Министерство образования и науки Российской Федерации
Федеральное агентство по образованию

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

НАУЧНАЯ СЕССИЯ ТУСУР–2010

**Материалы докладов
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2010»**

4–7 мая 2010 г.

В пяти частях

Часть 3

В-Спектр
2010

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

Н 34 **Научная сессия ТУСУР–2010:** Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 4–7 мая 2010 г. – Томск: В-Спектр, 2010. Ч. 3. – 280 с.
ISBN 978-5-91191-131-7
ISBN 978-5-91191-134-8 (Ч. 3)

Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых посвящены различным аспектам разработки, исследования и практического применения радиотехнических, телевизионных и телекоммуникационных систем и устройств, сетей электро- и радиосвязи, вопросам проектирования и технологии радиоэлектронных средств, аудиовизуальной техники, бытовой радиоэлектронной аппаратуры, а также автоматизированным системам управления и проектирования. Рассматриваются проблемы электроники СВЧ- и акустооптоэлектроники, нанофотоники, физической, плазменной, квантовой, промышленной электроники, радиотехники, информационно-измеритель-ных приборов и устройств, распределенных информационных технологий, вычислительного интеллекта, автоматизации технологических процессов, в частности в системах управления и проектирования, информационной безопасности и защите информации. Представлены материалы по математическому моделированию в технике, экономике и менеджменте, антикризисному управлению, автоматизации управления в технике и образовании. Также представлены доклады, касающиеся социокультурных проблем современности, экологии, мониторинга окружающей среды и безопасности жизнедеятельности.

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

ISBN 978-5-91191-131-7
ISBN 978-5-91191-134-8 (Ч. 3)

Вступительное слово

Здравствуйте, уважаемые коллеги! Вы держите в руках сборник работ студентов, аспирантов и молодых ученых, подготовленный Институтом системной интеграции и безопасности ТУСУРа (ИСИБ). На сегодняшний момент в состав института входят: Центр технологий безопасности, Удостоверяющий центр Сибири, Аттестационный центр по обработке конфиденциальной информации, Центр подготовки и переподготовки кадров, филиал ТУСУРа в г. Сургуте, кафедра комплексной информационной безопасности электронно-вычислительных систем, научно-производственные лаборатории: безопасных биомедицинских технологий, систем безопасности, речевых технологий, а также студенческое конструкторского бюро «Старт». С момента создания института прошло всего два года, однако за этот короткий период была проделана колоссальная работа.

За прошедший год институтом подготовлено и выпущено 5 учебников, 13 учебных пособий, из них 10 – с грифом СибРОУМО вузов по образованию в области информационной безопасности, 3 сборника научных и методических работ, более 110 научных публикаций в различных сборниках трудов и журналах, проведен IX Всероссийский конкурс студентов и аспирантов по информационной безопасности. Продолжен выпуск специалистов по защите информации, инженеров по проектированию и технологии ЭВС, в 2009 г. количество выпускников составило 108 человек.

Знаменательным событием прошедшего года стала высокая оценка многолетней работы коллектива на государственном уровне. Руководитель авторского коллектива профессор А.А. Шелупанов, профессор кафедры КИБЭВС А.П. Зайцев, доцент кафедры КИБЭВС Р.В. Мещеряков стали лауреатами премии Правительства Российской Федерации 2009 г. в области образования за создание комплекта учебных пособий, учебников и монографий по криптографическим, программно-аппаратным, техническим методам и средствам защиты информации, обеспечивающего подготовку специалистов в области информационной безопасности для образовательных учреждений высшего профессионального образования.

Следует отметить достижения начинающих исследователей – студентов и аспирантов кафедры. Аспирант В.Д. Зыков был назначен на стипендию Правительства РФ, студент А.И. Гуляев – на именную стипендию компании Dr.Web. Премию для поддержки талантливой молодежи, учрежденную Президентом РФ, получил студент 5-го курса, ныне аспирант В.В. Летахов. Это далеко не полный список побед за

прошедший год, что позволяет с уверенностью смотреть в будущее, благодаря успехам наших воспитанников и преемников.

Ставший традиционным тематический сборник «Системная интеграция и безопасность» составлен по результатам современных научных исследований в области автоматизации и информационной безопасности. Большая часть материалов подготовлена студентами и аспирантами под руководством сотрудников кафедры КИБЭВС института системной интеграции и безопасности. Это подразделение института имеет более чем 35-летнюю историю подготовки специалистов в области автоматизации, а также является одним из первых в стране и успешно развивающихся коллективов, углубленно занимающихся исследованиями в сфере информационной безопасности и подготовкой соответствующих специалистов.

Настоящий сборник включает более сотни работ. Как и в предыдущие годы, в его наполнении также приняли участие молодые ученые из различных регионов нашей страны: от Калининграда до городов Дальнего Востока. В этом году работы из других регионов составляют около 20% объема сборника, что свидетельствует об актуальности в России направлений работы нашего коллектива. Спасибо всем авторам за готовность поделиться с научным и профессиональным сообществом своими результатами!

С уважением проректор по научной работе,
директор Института системной интеграции и безопасности,
доктор технических наук, профессор,
академик МАНВШ, МАИ, АПБОП ***А.А. Шелупанов***

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

Всероссийская научно-техническая конференция студентов и молодых ученых «Научная сессия ТУСУР–2010» 4–7 мая 2010 г.

ПРОГРАММНЫЙ КОМИТЕТ

- Кобзев А.В. – председатель, президент ТУСУР, д.т.н., профессор;
- Шелупанов А.А. – сопредседатель, проректор по НР ТУСУР, зав. каф. КИБЭВС ТУСУР, д.т.н., профессор;
- Шурыгин Ю.А., ректор ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор;
- Ехлаков Ю.П., проректор по информатизации и управлению ТУСУР, д.т.н., профессор;
- Уваров А.Ф., проректор по инновационному развитию и международной деятельности ТУСУР, к.э.н.;
- Малютин Н.Д., начальник НУ ТУСУР, д.т.н., профессор;
- Казьмин Г.П., председатель комитета инновационной деятельности администрации г. Томска, представитель Фонда содействия развитию МФП в НТС по Томской обл., к.т.н.;
- Малюк А.А., декан фак-та информационной безопасности МИФИ, к.т.н., г. Москва;
- Беляев Б.А., зав. лабораторией электродинамики Ин-та физики СО РАН, д.т.н., г. Красноярск;
- Разинкин В.П., д.т.н., профессор, каф. ТОР НГТУ, г. Новосибирск;
- 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;
- Кориков А.М. – зав. каф. АСУ ТУСУР, заслуженный деятель науки РФ, д.т.н., профессор;
- Пустынский И.Н., зав. каф. ТУ ТУСУР, заслуженный деятель науки и техники РФ, д.т.н., профессор;
- Акулиничев Ю.П., председатель совета по НИРС РТФ, профессор каф. РТС ТУСУР, д.т.н.;
- Орликов Л.Н., председатель совета по НИРС ФЭТ, профессор каф.

ЭП ТУСУР, д.т.н.;
- Казакевич Л.И., председатель совета по НИРС ГФ, доцент каф. ИСР ТУСУР, к.ист.н.;
- Шарыгин Г.С., зав. каф. РТС ТУСУР, д.т.н., профессор;
- Голиков А.М., доцент каф. РТС ТУСУР, к.т.н.;
- Еханин С.Г., председатель совета по НИРС РКФ, д.ф.-м.н., профессор каф. КУДР ТУСУР;
- Лощилов А.Г., м.н.с. СКБ «Смена» ТУСУР, к.т.н.;
- Катаев М.Ю., профессор каф. АСУ ТУСУР, д.т.н.;
- Шарангович С.Н., зав. каф. СВЧиКР ТУСУР, к.ф.-м.н., доцент;
- Троян П.Е., зав. каф. ФЭ ТУСУР, д.т.н., профессор;
- Ходашинский И.А., профессор каф. АОИ, д.т.н.;
- Давыдова Е.М., зам. заф. каф. КИБЭВС по УР, доцент каф. КИБЭВС, к.т.н.;
- Коцубинский В.П., председатель совета по НИРС ФВС, зам. зав. каф. КСУП ТУСУР, доцент каф. КСУП, к.т.н.;
- Титов А.А., профессор каф. РЗИ ТУСУР, д.т.н.;
- Михальченко Г.Я., профессор каф. ПрЭ, д.т.н.;
- Мицель А.А., председатель совета по НИРС ФСУ, зам. зав. каф. АСУ ТУСУР, д.т.н., профессор;
- Осипов Ю.М., зав. отделением каф. ЮНЕСКО ТУСУР, академик Международной академии информатизации, д.э.н., д.т.н., профессор;
- Семиглазов А.М., профессор каф. ТУ, д.т.н.;
- Карташов А.Г., проф. каф. РЭТЭМ, д.б.н., профессор;
- Суслова Т.И., декан ГФ, зав. каф. КС, д.ф.н., профессор;
- Грик Н.А., зав. каф. ИСР ТУСУР, д.ист.н., профессор;
- Дмитриев В.М., зав. каф. ТОЭ, д.т.н., профессор;
- Пуговкин А.В., зав. каф. ТОР, д.т.н., профессор.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

- Шелупанов А.А. – сопредседатель, проректор по НР ТУСУР, зав. каф. КИБЭВС ТУСУР, д.т.н., профессор;
- Ярымова И.А. – зам. председателя, заведующий ОППО ТУСУР, к.б.н.;
- Юрченкова Е.А. – секретарь оргкомитета, инженер ОППО ТУСУР, к.х.н.

СЕКЦИИ КОНФЕРЕНЦИИ

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

Секция 2. Защищенные телекоммуникационные системы. Председатель секции – Голиков А.М., к.т.н., доцент каф. РТС.

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

Секция 4. Проектирование биомедицинской аппаратуры. Председатель подсекции – Еханин Сергей Георгиевич, д.ф.-м.н., профессор каф. КУДР.

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

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

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

Секция 8. Физическая и плазменная электроника. Председатель секции – Троян Павел Ефимович, зав. каф. ФЭ, д.т.н., проф.

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

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

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

к.т.н., доцент каф. КИБЭВС.

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

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

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

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

Подсекция 12.4. Методы стереоскопической визуализации. Председатель подсекции – Дорофеев Сергей Юрьевич, ассистент каф. КСУП.

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

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

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

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

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

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

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

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

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

Секция 20. Экология и мониторинг окружающей среды. Председатель секции – Карташев Александр Георгиевич, д.б.н., профессор каф. РЭТЭМ; зам. председателя – Смолина Татьяна Владимировна, к.б.н., ст. пр. каф. РЭТЭМ.

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

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

Подсекция 21.2. Философские проблемы инженерно-технического знания. Председатель подсекции – Московченко Александр Дмитриевич, зав. каф. философии, д.ф.н., профессор; зам. председателя – Раитина Маргарита Юрьевна, к.ф.н., доцент каф. философии.

Подсекция 21.3. Социально-философские проблемы современности. Председатель подсекции – Суслова Татьяна Ивановна, декан ГФ., зав. каф. КС, д.ф.н., профессор; зам. председателя – Захарова Лилия Леонидовна, доцент каф. КС, к.ф.н.

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

Секция 23. Автоматизация управления в технике и образовании. Председатель секции – Дмитриев Вячеслав Михайлович, зав. каф. ТОЭ, д.т.н., профессор; зам. председателя – Андреев Михаил Иванович, к.т.н., доцент ВКИЭМ.

