisco Security Framework (CSF), которая регламентирует методику оценки и проверки требований к безопасности системы и предписывает рассмотрение и выбор мер обеспечения безопасности для каждой конкретной области.

На рис. 1 представлена структура защищаемой сети предприятия с обозначением основных информационных потоков.

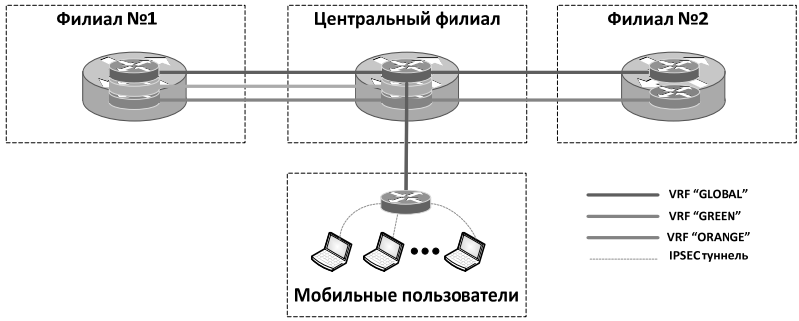


Рис. 1. Структурная схема VRF

Рис. 2. Функциональная модель системы защиты

Для разделения и изоляции отдельных видов производственного трафика между головным офисом, филиалами и мобильными пользователями применяется технология VRF, с помощью которой появляется возможность настраивать на одном маршрутизаторе несколько контекстов (таблиц) маршрутизации.

В соответствии с требованиями к безопасности корпоративной сети, перечню актуальных угроз и выбранной архитектурой построения безопасной сети было выбрано необходимое оборудование и спроектированы функциональная и логическая модели системы защиты (рис. 2, 3).

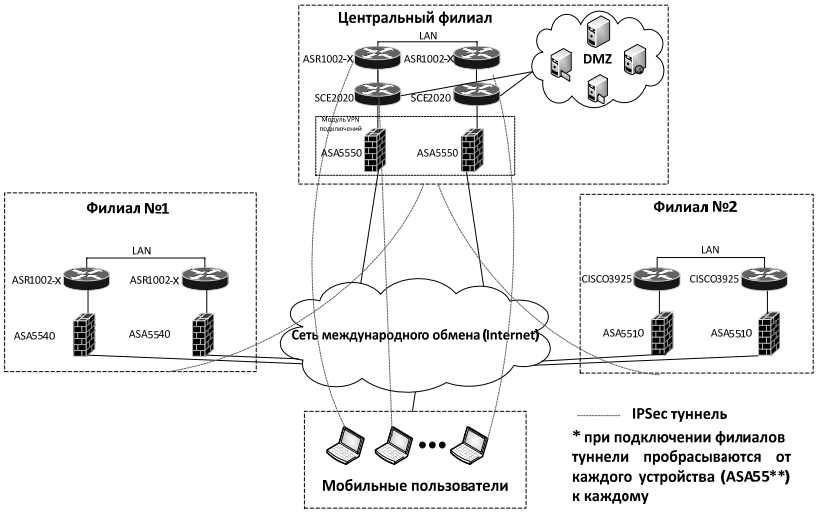


Рис. 3. Логическая модель системы защиты

ЛИТЕРАТУРА

1. Аналитический центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных данных [Электронный ресурс]. URL: http://www.infowatch.ru/analytics/reports/2583.

2. Архитектура и стратегия информационной безопасности Cisco [Электронный ресурс]. URL: http://www.smbtelecom.ru/Documentation/5_informatsionnaya_bezopasnost/1_obzor/arhitektura_i_strategiya_informacionnoy_bezopasnosti_cisco.pdf

3. Menga J., Timm C. CCSP: Secure Intrusion Detection and SAFE Implementation Study Guide. 2004. URL: http://books.google.ru/booksCCSP:+Secure +Intrusion+Detection+and+SAFE+pdf

4. Денисов П. Виртуализация сетевой инфраструктуры [Электронный ресурс]. 2012. URL: http://gasindustry.cisco.ru/files/20100329/VRF_Enterprise.pdf

ШИФР ХИЛЛА

С.Р. Субханкулова, студентка
Научный руководитель В.Н. Кирнос, доцент, к.т.н.
г. Томск, ТУСУР, каф. КИБЭВС, Sonya1m@yandex.ru

Одним из интересных многобуквенных шифров является шифр, разработанный математиком Лестером Хиллом (Lester Hill) в 1929 г., который базируется на линейной алгебре. Пространства исходных сообщений и криптотекстов совпадают: латинский алфавит. Перенумеруем буквы в порядке их следования в алфавите: A получает номер 0, B – номер 1, ... и Z – номер 25. Все арифметические операции выполняются по модулю 27.

27 (длина алфавита + пробел).

Выберем целое число $D <= 2$. Оно указывает размерность используемых матриц. В процедуре шифрования наборы из D букв шифруются вместе. Возьмем $D = 2$. Пусть ключ M – квадратная матрица порядка D, элементами которой являются числа 0 ... 26. Эта матрица должна удовлетворять требованию невырожденности, т.е. для неё должна существовать обратная матрица M–1, например:

$$M = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \quad \text{и} \quad M\text{–}1 = \begin{pmatrix} 3 & -3 \\ 2 & 5 \end{pmatrix}$$

(вся арифметика ведется по модулю 27).

Шифрование осуществляется с помощью уравнения $MP = C$, где P и C – вектор-столбцы длиной D. То есть каждый набор из D букв исходного сообщения определяет вектор P, компонентами которого являются номера букв. В свою очередь полученный вектор C также интерпретируется как набор из D букв.

Например: исходное сообщение: HELP определяет 2 вектора (по 2 буквы в каждом):

$$P1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \quad = \quad \text{и} \quad P2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}.$$

Из уравнений

$$M \times P1 = \begin{pmatrix} 6 \\ 7 \end{pmatrix} = C1 \text{ и } M \times P2 = \begin{pmatrix} 24 \\ 16 \end{pmatrix} = C2$$

получаем зашифрованный текст: GHYQ.

Для дешифровки сообщения используем матрицу M–1 [mod 27] и для шифротекста C вычисляем $P = M\text{–}1 \times C$ [mod 27].

В ходе работы была создана программа, которая очень проста в использовании. Программа представляет собой простейшую схему работы. При запуске пользователю предлагается ввести текст (латин-

ский), после чего появляются окошки для ввода элементов матрицы-ключа. После ввода элементов матрицы и нажатии кнопки «Проверить» в зависимости от того, имеет ли матрица обратную, появляется метка «Матрица подходит для расшифровки» или сообщение с просьбой ввести другие элементы матрицы (рис. 1).

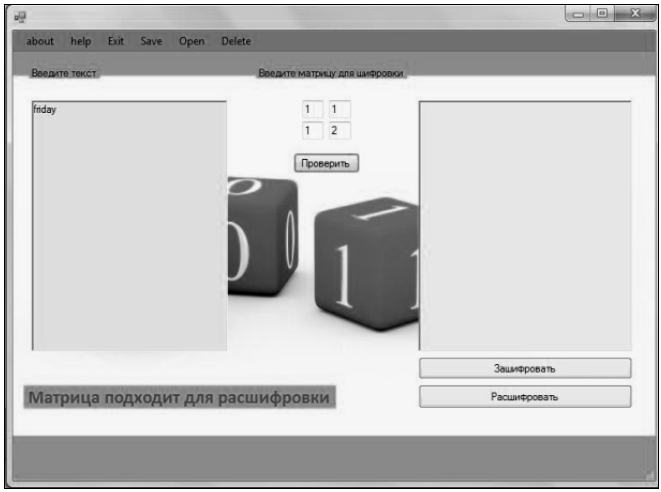


Рис. 1. Матрица имеет обратную

После того как будет введена подходящая матрица, появится окошко и кнопка «Зашифровать», при нажатии на которую текст будет зашифровываться: каждой букве будет поставлено в соответствие число, после чего элементы будут загоняться в матрицу и умножаться на матрицу-ключ, затем каждому числу будет поставлена в соответствие буква и результат будет выведен в окно (рис. 2).

Чтобы расшифровать текст, пользователь должен будет нажать кнопку «Расшифровать». При расшифровке каждой букве будет поставлено в соответствие число, после чего элементы будут загоняться в матрицу и умножаться на матрицу, обратную введённой. Затем каждому элементу результирующей матрицы будет поставлена в соответствие буква и результат будет выведен в соответствующее окно (рис. 3).

Пользователь также сможет сохранять и загружать исходный и зашифрованный текст, очищать окна и запрашивать пошаговую инструкцию использования программы, а также информацию о разработчике.

Для работы с данной программой достаточно одного пользователя, который имеет навыки работы в среде Windows.

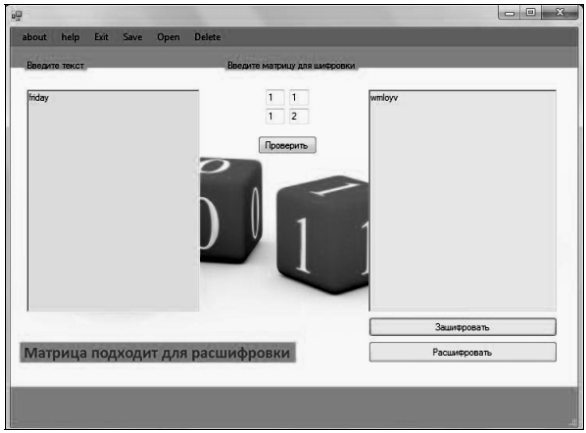


Рис. 2. Отображение зашифрованного текста во втором окне

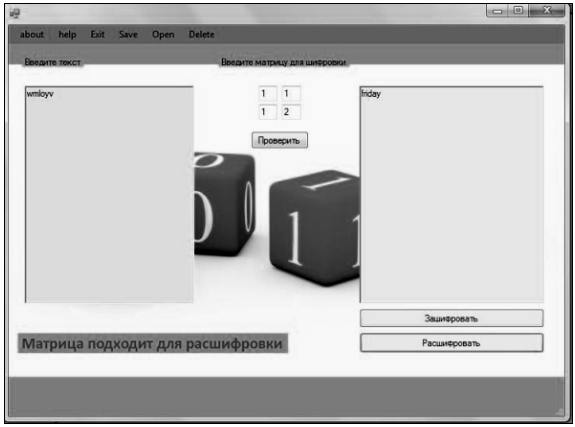


Рис. 3. Расшифровка текста

Данная программа может служить помощником пользователя в защите безопасности данных.

ЛИТЕРАТУРА

1. Кирнос В.Н., Шелупанов В.Н.. Информатика. Базовый курс. Томск: В-Спектр, 2010. 379 с.

2. Шилдт Г. C# 4.0: полное руководство. М.: Вильямс, 2011. 1056 с.