Секция 24. Проектная деятельность школьников в сфере информационно-коммуникационных технологий. Председатель секции – Татьяна

Борисовна Корнеева, заместитель директора по методической работе ОЦ «Школьный университет»; зам. председателя – Нехорошева Юлия Геннадьевна, начальник учебно-методичес-кого отдела ОЦ «Школьный университет».

Секция 25. Системы и сети электро- и радиосвязи. Председатель секции – Пуговкин Алексей Викторович, зав. каф. ТОР, д.т.н., профессор; зам. председателя – Демидов Анатолий Яковлевич, к.т.н., доцент каф. ТОР.

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

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

Материалы научных докладов,

предоставленные на конференцию, опубликованы в сборнике

«НАУЧНАЯ СЕССИЯ ТУСУР – 2010»

в пяти частях

1-я часть сборника включает доклады 1–7 секций;

2-я часть – доклады 8, 9, 10, 12-й секций;

3-я часть – доклады 11, 14-й секций;

4-я часть – доклады 13, 15, 16 и 20-й секций;

5-я часть – доклады 17–19, 21–26-й секций.

СЕКЦИЯ 11

АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

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

СОГЛАСОВАНИЕ РАЗНОТИПНЫХ ШКАЛ

Р.Ф. Акчурин, студент 4-го курса
г. Томск, ТУСУР, каф. КИБЭВС, nurka12@rambler.ru

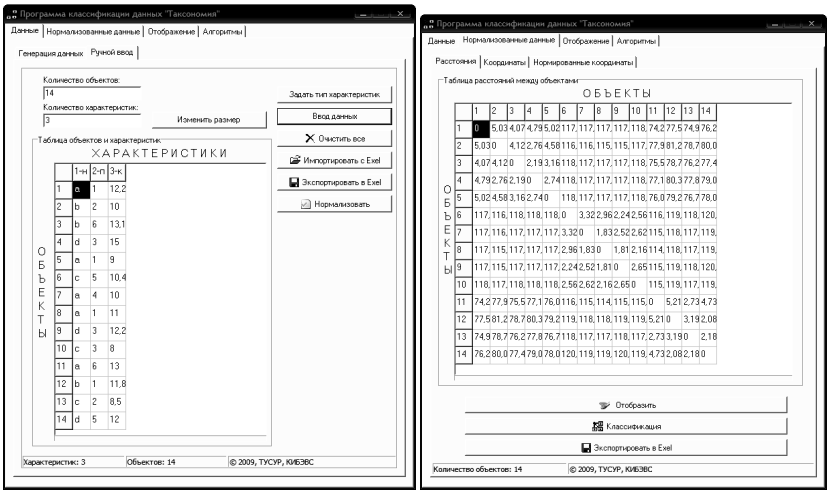
В настоящее время с развитием вычислительной техники возросла потребность обрабатывать большие объемы информации. Возросшие вычислительные мощности дали толчок развитию многим прикладным разделам математической теории, а современное программное обеспечение позволило эффективно реализовать трудоемкие вычислительные алгоритмы. Таким образом, средства вычислительной техники во многом помогают при анализе данных, основные действия которого – это разного рода сравнения.

Но, как правило, при обработке каких-либо данных (зачастую статистических) возникают проблемы их сравнения. Количественные меры сравнения похожести (корреляция) или различия (расстояние) считаются привычными для применения в обработке количественных данных. Однако при обработке статистических, экспериментальных и других данных встречаются не только данные количественного типа. Таким образом, все данные, которые могут обрабатываться, можно разделить на измеряемые в номинальных, количественных шкалах или шкалах порядка. Проблемами корректности преобразований значений, полученных путем измерений в шкалах различных типов, занимается теория измерений [1].

Зачастую обрабатываемые данные измеряются в различных шкалах, поэтому возникает проблема их согласования для последующего анализа, да и определение меры различия данных, определенных только в номинальной шкале, довольно затруднительно. Так, например, в рамках курсового проекта «Система классификации данных «Таксономия» потребовалось реализовать алгоритмы согласования объектов, характеристики которых определены в разнотипных шкалах, их оциф-

ровку и нахождение расстояния (меры различия) между обрабатываемыми объектами.

На вход подсистемы подаются данные в виде матрицы данных, которая содержит информацию об однотипных объектах, имеющих несколько характеристик (однотипных либо разнотипных), измеренных в одной из трех шкал: количественной, порядковой либо номинальной. После приема матрицы данных подсистема определяет шкалы, в которых измерены характеристики объектов, и в зависимости от полученных результатов начинает согласовывать характеристики и вычислять количественные меры различия между обрабатываемыми объектами для последующего их анализа. На рисунке представлен пример работы реализованной подсистемы, входящей в состав программы классификации данных.



Пример работы подсистемы согласования

В программе обрабатывается и было реализовано семь возможных вариантов:

– объекты имеют характеристики, измеренные только в номинальных шкалах;

– объекты имеют характеристики, измеренные только в количественных шкалах;

– объекты имеют характеристики, измеренные только в шкалах порядка;

– объекты имеют характеристики, измеренные в номинальных шкалах и шкалах порядка;

– объекты имеют характеристики, измеренные в количественных шкалах и шкалах порядка;

– объекты имеют характеристики, измеренные в количественных и номинальных шкалах;

– объекты имеют характеристики, измеренные в количественных, номинальных шкалах и шкалах порядка.

На выходе подсистема выдает матрицу данных, содержащих информацию о мере расстояний между объектами, подаваемых на вход подсистемы, имеющих несколько характеристик (измеренных в одинаковых либо различных шкалах).

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Пфанцагль И. Теория измерений. М.: Мир, 1976. 165 с.

ПЕРВИЧНАЯ ДЕКОМПОЗИЦИЯ РЕСУРСОВ И ЗАДАЧ САПР МОДЕЛИРОВАНИЯ АКТИВНЫХ ПРИБОРОВ НАНОЭЛЕКТРОНИКИ

А.Б. Андронов, С.О. Бургашвили, студенты 4-го курса;
Д.Д. Зыков, Л.А. Торгонский, доценты
г. Томск, ТУСУР, каф. КИБЭВС, 56000@sibmail.com

Совершенствование технологического оборудования микроэлектроники последней трети XX в. обеспечило выход на размеры элементов конструкций активных приборов нанометрового диапазона (10–100 нМ). При таких размерах возникает фундаментальный физический барьер [1, 2], за которым нарушается адекватность соответствия теоретических моделей переноса зарядов в микроэлектронных активных приборах наноэлектронным приборам. Потребовался расширенный учёт квантово-механических эффектов для объяснения новых явлений управляемой электропроводности в структурах приборов (с габаритными размерами хотя бы по одному измерению менее 20–100 нМ). Поведение носителей заряда в структурах наноэлектронных приборов представлено совокупностью фундаментальных явлений, определённых понятиями «квантовое ограничение», «баллистический перенос», «квантовая интерференция» и «туннелирование» [1, 2]. Теоретические прогнозы и экспериментальные исследования этих явлений позволили выйти на производственные реализации новых активных наноэлектронных приборов с уникальными параметрами быстродейст-

вия, габаритов и энергопотребления. Работа этих приборов основана на концепции переноса заряда *n*-мерным электронным газом (1-, 2-, 3-deg – dimension electrons gas) с низким уровнем энергетического рассеяния и высокой подвижностью. Структуры приборов, основанных на этой концепции, принято называть [2] HEMT-структурами (high electron mobility train). По производственным технологиям в настоящее время реализуются транзисторы со структурами pHEMT, mHEMT для сверхвысокочастотного диапазона (СВЧ) и быстродействующие цифровые комплементарные вентили на их основе. Пример варианта такой технологической структуры приведен на рис. 1.

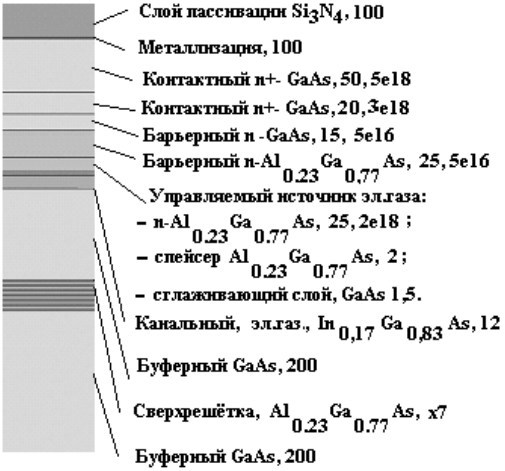


Рис. 1. Пример состава HEMT-структуры

На рис. 1 в обозначении слоя последовательно перечислены назначение, тип материала слоя, толщина слоя в нанометрах, уровень легирования (если легирование слоя применено). Соответственно толщины слоёв (и плоскостные размеры конструкции приборов) являются технологически уникальными, а контактирующие материалы структуры разнородны (гетероструктурны). В приборах преимущественно применяются гетероструктуры с согласованием атомных решёток контактирующих материалов. К настоящему времени исследованы перспективные технологические гетероструктуры Si-Ge, Si-C, AlxGa1-xAs-GaAs и др. Несогласованность свойств материалов контактных пар как фактор образования механических анизотропных деформаций (стрессов) дополнительно создает проблемы в конструкциях приборов наноэлектроники (изменение электрофизических свойств слоев, коробление пла-

стин, повышение доли брака изделий в производстве). В других условиях механические стрессы могут применяться как составные части процесса производства при создании одно- и двумерных нанообразований (наноплёнок, нанотрубок, наноспиралей) [1] .

Время и цена ошибок проектирования конструкций, цена потерь от производственного брака изделий актуализировали разработку и применение приборно-технологических САПР (TCAD). Одним из ведущих мировых лидеров в области создания приборно-технологических САПР (TCAD) является компания Synopsys. Семейство инструментов Sentaurus TCAD от компании Synopsys характеризуется [3], как динамично развивающееся семейство инструментов проектирования с периодом обновления 9 месяцев. Задачей Sentaurus TCAD является обеспечение разработчиков средствами приборно-технологического проектирования и интеграции этих средств, маршрут проектирования САПР больших микросхем. Важно, что ресурсы Sentaurus TCAD, во-первых рассчитаны на сквозное проектирование с согласованными форматами данных импорта и экспорта между подсистемами, а во-вторых, рассчитаны для работы с современными и перспективными сложными материалами (гетероструктурами Si-Ge, Si-C, AlxGa1-xAs-GaAs на Si, GaAs и др.). Ресурсы Sentaurus TCAD поддерживают моделирование и проектирование широкого класса активных приборов и моделирование их производства. Особый интерес в этом смысле представляют технологические HEMT-структуры и приборы для СВЧ микросхем, а ресурсы Sentaurus TCAD – для подготовки и переподготовки кадров для промышленных производств в этой сфере. С этой целью в рамках образовательной программы профессиональной переподготовки специалистов планируется установка продукта Sentaurus TCAD от компании Synopsys для постановки учебных классах университета. В отсутствие таких классов ведётся освоение и согласование материалов по объектам подготовки специалистов.

Анализ рекламных материалов компании Synopsys, обзорных материалов её представителей в России [3], как источник первичной информации для подготовки к работе с САПР Sentaurus TCAD, является целью предлагаемой статьи. Для грамотного использования и освоения ресурсов Sentaurus TCAD её пользователь должен иметь (или получить к её использованию) знания по следующим разделам:

– технологические процессы и сведения о производственном оборудовании;

– структурный состав приборов и параметры структур как продукта производства;

– качественная связь между формами и размерами плоских и объёмных конструкций приборов и их электрическими параметрами;

– понимание роли конструктивных и технологических факторов в проектировании приборов для отражения в электрических схемах замещения прибора.