3. Кирнос В.Н. Курсовые работы по информатике. Томск: ТУСУР, 2009. 36 с.

АЛГОРИТМ КОНФИДЕНЦИАЛЬНОГО КЛАСТЕРНОГО АНАЛИЗА МЕТОДОМ K-MEANS ПРИ ВЕРТИКАЛЬНОМ СЕКЦИОНИРОВАНИИ ДАННЫХ

А.В. Вашкевич, студент, В.Г. Жуков, доцент каф. БИТ, к.т.н.
г. Красноярск, СибГАУ, каф. БИТ, zhukov.sibsau@gmail.com

В коммерческой сфере возникла необходимость проводить совместный анализ данных, например с помощью методов кластерного анализа, при этом сохраняя конфиденциальность своих данных, но получая некоторые общие выводы, необходимые всем участникам анализа [1]. С этими целями разрабатывались протоколы конфиденциальных вычислений для простых функций, использующие криптографические примитивы – относительно простые криптографические преобразования – для применения в рамках решения задачи конфиденциальных многосторонних вычислений (КМВ). Задача КМВ состоит в том, чтобы каждый из участников КМВ получил результат, но ни один из них не узнал никакую дополнительную информацию об анализируемых данных других участников.

Тривиальным решением задачи КМВ является использование третьей доверенной стороны, которой участники передают свои данные, – она выполняет необходимые вычисления и отсылает полученный результат обратно. Однако наличие такой доверительной стороны не всегда возможно и допустимо на практике.

В алгоритмах конфиденциальной кластеризации, как правило, используется модель с получестными (semi-honest) участниками. Получестный участник следует протоколу, но волен использовать ту информацию, к которой он имеет доступ во время выполнения протокола, для попытки раскрытия данных других участников. При этом рассматривается возможность сговора (т.е. объединения знаний) некоторых из участников КМВ. В случае, когда злоумышленник, предоставляет заведомо неверную информацию и срывает получение корректных результатов, то он все равно не может узнать конфиденциальную информацию, т.к. она не может быть получена из результата, к которому имеет доступ злоумышленник.

Отметим характеристические признаки конфиденциальной кластеризации:

1) большое количество данных (за счет интеграции информационных объемов данных для анализа несколькими участниками);

2) необходимость в передаче данных по глобальным сетям связи.

На первом этапе исследований по применению КМВ в кластеризации должен рассматриваться алгоритм, имеющий высокую скорость работы, позволяющий работать с большими объемами данных и

имеющий относительно простую алгоритмическую сложность, чтобы позднее можно было применить криптографические примитивы для более сложных протоколов. Наиболее распространенным и изученным алгоритмом кластерного анализа, удовлетворяющим предъявляемым требованиям, является k-means – прообраз практически всех алгоритмов неиерархической кластеризации.

Данные для кластеризации могут быть по-разному распределены между участниками – различают вертикальное (участники содержат разные столбцы данных), горизонтальное (разные строки данных) и арбитральное (произвольное) секционирования данных. В зависимости от распределения различаются этапы кластеризации, в которых нужно сохранять конфиденциальность. При исследовании существующих решений было установлено, что при горизонтальном секционировании конфиденциальность обеспечивается существующими алгоритмами, перспективным является только недопущение раскрытия центров кластеров. Арбитральное секционирование данных на практике распространено мало. Рассмотрим подробно протокол с вертикальным секционированием.

На каждой итерации алгоритма конфиденциальной кластеризации при вертикальном секционировании с более чем двумя участниками вначале выполняется определение ближайшего кластера для всех точек. Было предложено два принципиально разных подхода:

1. Сначала между «особыми» участниками распределяется каждое расстояние от точки до всех кластеров, потом эти участники находят наименьшее из расстояний. «Особые» участники ни в коем случае не должны сговариваться друг с другом.

2. Все участники ищут (суммируют) не расстояния от точки до кластеров, а разницу между расстояниями от точки до кластеров. Следовательно, после суммирования достаточно определить, больше нуля разница или нет. Таким образом, при таком подходе в алгоритме отсутствуют «особые» участники, все участники равны между собой, а при сговоре нескольких участников будут раскрыты лишь косвенные данные.

Ко второму подходу относится только работа Самета и Мири [2]. В работе предложено использовать безопасную сумму (Secure Sum). Этот примитив также требует наличия несговаривающихся участников (участников i и $i+2$), однако протокол можно усложнить с помощью дробления слагаемых на части и изменения маршрута суммирования. Впрочем, у данного усовершенствования алгоритма есть недостаток: в случае $r=3$ участников маршруты нельзя менять, а при $r>3$ количество сговорившихся для раскрытия данных участников должно быть равно $r-1$, и при малых r возможностью сговора нельзя пренебречь

для данной модели нарушителей. Следовательно, при малом количестве участников необходимо осуществлять другой протокол суммирования.

Таким протоколом может быть безопасное скалярное произведение (Secure Dot Product, SDP) [3]. Протокол позволяет получать $\sum s_i = \prod r_i$, где s_i и r_i – известные только i-му участнику числа. Основной минус протокола: количество данных, передаваемых по сети, растёт пропорционально квадрату количества участников. Значит, при большом количестве данных, когда принципиален объем передаваемого трафика, необходимо обеспечить как можно меньшее количество передач между участниками. Можно применить усовершенствованную безопасную сумму. Существующие модернизации алгоритма не обладают преимуществом в скорости перед SDP, потому что дробят данные на максимально возможное количество частей, равное количеству всех участников. Необходимо разработать алгоритм, позволяющий дробить данные на минимальное количество частей так, чтобы обеспечивалась конфиденциальность для конкретной модели (с указанием допустимого количества сговорившихся участников).

Таким образом, в работе проведено исследование проблемы конфиденциальной кластеризации методом k-means при вертикальном секционировании данных, предложены пути модернизации существующих протоколов и определены условия, при которых необходимо применять тот или иной криптографический примитив.

Работа поддержана грантом Президента молодым кандидатам наук МК-473.2013.9.

ЛИТЕРАТУРА

1. Шутый Р.С. Рандомизированные протоколы, применяемые для выполнения конфиденциальных многосторонних вычислений в компьютерных сетях» // Санкт-Петербургский гос. ун-т телекоммуникаций им. М.А. Бонч-Бруевича, 2009.

2. Samet S., Miri A., Orozco-Barbosa L. Privacy-Preserving K-Means Clustering in Multi-Party Environment. Proceedings of International Conference on Security and Cryptography, Barcelona, Spain, 2007.

3. Malek B., Miri A. Secure dot-product protocol using trace functions. Proceedings of the IEEE International Symposium on Information Theory, 2006.

ИНТЕРНЕТ НА СЛУЖБЕ ТЕРРОРИЗМА

И.С. Васильева, студентка

Научный руководитель О.Н. Мызников, декан, доцент

г. Краснодар, КубГТУ, ИИТиБ, inna1523@mail.ru

Киберпространство предоставляет новые поля битв, которые террористические организации используют как средство достижения сво-

их кампаний. Большинство развитых стран переходят в режим электронного государства, дающего террористам новые цели. Как и в обычной повседневной среде, Интернет предлагает настоящие цели, которые станут привлекательными для определенных террористических организаций.

Рассмотрим борьбу с терроризмом в киберпространстве, т.е. кибертерроризм как форму нападения с использованием Интернета в качестве инструмента террористических действий.

Для начала нужно рассмотреть самих террористов, ведь понимание их психологии – наикратчайший путь к победе. Нет четкого профиля террориста, они приходят из всех слоев общества и различных уровней образования, занятости. Мы должны признать, что большинство террористических групп – это квалифицированные и умные люди, которые действуют с подлинной верой, а не группа невежд. Это следует учитывать в плане киберзащиты от терроризма. Они будут учиться, им потребуется время для планирования и найма специалистов самой высокой квалификации для достижения своей цели. Террористические группы испытывают трудности в передаче своих политических сообщений широкой публике, не подвергшись цензуре. И тут на выручку приходит Интернет и становится для них своеобразным транспортным средством.

Некоторые причины, почему кибертерроризм может стать более привлекательным для террористических групп:

– риск захвата уменьшается, поскольку атаки могут происходить удаленно;

– возможность нанести серьезные финансовые убытки без физических потерь;

– для этих нападений могут быть наняты профессионалы извне;

– успешная атака может получить всеобщую огласку, а неудачная останется незамеченной;

– привлечение сторонников по всему миру;

– использование Интернета в качестве метода мобилизации средств со всего мира;

– Интернет – идеальный инструмент пропаганды террористических групп, которые работает на глобальной основе и отдельные государства не могут контролировать их деятельность.

Преимущества кибертеррористических методов свидетельствуют о нарастающем числе террористических действий, совершенных посредством Интернета.

Деятельность радикальных групп широко распадается на две категории: поддержка мероприятий и оперативная деятельность.

Поддержка мероприятий в Интернете включает в себя распространение террористических целей с помощью пропаганды в поддерж-

ку радикализации мысли, такие как распространение и поощрение насилия. Многие террористические организации – хорошо организованные и финансируемые пропагандистские машины, службы новостей, видеоканалы и радиостанции в Интернете. Существует множество доказательств того, что кибер-джихадисты создают компьютерные игры, целью которых является убийство израильского солдата, президента США и т.д. Эти игры, безусловно, существуют и свободно распространяются в киберпространстве как средство распространения насилия и киберджихадистской точки зрения. Есть также сообщения, раскинутые по Интернету и направленные специально на детей для радикализации с раннего возраста.

Сбор средств является еще одной серьезной поддержкой террористической деятельности, которая происходит через Интернет с использованием новых форм денег, таких как WebMoney, с помощью кредитной карты и др.

Теперь Интернет – это новая общность, где террористы могут собраться вместе и убедить друг друга в правильности поставленных целей.

Оперативная деятельность. Огромные ресурсы Интернета, словно учебные пособия, которые могут помочь любому человеку самостоятельного обучиться радикальной программе.

Существует документ «Энциклопедия джихада» (the *Encyclopedia of Jihad*), который находится в открытом доступе, имеет несколько тысяч страниц и охватывает все – от того, «как построить самодельное взрывное устройство», до того, «как создать оружие массового уничтожения», «как участвовать в тайной связи», «как избежать обнаружения со стороны полиции». Интернет способствует оперативной террористической деятельности через свои коммуникационные возможности, позволяющие командовать и управлять в киберпространстве через вычислительные сети, текстовые сообщения, IP-телефонию или через использование анонимных ремейлеров. Интернет является одним из выдающихся оперативных мест для запугивания и терроризирования общественности.

Возможно, одним из наиболее перспективных особенностей Интернета является то, что он дает голос многим, кто не в состоянии вызвать внимание СМИ. Всемирная паутина нерегулируема и доступна практически каждому.

Изменение характера угроз привело к введению новых категорий приоритетов национальной безопасности, таких как:

– Национальная защита критически важных инфраструктур.