Разнообразие вопросов и задач, стоящих за названными направлениями знаний, с одной стороны, не является исчерпывающим. С другой стороны, уже в этом составе им соответствует необходимость понимания пользователями общих вопросов физики работы приборов и роли физических связей в приборах и владения специальными технологическими, конструкторскими, схемотехническими знаниями и навыками. На эти знания и навыки опираются инструменты САПР Sentaurus TCAD по приведенному ниже перечню [3]:

– Sentaurus Workbench (графический интерфейс открытия и управления проектом);

– Ligament (графический интерфейс моделирования техпроцессов);

– Sentaurus Process (интерфейс технологического моделирования и настройки проекта в 1D, 2D и 3D);

– Sentaurus Structure Editor (интерактивный графический интерфейс технологического моделирования структур);

– Mesh and Noffset3D (формирование сеток для моделирования процессов);

– Sentaurus Device (инструмент 1D, 2D и 3D приборного моделирования, с инструментами для создания сеток) (инструменты Sentaurus Mesh и Noffset3D);

– Inspect and Tecplot (просмотр образов проектов);

– PCM Studio (анализ производственого цикла).

На рис. 2 приведен примерный маршрут организации процессов проектирования в Sentaurus TCAD. В поз. *1–6* на рис. 2 показаны отдельные продукты TCAD окнами настройки управления (поз. *1*, *3*) и примеры формы отображения результатов (поз. *2*, *4–6*).

Интерес представляют сведения, актуальные для описания наноструктурных конструкций и технологии полевых СВЧ-транзисторов монолитных интегральных микросхем (МИМ) для рабочих частот гигагерцового диапазона в Sentaurus TCAD. Наноразмерными в приборах этих МИМ являются технологические слои HEMT-структуры, структуры затвора и, возможно, длины затвора и канала канала транзисторов. Для прочих пассивных элементов МИМ плоскостные размеры определяются классическими соотношениями, применяемыми в проектировании СВЧ-конструкций, а их наноразмерность не актуализируется.

Трехмерная конструкция полевого HEMT-транзистора показана на рис. 3.

Для полевых транзисторов проектными функциональными параметрами являются:

– электрическая прочность затвора (или рабочие напряжения изоляции);

– пороговые напряжения (напряжения отсечки тока стока) транзистора;

– ток насыщения транзистора;

– крутизна ВАХ;

– сопротивления и емкости схемы замещения;

– электродные емкости прибора;

– токи утечки электродов.

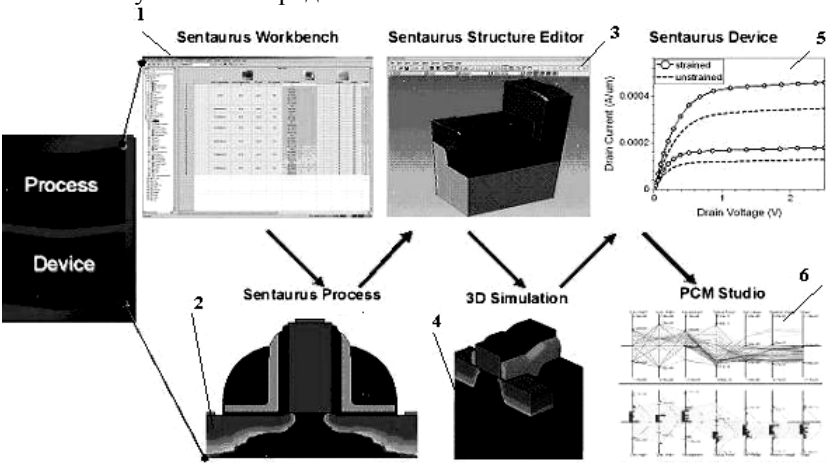


Рис. 2. Маршрут организации процессов проектирования в Sentaurus TCAD

Названные параметры являются выходными для контроля результатов обработки в инструментах Sentaurus Structure Editor, Sentaurus Device при наложении сеток для моделирования инструментами Mesh and Noffset3D.

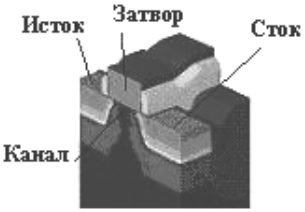


Рис. 3. Часть трёхмерной конструкции полевого HEMT-транзистора

Для интерактивного определения подлежат вводу тип материала слоя, толщина слоя, концентрации легирующих примесей, справочные физические константы (диэлектрические проницаемости, критические напряжённости, постоянные решёток, собственные концентрации и прочие атрибуты, которые целесообразно было бы определять связанными таблицами в составе библиотек САПР). Эти параметры имеют

отношение к формированию слойного состава ресурсами Sentaurus Workbench, Ligament, Sentaurus Process. Ресурсы Inspect для Sentaurus Structure Editor и Tecplot для Sentaurus Device позволяют визуализировать 2D- и 3D-структуры в графику электрических характеристик и потоков.

На выходе САПР, наряду со значениями функциональных параметров прибора, формируются сопоставимые сочетания применённых слоёв, их геометрические характеристики (толщины, формы, площади). По задаваемому производительному ресурсу технологического оборудования и последовательности включения его в производственный маршрут на выходе САПР может быть выдана одна из форм карты (формата вывода) процессов и параметров режимов и переходов технологического оборудования. Ввиду специфики задач организации производственного цикла такие задачи относят к самостоятельной производственной САПР с соответствующим форматом входных и выходных данных.

Важным критерием эффективности функционирования производственного комплекса является показатель выхода годных изделий и на промежуточных этапах, и на выходе производственного цикла. Ослабление влияния параметрических отклонений на появление брака достигается выбором проектных решений, обеспечивающих пониженную чувствительность функциональных параметров к изменению определяющих их факторов технологических процессов. Прямое решение задачи снижения процента брака, если его причинами и источниками не являются очевидные ошибки, – сложная многопараметрическая задача. Снижение угрозы выхода за пределы допустимых значений облегчается доступом через ресурсы PCM Studio САПР к информации о формах и диапазонах рассеяния функциональных параметров изделия. Факторами их отклонений могут быть рассеяния по толщине, ширине, длине слоёв, совмещению слоёв, рассеяние концентраций, рассеяние по температуре, по времени и т.д.

Применение ресурсов TCAD позволяет накапливать, применять, модифицировать отработанные решения и сокращать время их подготовки.

ЛИТЕРАТУРА

1. Борисенко В.Е., Воробьёва А.И., Уткина Е.А. Наноэлектроника. М.: Бином; Лаборатория знаний, 2009. 223 с.

2. Драгунов В.П., Неизвестный Н.Г., Гридчихин В.А. Основы наноэлектроники: Учеб. пособие. М.: Университетская книга; Логос; Физматкнига, 2006.496 с.

3. Радченко Д., Сбитнев К., Моделирование СВЧ-транзистора на основе эпитаксиальной гетероструктуры (HEMT) с помощью САПР Synopsys Sentaurus TCAD, СПб ФТНОЦ РАН // Производство электроники: технологии, оборудование, материалы. 2009. №7.

МЕТОДЫ И СРЕДСТВА ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ*

А.С. Бирюков, В.Е. Долгушин, студенты 3-го курса;
М.А. Сопов, науч. рук., ассистент
г. Томск, ТУСУР, каф. КИБЭВС, birarser@sibmail.com, kaka@bk.tomsk.ru

Для эффективного управления бизнесом в сфере электронной коммерции в настоящее время большое распространение получают методы бизнес-аналитики (BI – Business Intelligence) [6]. В сферу их применения входят задачи по прогнозированию объемов продаж, управлению количеством товарных запасов, определению оптимальных торговых наценок, выявлению типичных паттернов покупательского поведения, оптимизации навигации по сайту, улучшению рубрикации и т.п. [1].

Для анализа данных используются средства многомерного хранения и аналитической обработки данных (OLAP – Online Analytical Processing), представляющие бизнес-операции в виде фактов (объем продаж, число единиц на складе и т.д.) и измерений (время, география, поставщик, покупатель, товар и т.д.). Средства OLAP позволяют осуществлять стратегический обзор ситуации и в реальном времени получать ответы на вопросы, интересующие аналитика. Средства OLAP в основном предназначены для быстрого составления отчетности по консолидированным показателям процессов в различных разрезах и с произвольной глубиной «проваливания» в оперативные данные. Средства OLAP также идеально подходят для проверок заранее сформулированных аналитиком гипотез [3].

С целью автоматического обнаружения ранее неизвестных знаний в накопленных данных используются технологии интеллектуального анализа данных, называемые также «раскопкой данных» (Data Mining), «обнаружением знаний в базах данных» (Knowledge Discovery in Databases).

Data Mining – это процесс обнаружения в сырых данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности.

В отличие от технологии OLAP сам поиск закономерностей и шаблонов в данных осуществляется не пользователем системы, а самой технологией, реализующей несколько алгоритмов Data Mining (DM) [4, 5].

* Выполнено в рамках проекта ГПО КИБЭВС-0902 – Инженерия баз данных.

В список основных задач, решаемых алгоритмами DM, входят:

1) сегментация (выявление структуры, групп, кластеров);

2) поиск ассоциаций (связей между различными характеристиками);

3) поиск временных шаблонов;

4) регрессия (прогнозирование, классификация, восстановление функциональной зависимости между характеристиками).

Методы и средства интеллектуального анализа данных (ИАД)

Технологии интеллектуального анализа данных позволяют решать множество задач с привлечением методов математической статистики и теории вероятности, а также методов искусственного интеллекта.

1. Методы статистической обработки данных.

1.1. Предварительный анализ природы статистических данных (проверка гипотез стационарности, нормальности, независимости, однородности, оценка вида функции распределения и ее параметров).

1.2. Выявление связей и закономерностей (линейный и нелинейный регрессионный, корреляционный анализы).

1.3. Многомерный статистический анализ (линейный и нелинейный дискриминантный анализ, кластер-анализ, компонентный анализ, факторный анализ).

1.4. Динамические модели и прогноз на основе временных рядов.

2. Кибернетические методы.

2.1. Методы нейронных сетей. Формируются путем построения иерархической сети, узлами которой являются модели нервных клеток (нейронов), у которых выходной сигнал определяется взвешенной суммой входных сигналов. В свою очередь, входные сигналы представляют собой выходные сигналы нейронов предыдущего уровня. Входными сигналами всей сети являются параметры текущих рядов наблюдений. Основным недостатком является необходимость иметь очень большой объем обучающей выборки.

2.2. *Эволюционное программирование.* Получение оптимального решения путем имитации процесса эволюции популяции; вносятся различные, случайные изменения; совокупность решений образует новое поколение возможных решений, которое подвергается «естественному отбору», основанному на «критерии выживания».

2.3. *Генетические алгоритмы.* Аналогично эволюционному также происходит генерация, отбор и селекция возможных решений; помимо случайных изменений генной структуры происходит и направленная модификация, позволяя получать новые результаты решения.

- *Алгоритмы ограниченного перебора.* Вычисляют частоты комбинаций простых логических событий в подгруппах данных. Ограничением служит длина комбинации простых логических событий. На основании анализа вычисленных частот делается заключение о полез-

ности той или иной комбинации для установления ассоциации в данных, для классификации, прогнозирования и пр.

- *Логические методы* распознавания позволяют выявлять логические закономерности в данных и использовать их при прогнозировании, но при наличии линейных зависимостей между признаками и прогнозируемой величиной точность прогноза, сделанного «линейной машиной», может быть заметно выше.

Проведение условной классификации по методам и анализ средств ИАД позволили сделать следующие заключения. Несмотря на обилие методов ИАД, приоритет в эффективных современных разработках смещается в сторону использования логических (дедуктивных и индуктивных) моделей представления знаний. С их помощью решаются задачи прогнозирования, классификации, распознавания образов, извлечения из данных «скрытых» знаний, интерпретации данных, установления ассоциаций в БД. Результаты таких алгоритмов эффективны и легко интерпретируются. Однако известные методы поиска логических правил не поддерживают функцию обобщения найденных правил и функцию поиска оптимальной композиции таких правил. Решением перечисленных проблем можно добиться новых, более успешных результатов в области разработок ИАД.

ЛИТЕРАТУРА

1. Кейс: Применение методов интеллектуального анализа данных (Data Mining) в интернет-торговле, http://www.spellabs.ru/

2. Когаловский В. Происхождение ERP // Журнал «Директору информационной службы» #05/2000,www.interface.ru,12/03

3. Киселева М., Соломатина Е. Средства добычи знаний в бизнесе и финансах // Открытые системы. 1997. № 4.

4. Основные проблемы ERP-систем // Журнал JetInfo №2(105)/2002, www.jetinfo/2002/2/1/article1.2.2002.html, 03/04

5. Программы планирования ресурсов (ERP) необходимы, но недостаточны:. Март 2000, http://www.bizcom.ru,01/04

6. Федоров А., Елманова Н. Введение в базы данных: средства Business Intelligence // КомпьютерПресс 3'2001, http://www.olap.ru, 02/03

7. Мусаев А. Интеллектуальный анализ данных: Клондайк или Вавилон? // Банковские технологии. 1998. №11–12.

РЕАЛИЗАЦИЯ ОСНОВЫ ПОДСИСТЕМЫ АНАЛИЗА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПОИСКА, АНАЛИЗА И ПРИНЯТИЯ РЕШЕНИЙ В СЕТИ ИНТЕРНЕТ (ПУАРО)*

А.С. Бондаренко, студент 5-го курса;
А.В. Ефремкин, Р.Р. Вильданов, студенты 4-го курса
г. Томск, ТУСУР, каф. КИБЭВС, boalse@yandex.ru

На Научной сессии ТУСУР–2009 был представлен доклад [1, с. 29], описывающий концептуальную модель автоматизированной системы поиска, анализа и принятия решений в сети Интернет (ПУАРО). В продолжение темы в данной статье будут рассмотрены алгоритмы, уже реализованные в описанной системе.

Сначала необходимо по запросу пользователя загрузить html-страницы, выданные поисковой системой и поместить их в хранилище на жесткий диск. После загрузки страниц их нужно очистить от html-тегов, чтобы упростить анализ. Задача очистки от тегов решается в системе при помощи алгоритма, находящего пары символов «<» и «>», следующих друг за другом и удаляющих содержание между ними (рис. 1).

После очистки от html-тегов текст анализируется методом Зипфа. Данный алгоритм выделяет все слова, находящиеся в тексте, и ранжирует их по количеству встречаемости (ось абсцисс на рис. 2).

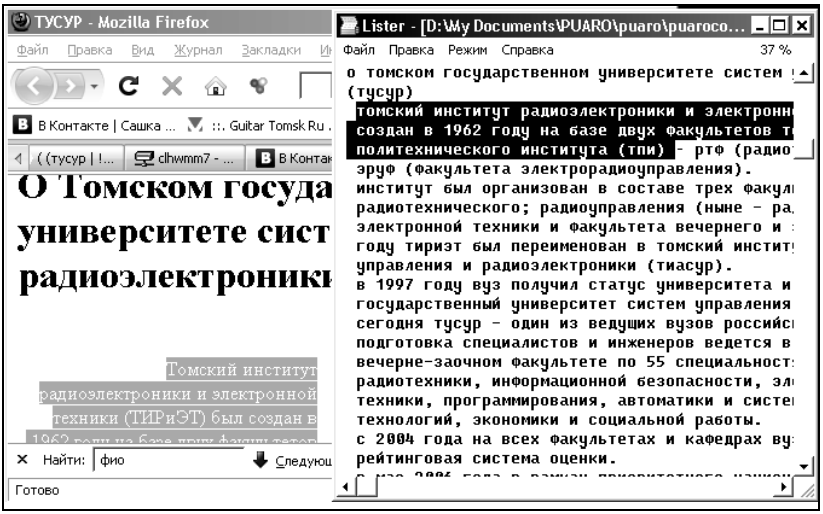


Рис. 1. Результат работы алгоритма по очистке текста от html-тегов

* Выполнено в рамках проекта ГПО КИБЭВС-0701 – Автоматизированная система поиска, анализа и принятия решений «ПУАРО».

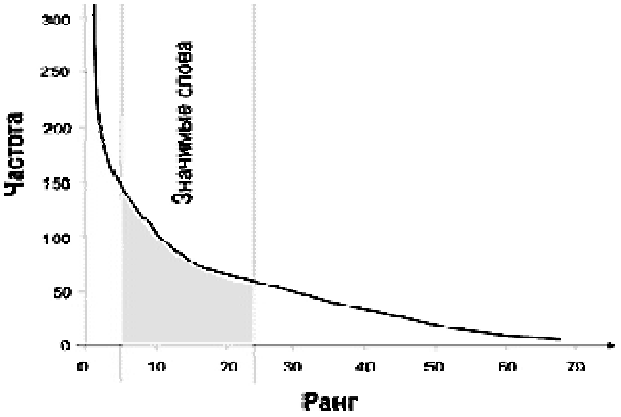


Рис. 2. Значимые слова, выделяемые алгоритмом Зипфа

После ранжирования отсеиваются все слова, встречающиеся чаще некоторого заданного порогового значения K1, а также слова, встречающиеся реже некоторого заданного порогового значения K2, в результате остаются только значимые слова (рис. 3). Пороговые коэффициенты K1 и K2 определяются опытным путём.

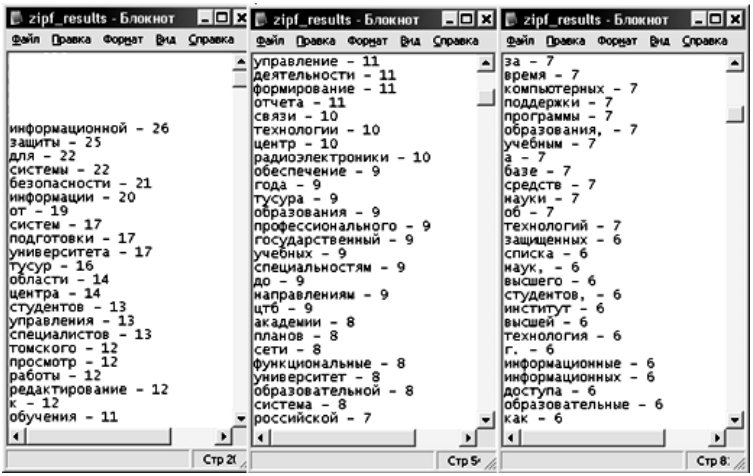


Рис. 3. Значимые слова, выделяемые алгоритмом Зипфа по запросу «ТУСУР»

Рассмотренные в статье алгоритмы являются фундаментальными для дальнейшего развития системы по заданной ранее концепции, их реализация позволит внедрить в систему алгоритмы анализа и принятия решений более высокого уровня.

Научный руководитель – А.А. Шелупанов, д.т.н., профессор, зав. кафедрой КИБЭВС, проректор по научной работе ТУСУР.

ЛИТЕРАТУРА

1. Научная сессия ТУСУР-2009: Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых, 12–15 мая 2009 г.: В 5 ч. Ч. 3. Тематический выпуск «Системная интеграция и безопасность». Томск: В-Спектр, 2009. 392 с.

ОЦЕНИВАНИЕ НЕИЗВЕСТНЫХ ПАРАМЕТРОВ ОБЪЕКТОВ ПУТЕМ СОВМЕСТНОГО ПРИМЕНЕНИЯ РЕКУРРЕНТНОГО МНК И АЛГОРИТМА КУМУЛЯТИВНЫХ СУММ

А.В. Димаки, к.т.н., доцент; А.А. Светлаков, д.т.н., профессор
г. Томск, ТУСУР, каф. ЭСАУ,dav18@yandex.ru

Многие объекты и процессы, встречающиеся в современной технике, являются нестационарными в том смысле, что все или часть их параметров может скачкообразно изменяться со временем. Примерами подобных нестационарных объектов являются двигатели, работающие с переменной нагрузкой, трубопроводы, запорные элементы которых скачкообразно изменяют свое положение, и т.д. При решении задачи параметрической идентификации таких объектов возникает ряд проблем, связанных с необходимостью обнаружения моментов скачкообразного изменения или «переключения» их параметров [1].

В настоящее время в системах управления, работающих в реальном времени, широкое распространение получили алгоритмы идентификации, относящиеся к классу рекуррентных [2]. Такие алгоритмы позволяют, в частности, уточнять оценки неизвестных параметров объекта по мере поступления новых значений его выходов. Однако применительно к нестационарным объектам такие алгоритмы демонстрируют значительное запаздывание при подстройке получаемых модельных оценок по отношению к скачкообразному изменению параметров объекта. В связи с этим представляет интерес разработка новых методик и алгоритмов для уменьшения «времени реакции» идентификаторов на упомянутые «скачки».

Рассмотрим объект с одним выходом Y, принимающим в момент времени t_i значение y_i, и предположим, что зависимость $y(t)$ описывается алгебраическим полиномом второго порядка, неизвестные нам коэффициенты a^k которого могут к тому же скачкообразно изменяться в произвольный момент времени. Для получения оценок $\tilde{a}_i^k$ по периоди-

чески поступающим значениям выхода естественно применить рекуррентный метод наименьших квадратов (РМНК) [3].

Алгоритм решения данной задачи на i-м шаге по времени записывается следующим образом:

$$\begin{aligned}
&\mathbf{u}_i^T = (1; t_i; t_i^2), \;\; q_i = \mathbf{u}_i^T \mathbf{P}_{i-1} \mathbf{u}_i + 1, \\
&\mathbf{P}_i = \mathbf{P}_{i-1} - \mathbf{P}_{i-1} \mathbf{u}_i (1/q_i) \mathbf{u}_i^T \mathbf{P}_{i-1}, \\
&\mathbf{a}_i = \mathbf{a}_{i-1} + \mathbf{P}_i \mathbf{u}_i \left(y_i - \mathbf{u}_i^T \mathbf{a}_{i-1} \right).
\end{aligned} \tag{1}$$

При этом предполагается, что в начальный момент времени

$$\tilde{\mathbf{a}}_i = \mathbf{0}, \quad \mathbf{P} = \gamma \mathbf{E}, \gamma >> 1. \tag{2}$$

Как показали результаты тестирования алгоритма (1), при скачкообразном изменении параметров идентифицируемого объекта требуется значительное время для подстройки оценок $\tilde{\mathbf{a}}_i$ под новые значения параметров объекта.

Для уменьшения «времени реакции» РМНК применим известный алгоритм, называемый методом кумулятивных сумм [4], сущность которого заключается в следующем. Определим кумулятивную сумму $S_j^i(\nu)$ следующим образом:

$$S_j^i(\nu) = \sum_{k=j}^{i} \left(y_k - \mathbf{u}_k^T \mathbf{a}_k \right), \tag{3}$$

где индекс j соответствует моменту времени t_j, в который произошло предыдущее переключение параметров объекта. Момент времени t_i, такой, что

$$\left| S_j^i \right| > \lambda, \tag{4}$$

где λ – некоторое пороговое значение, считается моментом переключения параметров объекта. Значения вектора оценок параметров $\tilde{\mathbf{a}}_i$ и весовой матрицы $\mathbf{P}$ устанавливаются согласно (2).