– Возврат к концепции обороны Родины; глубокое воздействие как на состав, так и на функциональные возможности разведывательного сообщества.

– Создание глобальных и региональных альянсов против терроризма и распространения оружия массового уничтожения и наркотрафика, для извлечения выгоды из совместных международных условий и обмена оперативной информацией.

Последствием таких изменений с функциональной стороны является рост потребности в разведывательных аналитиках нового образца. Они должны обладать набором навыков, которые имеют решающее значение в современных условиях.

С управленческой стороны не стоит полагаться только лишь на разведку. Глобальный охват и контрразведка имеют большее значение в наше время, время нетрадиционных угроз.

Безопасность является деятельностью, которая должна постоянно совершенствоваться в соответствии с динамичной средой угроз. Информационные ресурсы являются ключевой основой для «выживания» при атаке, и они же – фундаментальная цель. Для того чтобы реагировать на угрозы, нужно вовремя выявлять, пресекать, оценивать, предупреждать, реагировать и расследовать компьютерные вторжения и иные противоправные действия. Исходя из этого, следующая формула актуальна как никогда: Объединение возможностей + Инновации + Ресурсы + Лидерство = Стратегическое преимущество.

Только сотрудничество между странами остановит рост Интернет-преступлений – сейчас время консолидации. Время усиления систем наших оборон перед лицом нарастающей опасности ужасающего будущего!

ЛИТЕРАТУРА

1. Барис В.В. Геополитические контуры России. М., 2002. 392 с.
2. Расторгуев С.П. Информационная война. М., 1998. 415 с.

РАЗРАБОТКА ПРОЕКТА ЛАБОРАТОРНОГО СТЕНДА «СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ»

С.А. Волков, студент
Научный руководитель А.С. Ковтун, инженер ЦТБ ТУСУРа
г. Томск, ТУСУР, каф. КИБЭВС, Semyon@mail2000.ru

Системы видеонаблюдения находят широкое применение в различных областях нашей жизни.

Главная задача – защитить имущество (дом, дачу, квартиру, автомобиль) от злоумышленников [1].

И еще видеонаблюдение создает систему глобальной безопасности, которая, отслеживая повседневную ситуацию, позволяет вовремя заметить скрытую угрозу [2].

Целью преддипломной практики является разработка проекта лабораторного стенда «Системы видеонаблюдения». Стенд «Системы видеонаблюдения» необходим для усовершенствования методической и материально-технической базы кафедры КИБЭВС, предназначен для проведения лабораторных работ студентами кафедры. Лабораторный стенд будет располагаться в учебной аудитории №108 корпуса ФЭТ ТУСУРа.

Данный учебный стенд должен существенно облегчить обучение студентов. В процессе обучения студенты кафедры изучат средства видеонаблюдения и регистрации, технические характеристики оборудования и научатся применять полученные знания на практике:

– подключение видеокамер;

– режимы работы видеорегистратора.

В рамках выполнения преддипломной практики для создания лабораторного стенда «Системы видеонаблюдения» была выбрана система видеонаблюдения на основе видеорегистратора.

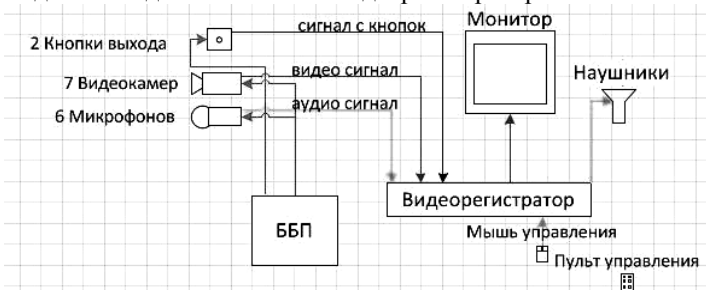


Рис. 1. Структурная схема подключения

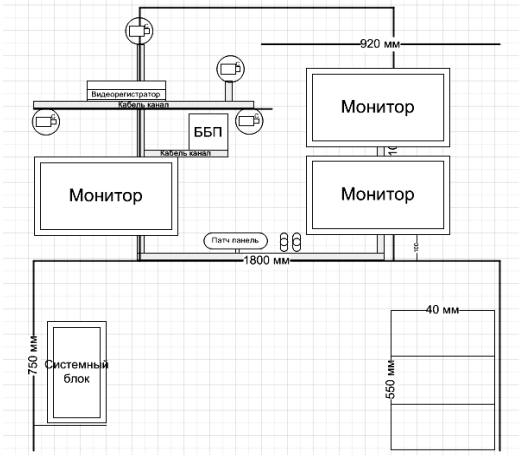


Рис. 2. Проект рабочего стенда «Системы видеонаблюдения»

Также был спроектирован сам стенд и рабочее место оператора.

Рабочее место включает: рабочий стол, 3 мягких стула, 3 монитора, компьютер, мышь, клавиатуру, видеокамеры, микрофоны, источник питания для камер, видеорегистратор, кнопки выхода и соединительные провода.

В конечном итоге преддипломной практики частично собран проект лабораторного стенда «Системы видеонаблюдения» (рис. 3).

Рис. 3. Частично собранный проект лабораторного стенда «Системы видеонаблюдения»

В результате проделанной работы был разработан и частично собран проект лабораторного стенда «Системы видеонаблюдения». Были исследованы принципы работы систем видеонаблюдения, их состав, тип, а также способы подключения компонентов видеонаблюдения, используя разные типы кабелей.