На рис. 1 показаны результаты работы описанного выше алгоритма на модельном примере. Выход объекта описывался квадратичной функцией вида

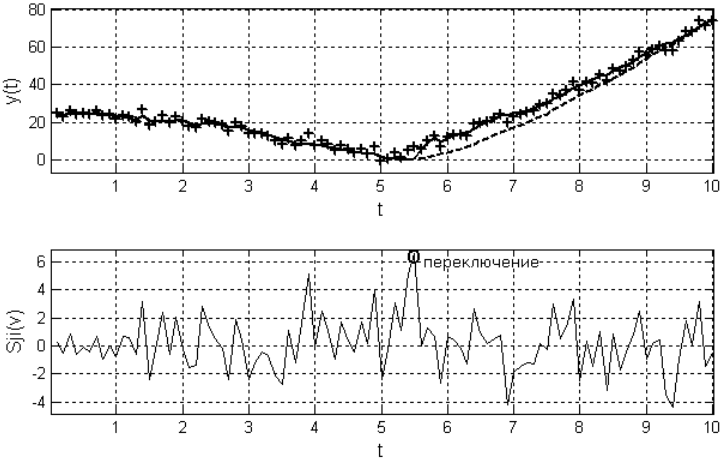
$$y(t) = \begin{cases} 25 - t^2 + \varepsilon(t), & t \le 5, \\ t^2 - 25 + \varepsilon(t), & t > 5. \end{cases} \tag{5}$$

где $\varepsilon(t)$ – нормально распределенный шум измерений выхода объекта.

Сплошной линией показана аппроксимирующая зависимость, полученная с помощью метода кумулятивных сумм, крестиками показаны значения функции $y(t)$, имитирующей зашумленный выход объекта,

штриховой линией показана аппроксимирующая зависимость, полученная без использования метода кумулятивных сумм.

Как видно из рисунка, применение метода кумулятивных сумм для отслеживания моментов «переключений» параметров объекта позволяет значительно снизить время подстройки их оценок.



Пример работы алгоритма оценки параметров объекта (кружком показано обнаруженное «переключение» параметров)

Остается открытым вопрос об оптимальном значении порога λ. В настоящем алгоритме данное значение было принято равным $\lambda = 3\sigma$, где σ – с.к.о. шума измерений, что позволило добиться достаточно точного обнаружения момента переключения без ложных срабатываний алгоритма.

Работа выполнена при финансовой поддержке проекта №2249 в рамках Аналитической ведомственной целевой программы «Развитие научного потенциала высшей школы (2009–2010 г.)»

ЛИТЕРАТУРА

1. Основы управления технологическими процессами // Под ред. Н.С. Райбмана. М.: Наука, 1978. 440 с.

2. Рубан А.И. Идентификация нелинейных динамических объектов на основе алгоритма чувствительности. Томск: Изд-во ТГУ, 1975. 272 с.

3. Льюнг Л. Идентификация систем. Теория для пользователя. М.: Наука, 1991. 432 с.

4. Обнаружение изменения свойств сигналов и динамических систем: Пер. с англ. М. Бассвиль, А. Вилски, А. Банвенист и др.; под ред. М. Бассвиль, А. Банвениста. М.: Мир, 1989. 278 с.

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ПОДСИСТЕМ МОДЕЛИРОВАНИЯ В АСУ ТП ПОДГОТОВКИ НЕФТИ

Т.В. Ганджа, Н.А. Гиркин, ОАО «Сургутнефтегаз»
г. Томск, ТУСУР, nikitagirkin@mail.ru

В данном статье дается оценка перспектив внедрения подсистемы моделирования в АСУ ТП подготовки нефти и газа. Рассматривается моделирование технологических процессов транспортировки нефти, сепарации нефти от попутного газа, воды и солей, закачки воды для поддержания пластового давления. Под объектами автоматизации рассматриваются нефтесборные коллекторы от кустов скважин до площадок сепарации, дожимные насосные станции (ДНС), установки предварительного сброса воды (УПСВ), кустовые насосные станции (КНС) и высоконапорные водоводы системы поддержания пластового давления (ППД).

В качестве официальных исходных данных рассмотрим перечень основных научно-технических проблем ОАО «Сургутнефтегаз» на 2009–2010 гг., объявленных перед 30 научно-технической конференцией молодых специалистов компании. Из всего перечня можно выделить ряд проблем, решение которых, по нашему мнению, может быть найдено с помощью системы моделирования технологических процессов:

1) Контроль состояния и обнаружение утечек на нефтепроводах.

2) Образование устойчивых солеотложений на внутренних стенках высоконапорных водоводов системы ППД.

3) Определение начала отложения гидратов в газопроводах.

4) Образование стойких нефтяных эмульсий.

5) Необходимость уменьшения содержания нефтепродуктов в подтоварной воде после очистных сооружений на ДНС с УПСВ.

6) Перегрев и деформация жаровых труб аппаратов УПСВ вследствие твердых отложений в межтрубном пространстве.

7) Необходимость понижения температуры помутнения и застывания дизтоплива с установки получения битума.

К перечню научно-технических проблем можно добавить некоторые производственные проблемы подготовки нефти:

8) Отказы измерительных датчиков и исполнительных устройств.

9) Засорение, отложение парафина и замерзание трубопроводов.

10) Отключение электропитания объектов подготовки.

11) Потребность обучения оперативного персонала имитацией действий в различных технологических режимах и авариях.

12) Нестабильность качества отделения солей от нефти.

13) Отсутствие точной настройки контуров автоматического регулирования, в том числе отсутствие связанных контуров.

14) Отсутствие ряда измерительных приборов (установка которых связана с высокими затратами) и т.д.

В перечисленном ряде проблем можно условно выделить группы, связанные с:

– транспортом нефти, газа и воды по трубопроводам (проблемы 1, 2, 3, 9);

– сепарацией нефти от газа, пластовой воды, солей (проблемы 4, 5, 6, 12);

– действиями оперативного персонала в аварийных ситуациях и сбоях технологического режима (проблемы 8, 10, 11);

– повышением качества технологического процесса (проблемы 7, 13, 14).

Рассмотрим, как внедрение системы моделирования технологического процесса может способствовать решению указанных проблем.

Работа с точной математической моделью может дать персоналу глубокое понимание технологического процесса. Предоставляется возможность имитации различных технологических режимов для обучения персонала, в том числе отработка действий в аварийных ситуациях. Для обучения персонала система моделирования должна обладать функциональностью расчета переходных процессов, работы в динамическом режиме, обмена данными с АСУ ТП объектов в реальном времени.

При известном химическом составе нефти и газа математическая модель достаточно точно описывает движение потока среды по трубопроводам в реальном времени, что может дать возможность при достаточном количестве датчиков давления диагностировать изменение объема среды (порыв), возрастание гидравлического сопротивления (засор, отложение парафина. замерзание), изменение потока тепловой энергии (нарушение теплоизоляции трубопроводов и аппаратов, потеря теплопроводности теплообменников). Система моделирования должна при этом обладать функциональностью выдачи предупредительных сигналов в действующую АСУ ТП на АРМ операторов.

Существующая избыточность измерительных датчиков на ДНС, УПСВ и КНС дает возможность использовать данную избыточность для автоматической настройки параметров модели. Такая система моделирования должна быть устойчивой к отказу нескольких измерительных датчиков и сама диагностировать данные отказы в реальном времени. Дополнительно модель может осуществлять расчет параметров, непосредственное измерение которых затруднено. К таким параметрам относится расход нефти и газа на входе ДНС, содержание соли в товарной нефти на выходе ДНС. Система моделирования должна при этом обладать функциональностью автоматической настройки параметров и анализа входных данных с измерительных устройств.

Математическая модель, рассчитывающая химические реакции, должна предсказать условия отложения гидратов и солей в трубопроводах и технологических установках. Математические модели смесителей, сепараторов и отстойников могут описать процесс разрушения стойких нефтяных эмульсий при подготовке товарной нефти и подтоварной воды, а также процесс вымывания солей из нефти. Математическая модель колонны должна описать процесс перегонки нефти и получения фракций с заданными характеристиками.

Функция расчета с кратным шагом во времени может дать возможность прогнозирования развития технологического процесса на заданную глубину при известных начальных условиях, в том числе прогноз развития технологического процесса при фиксированном положении клапанов регулирования, задвижек и насосов (ситуация отключения электропитания объектов подготовки).

К дополнительным полезным функции системы моделирования можно отнести функцию автоматической настройки контуров регулирования, в том числе связанных.

В данной статье были перечислены некоторые актуальные на текущий момент научно-технические и производственные проблемы сбора и подготовки нефти и газа, дана оценка перспектив внедрения подсистемы моделирования в действующие АСУ ТП для решения указанных проблем.

СРАВНЕНИЕ ERP-СИСТЕМ*

Т.В. Остапчук, Ю.В. Гирная, студенты 3-го курса;
М.А. Сопов, науч. рук., ассистент
г. Томск, ТУСУР, каф. КИБЭВС, littletanchik@mail.ru, zverushka05@sibmail.com

Каждой организации необходима динамичная стратегия для того, чтобы быть на высоте в сегодняшнем быстро меняющемся мире. Чтобы предоставить бизнесу оптимальную поддержку и обеспечить быструю реакцию на возникающие изменения, необходима мощная, гибкая и открытая инфраструктура информационных технологий (ИТ). Именно с ее формированием и связана Enterprise Resourse Planing System – система планирования ресурсов предприятия (ERP-система). Однако внедрение ERP-системы – очень сложный процесс, затрагивающий и перестраивающий всю структуру компании. Приняв решение о внедрении,

* Выполнено в рамках проекта ГПО КИБЭВС-0902 – Инженерия баз данных.

необходимо провести серьезный анализ существующих ERP-систем, понять, какая система наиболее полно удовлетворяет потребностям и целям предприятия.

ERP-системы классифицируют по многим признакам. Это и функциональные возможности, и стоимость внедрения проекта, и программно-аппаратные платформы, на которых реализована ERP. Кроме того, некоторые эксперты делают попытку классификации систем управления ресурсами предприятия по наличию/отсутствию у продукта отраслевого решения.

На российском рынке ERP-систем по данным за 2008 г. присутствует множество поставщиков: как иностранных, так и отечественных. По оценкам экспертов, львиную долю отечественного рынка (свыше 53%) занимает немецкий SAP, следом за ним идёт продукт отечественно поставщика 1С (около 19%). Затем практически наравне идут продукты Microsoft Business Solution и Oracle (каждая занимает чуть больше 8% российского рынка ERP-систем). Столь значительный отрыв SAP можно отчасти объяснить тем, что немецкий концерн первым вышел на российский рынок, открыв свое представительство еще в 1992 г. На мировом рынке ситуация несколько иная и основная борьба за лидерство разворачивается между SAP и Oracle (табл. 1).