Продолжением преддипломной практики будет написание дипломного проекта, в котором планируется завершение сборки стенда и разработка лабораторных работ:

1. Подключение компонентов системы видеонаблюдения, используя различные типы кабелей.
2. Настройка и управление компонентами системы видеонаблюдения через сеть Интернет.
3. Администрирование систем видеонаблюдения на основе видеорегистратора.
4. Организация системы видеонаблюдения, реагирующей на движение и тревожные датчики.
5. Исследование работы видеокамеры с вариофокальным объективом.
6. Определение угла обзора объективов видеокамер.

ЛИТЕРАТУРА

1. Лафишев М.А. Проектирование систем видеонаблюдения, предназначенных для эксплуатации в темное время суток и в условиях плохой видимости // Матер. междунар. науч.-практ. конф. «Инновации на основе информационных и коммуникационных технологий». 2011. С. 300–303.

2. Булгаков В.Г. Системы видеонаблюдения как средство фиксации динамических признаков человека // Всерос. науч.-практ. конф. «Современные проблемы борьбы с преступностью»: сб. матер. (юридические науки). 2010. С. 18–19.

3. ГОСТ Р 78.36.008-99. Проектирование и монтаж систем охранного телевидения и домофонов. Рекомендации.

4. Требования Санитарных правил и норм (СанПиН) 2.2.2/2.4.1340–03.

РАЗРАБОТКА ИНФОРМАЦИОННОГО ТАБЛО ДЛЯ ВЫВОДА И ОБРАБОТКИ ИНФОРМАЦИИ НА ПРИМЕРЕ РАБОТЫ СЕКРЕТАРИАТА СОРЕВНОВАНИЙ

Е.В. Воронко, студент

Научный руководитель Д.В. Кручинин, ассистент

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

Проект ГПО-1204 – «Инженерия баз данных»

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

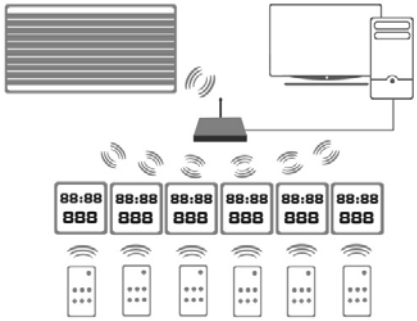


Рис. 1. Автоматизированный комплекс

Разработка автоматизированного комплекса, который представляет собой сложную систему передачи, приема, хранения, обработки и отображения информации, производится поэтапно (рис. 1).

Первая операция, которую выполняет автоматизированный комплекс, – это прием информации с пульта дистанционного управления (информации о спортивных соревнованиях). С пульта поступает такая информация, как время и кол-во выполненных упражнений спортсменом.

Все это отображается на семисегментном индикаторе малого информационного табло. После того как спортсмен закончил выполнять упражнение, данные с малого табло передаются в базу данных в ЭВМ с последующим хранением и обработкой. Вся информация передается через беспроводную сеть (в роли приемника-передатчика выступает радиостанция, которая является главным связывающим звеном всего аппаратного комплекса). После обработки данных в СУБД вся необходимая информация выводится на большое индикаторное табло.

Цель данной работы – разработка информационного табло для ввода и обработки информации на примере работы секретариата соревнований.

Первым этапом в рамках данной работы было разработано малое электронное табло. Информационное табло представляет собой двухстороннее табло, размеры которого 600×600 мм и толщина не более 30 мм (рис. 2, 3).

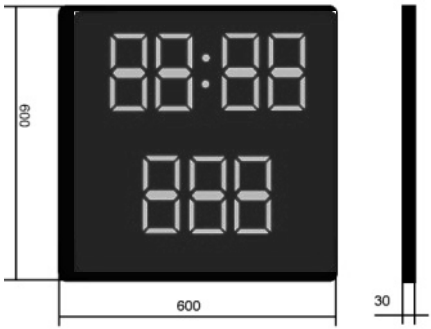


Рис. 2. Основной вид табло

Рис. 3. Разъемы с боковой стороны

Основой частью малого электронного табло является однокристальный микроконтроллер Atmega 16L и сверхяркий светодиод SMD5050, в результате чего стоимость спроектированного малого табло низкая по сравнению с его аналогами (электронная схема изображена на рис. 4).

Помимо самого табло, были реализованы приемная (рис. 6) и передающая (рис. 5) части. Передающая часть (пульт ДУ) состоит из передатчика MAX1479 + шифратор команд ATMEGA8L и приемной части, которая состоит из MAX1473, является супергетеродинной и может работать на частоте 315–433 МГц (подключается напрямую к основной схеме табло).