Таблица 1

Основные иностранные ERP-системы, представленные на российском рынке по данным CNews Analytics [1]

Решение	Сфера применения	Срок внедрения	Стоимость внедрения
SAP R/3	Оборонные, нефтегазовые компании, металлургия, энергетика, телекоммуникации, банковский сектор	1–5 лет и более	Лицензия на 1 раб. место $7 тыс. Стоимость внедрения выше в 2–3 раза
Oracle Application	Тяжелая, химическая промышленность, телекоммуникации, финансовый сектор	1–5 лет и более	Лицензия на 1 раб. место $5 тыс. Стоимость внедрения выше в 2–3 раза
IFS Application	Машиностроение, энергетика, пищевая промышленность, фармацевтика	0,8–3 года и более	Полная стоимость внедрения может достигать $250 тыс.
Baan ERP	Автомобилестроение, химическая, пищевая промышленность, фармацевтика	6 мес–1,5 года и более	Лицензия 1 раб. место – $3 тыс. Стоимость внедрения выше 1–3 раза

Решения Oracle и SAP – мировые лидеры в сегменте систем управления предприятием. Продукты обоих поставщиков относятся к классу

крупных интегрированных систем и обладают широкой функциональностью, позволяющей удовлетворить потребности бизнеса практически в любой отрасли. Тем не менее высокая стоимость лицензий, консалтинговых услуг и поддержки решений Oracle и SAP нередко являются причиной предпочтения решений других поставщиков [1]. Также достаточно хорошо известна на российском рынке система – Baan ERP. Послужной список внедрений Baan в России весьма внушителен и охватывает самые разные сегменты – от машиностроения и нефтегазовой отрасли до пищевой промышленности (табл. 2).

Таблица 2

ERP-системы российского производства [1]

Решение	Сфера применения	Срок внедрения	Стоимость внедрения
«Галактика»	Нефтегазовая отрасль, машиностроение, химия, энергетика, металлургия и др.	4 мес. – 1,5 года и более	Лицензия 1 раб. место $350–1200. Стоимость внедрения 50–100% этой суммы
«Парус»	Машиностроение, нефтегазовые компании, энергетика	4 мес. – 1 год и более	Лицензия 1 раб. место $1–2 тыс. Стоимость внедрения 100–200% этой суммы
«1С: Предприятие 8.0»	Машиностроение, пищевая промышленность и др.	3–9 мес. и более	Лицензия 1 раб. место $150–600. Стоимость внедрения $200–1000

Отечественные решения являются в первую очередь учетными системами, регистрирующими осуществленные операции, возможности планирования в них представлены слабо. Существенным плюсом российских разработок является относительно невысокая стоимость.

Анализ доли ведущих поставщиков на рынке ERP-систем в России в период с 2003 по 2008 г., результаты работы приведены на рис. 2.

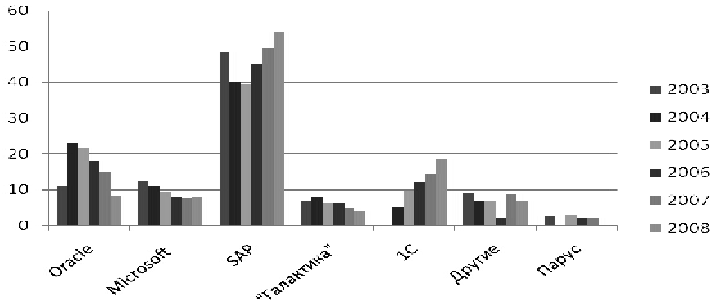


Рис. 2. Доли ведущих поставщиков на рынке ERP-систем в России в период 2003–2008 гг.

Из данного анализа можно сделать вывод, что ведущим поставщиком ERP-систем в России является компания SAP. Но также можно увидеть, что компания 1С в период 2003–2008 гг. в несколько раз увеличила свою долю на рынке ERP-систем в России и является ведущим отечественным производителем систем управления предприятием.

ЛИТЕРАТУРА

1. Игнатов С. Сравниваем ERP по ключевым характеристикам // Интернет-ресурс: www.cnews.ru
2. ERP в России и в Мире //Интернет-ресурс: erp-tools.ru
3. Рейтинги ERP-систем// Интернет-ресурс: www.erp-online.ru

УСТРОЙСТВО ОБУЧЕНИЯ ШРИФТУ БРАЙЛЯ*

И.Н. Глибчук, А.А. Терентьева, студенты 4-го курса;
Л.А. Торгонский, науч. рук., доцент
г. Томск, ТУСУР, каф. КИБЭВС, ejik-fast@sibmail.com

Знакомство авторов статьи с проблемами обучения слепых и слабовидящих людей [1] убедило их в актуальности содействия, по мере возможностей, этой категории людей в преодолении хотя бы части проблем их социализации. Статья посвящен описанию устройства для обучения шрифту Брайля [2]. Этот шрифт осязательного восприятия символов используется слепыми и слабовидящими людьми, как альтернативный традиционным алфавитам зрительного восприятия текстов.

В статье предлагается и рассматривается несложное, по меркам современного уровня развития микропроцессорной техники [3], функциональное устройство, предназначенное для применения в арсенале технических средств обучения слабовидящих людей шрифту Брайля. Реализованный в устройстве принцип обучения основывается на подтверждении осязательно воспринимаемого образа символа Брайля сигналом голосового сообщения, соответствующим принятому в человеческом сообществе языку. Устройство, структурная схема которого приведена на рис. 1, содержит модуль упорядоченно расположенных на лицевой панели клавиш с символами рельефного шрифта Брайля и специальными символами управления, модуль излучателя звукового сигнала и микроконтроллер, для которого, в отсутствие достаточной встроенной памяти, может потребоваться модуль внешней памяти для хранения эвуковых образов символов алфавита. Нажатие на клавишу с

* Выполнено в рамках проекта ГПО КИБЭВС-0901 – Тактильная панель ввода-вывода для слепых и слабовидящих людей.

опознаваемым в обучении символом сопровождается активизацией состояния бинарного датчика, связанного с клавишей. Микроконтроллер в составе приведенной структуры устройства предназначен для управления опросом, опознанием активизированных датчиков модуля клавиш и управления операциями отработки со звуковым сопровождением.

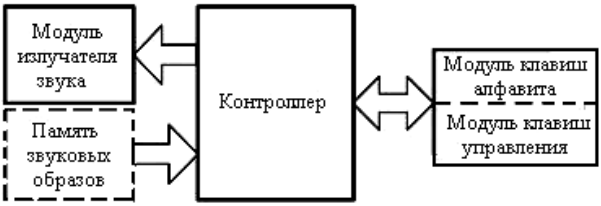


Рис. 1. Структурная схема устройства

На устройстве могут быть реализованы разные сценарии обучения алфавиту Брайля (и не только), но эти вопросы выходят за пределы материала статьи.

Устройство проектируется в виде автономного прибора с питанием от двух сухих батарей габарита AAA-1,5V. Внешний вид прибора показан на рис. 2. Проектные размеры прибора равны 90×60×15 мм.

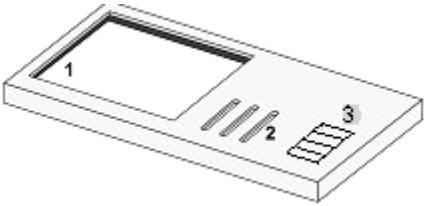


Рис. 2. Внешний вид прибора.
1 – поле клавиш алфавита;
2 – зона излучателя звука;
3 – поле переключателей управления

Компоновочная схема прибора приведена на рис. 3. Печатная плата *6* является несущей частью конструкции прибора. На ней в поле *1* установлены 40 двухполюсных микропереключателей (5 строк по 8 элементов), с подклеенными к толкателям клавишами с рельефом Брайля для русского алфавита (от А до Я) и знаками препинания (точка, запятая, восклицательный знак, вопросительный знак, двоеточие, точка с запятой, дефис). В поле *5* компоновочной схемы размещаются фиксируемый выключатель питания прибора и три контролируемые кнопки отключения звука, установки одной из двух градаций громкости и одной из двух градаций длительности озвучивания. Кроме микроконтроллера *4*, на плате со стороны основания корпуса размещены резисторы и прочие элементы схемы прибора (элемент памяти звуковых образов изучаемого алфавита, линейный усилитель сигнала).

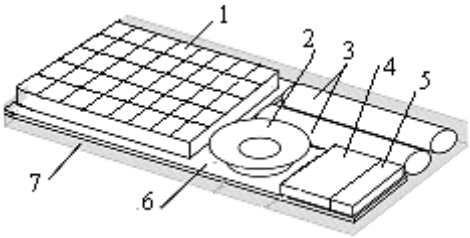


Рис. 3. Эскиз компоновки модулей прибора: *1* – модуль клавиш алфавита; *2* – динамик; *3* – элементы питания; *4* – микроконтроллер; *5* – модуль клавиш управления; *6* – несущая плата; *7* – основание корпуса

Проектная работа по звуковой части прибора не завершена. Варианты звуковых образов символов алфавита моделируются и находятся в стадии отбора. Звуковые образы формируются на основе равноинтервальной дискретизации реального звукового сигнала длительностью 1–2 с с числом отсчётов не более 1000–2000 на при числе уровней квантования не более 128 (с временем преобразования 8–10 мкс). По завершению отбора будут приняты решения по корректировке электрической схемы прибора и программы управления контроллера.

По предварительному анализу полученных результатов можно заключить, что в аппаратных ресурсах прибора должны присутствовать, вне или внутри контроллера, таймер, цифро-аналоговый преобразователь (ЦАП), память данных (констант) до 64 кб, линейный усилитель с выходной мощностью не менее 20 мВт. Функциональные и принципиальные схемы и программные модели прибора подготовлены для случая применения внешней памяти звуковых примитивов и внешнего линейного усилителя.

Требуемое число восьмиразрядных портов контроллера для работы с датчиками должно быть не менее двух, а для контроллеров с внешней памятью констант – четырёх. Ориентировочно допустимый интервал времени между выдачей отсчётов на ЦАП составляет не менее 500 мкс, что позволяет применять процессорные модули с длительностью машинного цикла до 10–20 мкс, т.е. тактовая частота процессора должна быть не менее 1 МГц.

В работе над прибором наиболее значимыми оказались проблемы изготовления клавишных модулей. Принятое решение об использовании кнопок с подклеенной к толкателю кнопки клавишей без специальной оснастки трудоёмко, а выйти на вариант прессования элементов конструкции клавишных модулей пока не удалось. Работу и в этом направлении, и в части совершенствования прибора, с целью сделать его доступным для применения, планируется продолжить после изготовле-

ния и испытания макетного образца прибора. Такой прибор вполне полезен и для иных приложений, как детская умная игрушка в изучении азбук и иных объектов и понятий окружающего мира.

ЛИТЕРАТУРА

1. Швецов В.И., Рощина М.А. Компьютерные тифлотехнологии в социальной интеграции лиц с глубокими нарушениями зрения: Учеб. пособие. Нижний Новгород; Нижегородский государственный университет им. Н.И. Лобачевского, 2007. 154 с.

2. Русская страница BAUM Retec AG [Электронный ресурс]. Режим доступа: http://www.tibsev.org/help/Braille.htm

3. Александров и др. Микропроцессорные системы / Под ред. Д.В. Пузанкова. СПб.: Политехника, 2002. 935 с.

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В МЕХАНИЗМАХ ПРИНЯТИЯ РЕШЕНИЙ*

А.И. Гуляев, студент 4-го курса

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

Любую нейронную сеть перед использованием необходимо обучать. Данный процесс очень трудоемкий и долгий. Но есть возможность применения нейронных сетей, обучение которых происходит без учителя. Для работы такой сети необходимы лишь некоторые начальные значения. В чем преимущество данных сетей? Данные сети могут найти связи, которые сложно заметить при работе обычной сети, так как она запрограммирована начальными значениями [1]. Применение таких сетей удобно при кластеризации данных. При получении информации появляется возможность перевести многомерное пространство в двумерное пространство. При этом строится визуальная картина полученных кластеров. Также возможно вычисление недостающих событий при помощи продукционных систем и обозначении их при помощи расстояния Хэмминга. Что дает использование таких конструкций? При принятии решения очень часто бывает, что полученной информации недостаточно и требуется система, которая может их обнаружить. Во-вторых, не всю информацию можно связать друг с другом напрямую, нейронные сети без учителя позволяют находить такие связи, по причине, описанной выше. Наиболее интересным примером являются нейронные сети Кохонена. Они являются сетью без учителя [1]. Также одним из вариантов сети являются самоорганизующиеся карты Кохо-

* Выполнено в рамках проекта ГПО КИБЭВС-0701 – Автоматизированная система поиска, анализа и принятия решений «ПУАРО».

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

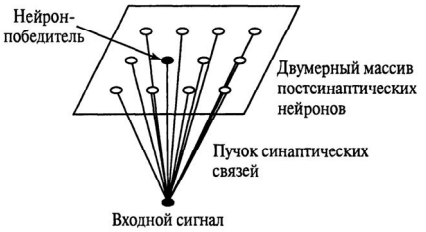


Рис.1. Самоорганизующаяся карта признаков (модель Кохонена)

Таким образом, кластерный анализ на нейронных сетях является довольно интересной системой, связанной с принятием решений. К большому сожалению, большинство систем на рынке являются закрытыми, и узнать, какие алгоритмы они используют, проблематично, если вообще возможно. Поэтому данный метод сложно считать новым, тем не менее дальнейшее исследование может принести очень интересные результаты. В результате можно получить систему, которая может обрабатывать почти любые данные не только в рамках поставленной задачи. Данная особенность позволяет расширить спектр использования данной системы не только в системах продержки принятия решений, но и во многих других областях. Несмотря на это, тематика принятия решений является наиболее обширной сферой применения данных технологий. Принятие решений требуется во многих сферах, если не во всех. И везде сталкиваются с тем, что имеется какая-либо неопределенность, с которой необходимо разобраться. Тут как раз и приходит очередь использования технологий, которые могут нестандартно исследовать имеющуюся ситуацию.

Научный руководитель – А.А. Шелупанов, д.т.н., профессор, зав. кафедрой КИБЭВС, проректор по научной работе ТУСУРа.

ЛИТЕРАТУРА

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

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

ПРИБОР ДЛЯ ЛОКАЛИЗАЦИИ НЕИСПРАВНОСТЕЙ В ЦИФРОВЫХ СХЕМАХ

М.М. Хандорин, студент 5-го курса;
Л.А. Торгонский, науч. рук., доцент
г. Томск, ТУСУР, каф. КИБЭВС, M.Khandorin@gmail.com

Для локализации неисправностей в цифровых устройствах применяются приборы и инструменты с простейшими функциями выдачи и приема контрольных сигналов (логические пульсаторы (задатчики) и пробники) и автоматизированные приборы с функциями программной обработки контрольных сигналов (одно- многоплюсные анализаторы, включая сигнатурные, эмуляторы, отладчики). Приборы второй модификации позволяют снизить трудоёмкость процесса обнаружения неисправности. Этот фактор явился определяющим для применения в учебной лаборатории устройств локализации неисправностей второго типа. Материал статьи посвящён прибору внутрисхемной эмуляции сигналов центрального микропроцессора (с шинной архитектурой внешних соединений с окружением) тестируемых плат учебных стендов [1]. В состав прибора включён однополюсный логический пробник, расширяющий возможности индикации и автоматической обработки выходных состояний в узлах тестируемых плат. Проект реализован в виде макетного изделия и прошёл успешную апробацию в тестировании плат учебных стендов в лаборатории микропроцесссорной техники кафедры.

В состав прибора входят персональный компьютер (ПК), микропроцессорный модуль формирования выходных и приёма входных сигналов (МФВиПВС), соответствующих эмулируемому узлу (рис. 1), модуль однополюсного логического пробника (МОЛП) с встроенной индикацией состояний и цепью программного опроса. Конструкции тестируемых плат учебных стендов допускают съём и замену микропроцессора с числом контактов внешних подключений 40 и микросхем постоянных ЗУ с числом контактов по 24. Эти особенности конструкции плат стендов ограничили число эмулируемых линий в МФВиПВС значением 40, с двухрядным расположением штыревых выводов при шаге 2,5 мм. Для эмуляции состояний объектов с иным расположением или числом контактов в МФВиПВС предусматриваются дополнительные переходные колодки. На компьютере размещены программа специализированного интерфейса пользователя, графическая форма которого приведена на рис. 2, и библиотека программ управления МФВиПВС. Модуль МФВиПВС реализован на ОМЭВМ ATmega64-16AU фирмы Atmel. Число выводов с битовым доступом в выбранной ОМЭВМ соответствует требуемому их составу для эмуляции. Приме-

нение микроконтроллера с квазидвунаправленными битовыми портами ввода/вывода позволяет свободно перенастраивать назначение входов/выходов при эмуляции. Допустимая токовая нагрузка для выходных сигналов составляет до 10–15 мА. Применённая в приборе ОМЭВМ своими встроенными средствами поддерживает загрузку программы и обмен данными с ПК по последовательному интерфейсу UART по протоколу RS-232.

Распространённой в современных ПК и удобной по конструкции средств подключения внешних устройств, по функциональным показателям является USB (универсальная последовательная шина). Этот интерфейс обладает высокой скоростью работы и позволяет своими соединениями обеспечить электропитание подключаемых устройств током до 500 мА при напряжении 5 В от ПК [3]. В процессе анализа требований к составу принято решение со стороны ПК применить интерфейс USB, а между ОЭВМ и ПК установить преобразователь USB-UART на специализированной микросхеме FT232 модификации R. Применение преобразователя интерфейсов упрощает написание драйверов для ПК, так как эмулятор будет опознан операционной системой компьютера, как виртуальный COM-порт. Модификация типа R, как требующая меньшего числа навесных компонентов [2], была применена для прибора, рассматриваемого в статье (см. рис. 1).

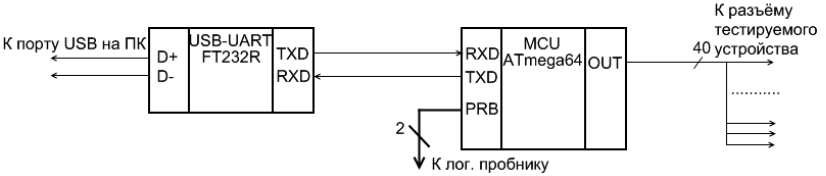


Рис. 1. Структурно-функциональная схема прибора

Как программно управляемый, рассматриваемый прибор функционирует под управлением двух программных модулей. Один из них размещен на ПК и поддерживает графический интерфейс, внешнее управление загрузкой программ формирования сигналов поддерживает выдачу и приём данных в обмене с МФВиПВС. Другой модуль размещается в программной памяти ОМЭВМ и поддерживает прием команд управления от ПК, формирование выходных сигналов эмуляции и приём сигналов с тестируемого устройства и логического пробника и передачу данных в ПК.

Любой обмен данными между ПК и МФВиПВС происходит только по запросу от ПК. В программе ПК прибора предусмотрено шесть команд управления МФВиПВС и МОЛП:

– настроить линию порта на выход;
– настроить линию порта на вход;
– установить линию в состояние 1;
– установить линию в состояние 0;
– опросить линию, настроенную на вход;
– опросить логический пробник.

После выполнения очередной команды прибор переходит в режим ожидания до приёма следующей команды.

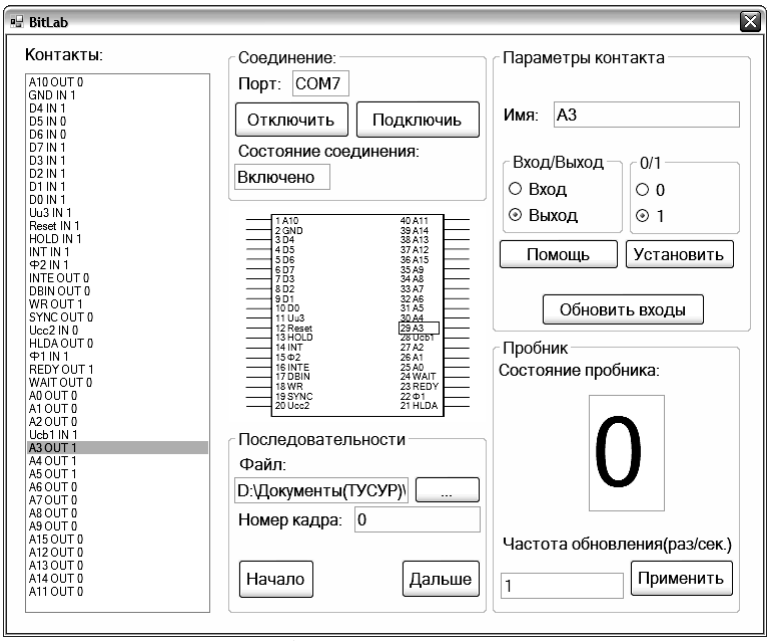


Рис. 2. Форма интерфейса настройки и управления прибора

В зависимости от действий пользователя ПК посылает команды к прибору. Графический интерфейс позволяет: настраивать линии ввода/вывода МФВиПВС (группа «Параметры контакта»), отображать состояние МОЛП (группа «Пробник»), эмулировать временные диаграммы работы микросхем или интерфейсов (группа «Последовательности»). Последовательности задаются в текстовом файле, который содержит псевдонимы контактов, их направление ввод или вывод и логическое состояние для выходов. Программа опрашивает линии, настроенные ввод, при текущих состояниях сигнала на линиях, настроенных на вывод (рис. 2).

По результатам работы реализованы аппаратные и программные модули прибора. Лабораторные испытания прибора подтвердили правильность принятых решений.

Подготовлены библиотека специализированных модулей программ управления МФВиПВС и руководство по их постановке и эксплуатации при тестировании платы процессора стенда УМК.

Благодаря универсальности функциональной настройки сорока битовых портов ввода/вывода ОМЭВМ МФВиПВС и открытости библиотеки драйверов эмуляции процессов, спектр возможных применений прибора ограничен лишь составом конструкций средств подключения, составом и содержанием установленных драйверов и параметрами сигналов эмуляции процесса МФВиПВС прибора (уровни, фронты, задержки загрузки).

Программное обеспечение прибора установлено на операционной платформе Linux.

ЛИТЕРАТУРА

1. Торгонский Л.А. Учебные стенды: Справ. пособие. Ч. 1. Томск: ТУСУР, 2007. 50 с.

2. Уильямс Г.Б. Отладка микропроцессорных систем: Пер. с англ. М.: Энергоавтомиздат, 1988. 253 с.

3. Гук М. Интерфейсы ПК: Справочник. СПб.: ЗАО «Изд-во «Питер», 1999. 416 с.

4. Трамперт В. Измерение, управление и регулирование с помощью AVR-микроконтроллеров. Киев: МК-Пресс, 2006. 208 с.

АНАЛИЗ СТРУКТУРЫ СЕТИ УЧРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ

С.Ю. Исхаков, аспирант

г. Томск, ТУСУР, каф. КИБЭВС, frosty@ssmu.ru

Построение локально-вычислительных сетей (ЛВС) [1] организаций без учета особенностей конкретной организации приводит к тому, что даже сеть, содержащая современные программные и аппаратные средства может использоваться неэффективно.

На базе ЛВС Сибирского государственного медицинского университета проводится исследование, направленное на разработку моделей и алгоритмов для оценки загрузки сети и ее работоспособности.

Первым этапом является анализ объекта исследования. На рис. 1 представлена физическая модель исследуемой ЛВС.