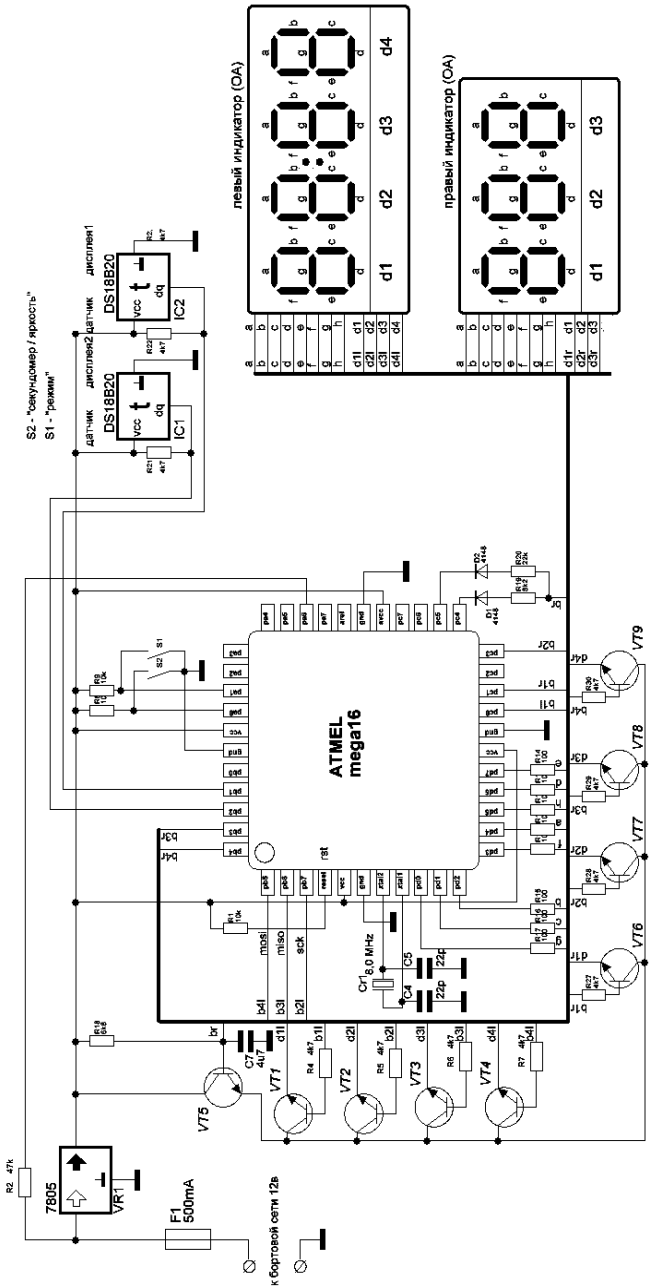


Рис. 4. Основная схема табло

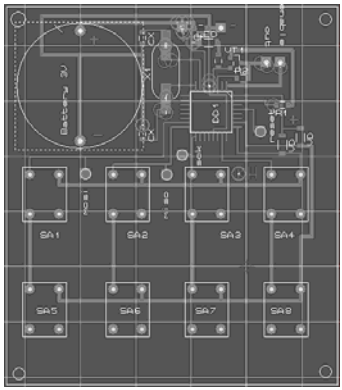


Рис. 5. Передатчик

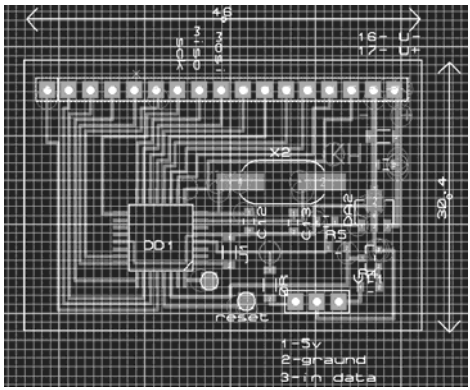


Рис. 6. Приемник

ЛИТЕРАТУРА

1. Мортон Д. Микроконтроллеры AVR. Вводный курс. М.: Додэка–XXI, 2006. 274 с.

2. Денисов Н.П., Шарапов А.В., Шибаев А.А. Электроника и схемотехника. Ч. 1, 2. Томск, 2003. 270 с.

3. Шустов М.А. Практическая схемотехника. Ч. 1–3. М.: Альтекс-А, 2003.

КЛЮЧЕВОЙ КОНТЕЙНЕР

Е.В. Цыбань, С.В. Штыгайло, А.Ю. Якимук, студенты,
М.А. Сопов, ст. преподаватель
г. Томск, ТУСУР, ФВС, каф. КИБЭВС, yakimuk-alex@mail.ru

В современном мире для подтверждения авторства документа, контроля его целостности и поддержания защиты информации, содержащейся в нем, от перехвата используют цифровую подпись. Цифровая подпись содержит в себе связку открытого и закрытого ключей шифрования. В свою очередь, к открытому ключу прилагается личный сертификат – это такой цифровой документ, которым подтверждается соответствие между информацией, способной однозначно идентифицировать владельца ключа, и его открытым ключом.

Поскольку использование сертификатов задействует большую аудиторию пользователей, чем использование ключевых контейнеров, информации по сертификатам (чем они являются, какие существуют виды, применение) гораздо больше. Сведения о сути ключевых контейнеров крайне труднодоступны. В Интернете можно найти или вопросы пользователей с просьбой помочь в решении возникших ошибок при работе с ключевым контейнером, или крайне отдаленные от

строгого определения слова. Открытый ключ является необходимым при проверке подлинности документа, а соответствующий ему закрытый ключ – для зашифровки данных.

Сертификаты могут быть представлены в следующих форматах:

– «*.cer» и «*.crt» – представляют собой сертификаты в формате X.509. Включают два варианта: платформенно-независимый метод хранения сертификатов (DER encoded binary X.509) и вариант кодирования, который был разработан для прохождения сертификатом без повреждений через все почтовые шлюзы (Base-64 encoded X.509).

– «*.p7b» и «*.spc.» – сертификаты стандарта PKCS #7 позволяют пользователю сохранять кроме самого сертификата еще и его путь сертификации.

– «*.pfx» и «*.p12» – файл обмена личной информации PKCS #12, позволяющий включать закрытые ключи. Непременным условием разрешения на включение закрытого ключа является то, что ключ помещается как разрешённый к экспорту.

– «*.sst» – формат, используемый в случае, если экспортируется сразу несколько сертификатов [1].

Формат сертификата определяет структуру самого контейнера. Расширения стандартов PKCS#8 и PKCS#12 используются в качестве транспортного ключевого контейнера ключей ГОСТ Р 34.10-2001 [2]. Ключевой контейнер – это объект, хранящий закрытый ключ и сертификат открытого ключа (соответствующий ему закрытый ключ + открытый ключ в общем случае). Федеральная служба безопасности (ФСБ), которая сертифицирует СКЗИ, не предъявляет жестких требований к формату ключевого контейнера. Соответственно каждый разработчик создает контейнер в своем СКЗИ (средства криптографической защиты информации) на свое усмотрение. Возникает проблема, когда контейнер, созданный в одном СКЗИ, не распознается, а соответственно и не используется в другом, что в свою очередь ограничивает пользователей.

Ключевой контейнер представляет собой папку с шестью файлами, имеющими расширение «*.key» (рис. 1). Если данные файлы будут повреждены или утеряны, закрытый ключ не будет работать, а значит – будет невозможно поставить цифровую подпись под документом или подтвердить, кому этот документ принадлежит. Восстановить ключевой контейнер является невозможной задачей в условиях, если нет в наличии его резервной копии.

Рис. 1. Пример содержимого ключевого контейнера для «КриптоПро CSP»

Таким образом, ключевые контейнеры – это специализированная методика хранения закрытых ключей. И их физическое представление целиком и полностью зависит от того, к какому типу относится ключевой носитель, на который данные файлы были записаны. Это может быть flash-накопитель, дискета, жесткий диск, в некоторой директории которого и расположен набор файлов, содержащий ключевую информацию. В ситуациях, когда в качестве ключевого носителя выбрана смарт-карта, файлы хранятся в защищенной области памяти смарт-карты. А в случае с реестром их содержит раздел реестра, отвечающий за хранение параметров. Если используется дискета или flash-накопитель, копирование ключевого контейнера возможно выполнить средствами Windows. Также этот способ доступен для версий КриптоПро CSP не ниже 3.0.

Пароль, устанавливаемый на контейнер, для смарт-карт и для прочих типов носителей имеет разное значение. Ключи для смарт-карт обычно защищаются дополнительно специальным кодом доступа, необходимым для обращения к защищенной памяти смарт-карты (Personal Identification Number – PIN), задаваемым при формировании ключевого контейнера и запрашиваемым при каждой из возможных операций, проводимых с защищенной памятью (чтение, запись, удаление и др.). Для других носителей с целью повышения безопасности на контейнер можно установить пароль. В этом случае всё содержимое контейнера хранится не в открытом виде, а в зашифрованном на этом пароле. Пароль задается при создании контейнера, в дальнейшем для чтения ключей из контейнера необходимо будет вводить пароль [3].

Существует некоторые ограничения на использование ключевых контейнеров. Так, например, в одном ключевом контейнере одновременно могут находиться не более одной пары ключей подписи, одной пары ключей обмена и одного симметричного ключа. В ситуации, когда используются более одного алгоритма симметричного шифрования, соответствующих ключей может оказаться несколько, а именно, по одному ключу на каждый из алгоритмов. В паре лишь открытый ключ может быть вне контейнера. Закрытые ключи в паре ключей экспортируются исключительно в зашифрованном виде. Некоторыми криптопровайдерами искусственно создана ситуация, когда принципиально запрещен экспорт закрытых ключей, даже в зашифрованном виде. Симметричные ключи при экспорте подлежат обязательному шифрованию на открытом ключе лица, получающего их, либо на ключе согласования. Для вычисления хеш-функций создаются объекты хеширования. Для создания объектов хеширования создавать контейнер не нужно.

ЛИТЕРАТУРА

1. Форматы файлов сертификатов [Электронный ресурс]: Электрон. дан. [Technet Microsoft]. Режим доступа: http://technet.microsoft.com/ru-ru/library/cc770735.aspx, свободный. Загл. с экрана.

2. Транспортный ключевой контейнер [Электронный ресурс]: Электрон. дан. [Методические рекомендации технического комитета по стандартизации «Криптографическая защита информации»]. Режим доступа: https://www.tc26.ru/metodiki/containers_v1/transport_v1.html, свободный. Загл. с экрана.

3. Что такое ключевой контейнер? Зачем нужен пароль на контейнер? [Электронный ресурс]: Электрон. дан. [КриптоПро]. Режим доступа: http://www.cryptopro.ru/faq/chto-takoe-klyuchevoi-konteiner-zachem-nuzhen-parol-na-konteiner, свободный. Загл. с экрана.

СОДЕРЖАНИЕ

СЕКЦИЯ 16

ВЫЧИСЛИТЕЛЬНЫЙ ИНТЕЛЛЕКТ

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

СЕКЦИЯ 17
АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

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

СЕКЦИЯ 18

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель секции – **Шелупанов А.А.**, проректор по НР ТУСУРа, зав. каф. КИБЭВС, д.т.н., профессор*
*зам. председателя – **Конев А.А.**, доцент каф. КИБЭВС, к.т.н.*

Научное издание

Материалы
Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2013»

15–17 мая 2013 г., г. Томск

В пяти частях

Часть 4

Корректор – **В.Г. Лихачева**
Верстка **В.М. Бочкаревой**

Издательство «В-Спектр»
Сдано на верстку 01.04.2013. Подписано к печати 30.04.2013.
Формат $60\times84^{1}/_{16}$. Печать трафаретная. Печ. л. 16,625.
Тираж 500 экз. Заказ 11.

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