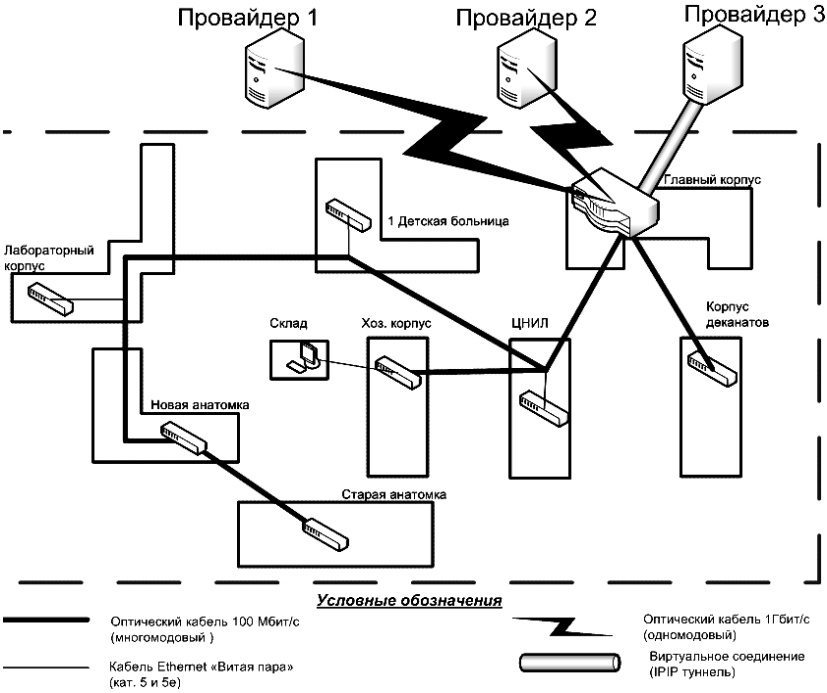


Рис. 1. Физическая модель исследуемой ЛВС

Логическая структура сети построена на основе технологии виртуальных сетей VLAN [1] и технологии Active Directory [2] компании Microsoft. В главном корпусе (см. рис. 1) находится центральный узел связи, состоящий из головного маршрутизатора; аппаратного фаерволла [3]; управляемого коммутатора уровня L3; группы серверов сервисов общего пользования (web-сервер, почтовый сервер и т.д.); группы серверов, обеспечивающих работу двух доменов Active Directory, связанных между собой нетранзитивными отношениями.

Головной маршрутизатор является каналообразующим звеном ЛВС. Он обеспечивает маршрутизацию, анализ и блокирование трафика определенных сервисов (пиринговые сети [1] и т.д.), балансировку нагрузки и резервирование каналов связи. Предоставляет доступ в ЛВС клиентам из сетей территориально удаленных филиалов организации с помощью технологий VPN.

Аппаратный фаерволл содержит списки контроля доступа [3], а также обеспечивает аутентификацию [3] пользователей при выходе за пределы ЛВС организации. Аутентификация построена на базе техно-

логии «cat-through proxy» компании Cisco Systems. В качестве базы данных пользователей используется RADIUS-сервер.

Управляемый коммутатор выполняет роль структурообразующего элемента ЛВС. Организует структуру виртуальных сетей VLAN для сегментирования ЛВС и предотвращения широковещательных штормов внутри сети организации. Содержит списки контроля доступа [1] для разграничения прав между отдельными VLAN и защиты серверов от атак внутри сети.

Особенностями ЛВС являются: гетерогенность как программных, так и аппаратных средств; территориальная удаленность филиалов; наличие «обособленных» подразделений внутри кампусной сети университета, имеющих собственную ЛВС, но в целом подчиняющихся общим правилам работы внутри сети организации.

Кроме того, в сети используется наличие нескольких различных баз данных для аутентификации, в некоторых случаях дублирующих друг друга. В частности, отдельно происходит аутентификация пользователей, работающих в доменах [2] Active Directory, аутентификация пользователей при работе за пределами ЛВС университета, аутентификация пользователей при работе с почтовым сервером.

На рис. 2 приведена схема аутентификации в сети университета.

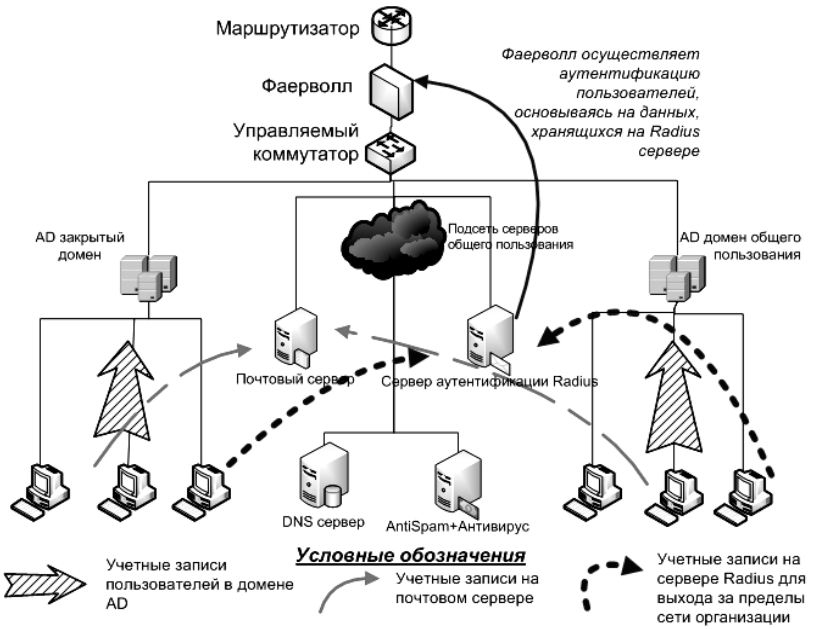


Рис. 2. Схема аутентификации в исследуемой ЛВС

В результате анализа объекта исследований были построены физическая и логическая модели ЛВС, изучена схема аутентификации пользователей, составлен список используемого программного и аппаратного обеспечения.

Эти данные позволят более точно определить тематику обзора существующих разработок в области данного исследования и помогут в дальнейшем конкретизировать цели и задачи при разработке алгоритмического обеспечения оценки загрузки данной ЛВС.

Научный руководитель – А.А. Шелупанов, д.т.н., профессор, зав. кафедрой КИБЭВС, проректор по научной работе ТУСУРа.

ЛИТЕРАТУРА

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учеб. для вузов. 3-е изд. СПб.: Питер. 2006. 958 с.

2. Томас О., Поличелли Дж., Миллер Д.Р. Администрирование корпоративных сетей на основе Windows Server 2008: Учеб. курс Microsoft / Пер. с англ. М.: Русская редакция, 2009. 528 с.

3. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А.. Основы информационной безопасности: Учеб. пособие. М.: Горячая Линия-Телеком, 2006. 544 с.

МОДЕЛЬ ДЕТЕРМИНИРОВАННОЙ СЕТИ РОБОТОВ

К.В. Картавцев, аспирант

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

Модель детерминированной сети роботов позволяет руководить деятельностью автономных роботов, планировать их поведение и взаимодействие, адаптироваться к изменениям, произошедшим в среде, изучать и разрешать конфликты между роботами с помощью обмена информацией.

Основной целью данной работы является разработка и реализация алгоритмов управления взаимодействием и коллективным поведением группы автономных роботов, направленного на решение общей задачи.

Для решения рассматриваемой задачи был применен подход, основанный на центральном последовательном управлении (ЦУПос). В этом случае центр управления связан с каждым элементом группы непосредственно (см. рис.) и шагом работы системы управления является движение одного элемента группы. Очередность выбора элементов для шага может быть различной.

Вызовы от роботов поступают в центр управления группами через единичные интервалы времени.

Центр управления получает от каждого робота информацию о текущем положении, о состоянии окружающего робот участка среды. Данная информация обрабатывается центром управления, после чего он отправляет роботу координаты промежуточной цели движения.

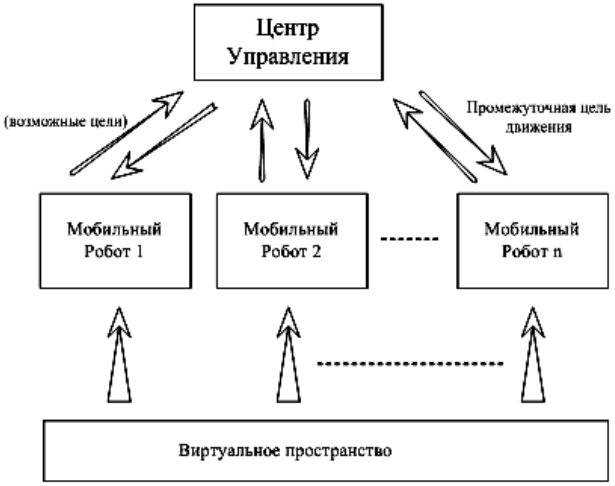


Рис. 1. Модель детерминированной сети роботов

Как только центр управления заканчивает обслуживание некоторого вызова, он немедленно начинает обслуживать следующий, а обслуженный вызов покидает центр управления. Центр управления простаивает только в случае отсутствия вызовов.

Вызовы обслуживаются центром управления с помощью правила, согласно которому поступаемые от роботов заявки обслуживаются не по очереди (когда сначала обслуживаются вызовы, пришедшие в момент времени $k = 1$, затем вызовы, пришедшие в момент $k = 2$, и т.д.), а с помощью определения приоритетных вызовов (например, вызов об обнаружении цели). То есть вызовы различных типов образуют две различные очереди. И только если приоритетная очередь пуста, центр управления начинает обработку заявок из второй очереди.

Сам робот представляет собой автономную интеллектуальную систему, которая обладает следующими характеристиками:

1) тело робота (обладает определенной формой и размерами);

2) сенсорная система (имитирует органы чувств человека);

3) система управления.

Для выполнения поставленных задач мобильные роботы должны обладать измерительными приборами (датчиками).

Виртуальные датчики являются совмещенными моделями логического датчика и вычислительного модуля. В каждом виртуальном датчике выполняются сенсорные и вычислительные операции.

Для осуществления движения к промежуточной цели, мобильный робот должен обладать прибором измерения расстояния. Реальные роботы часто используют лазерные дальномеры. Кроме того, считается, что мобильный робот способен различать целевую точку.

Полученные от виртуальных датчиков данные мобильный робот самостоятельно анализирует и обрабатывает для дальнейшего использования и движения.

После того, как только робот достиг промежуточную точку движения, либо обнаружил конечную цель, он делает запрос к центру управления, для вычисления новой промежуточной цели движения.

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Жданов А.А., Крыжановский М.В., Преображенский Н.Б. Бионическая интеллектуальная адаптивная система управления мобильным роботом // Искусственный интеллект. 2002. Т. 4. С. 341–350.

2. Захаров В.Н. Современная информационная технология в системах управления // Известия академии наук. Теория и системы управления. 2000. №1, С. 70–78.

3. Станкевич Л.А.. Мультиагентная технология в когнитивных системах управления автономными роботами // Экстремальная робототехника: X науч.-техн. конф. СПб., 1999. С. 13–20.

4. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. 2-е изд. М.: Наука, 1987.

GPS-GSM-СИСТЕМА НАБЛЮДЕНИЯ ЗА ТРАНСПОРТОМ

А.В. Кириченко, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС

В настоящее время во всем мире намечается значительный рост интереса к системам, обеспечивающим автоматизацию контроля за перемещением автотранспорта. Изначально системы слежения GPS были военной разработкой, то теперь они служат самым мирным целям: увеличение экономической эффективности работы транспортного предприятия через минимизацию нецелевого использования транспорта, четкое следование маршруту перевозок, контроля над расходом топлива. Как результат, серьезно экономятся финансовые средства. К тому же систему GPS мониторинга транспорта вполне реально использовать

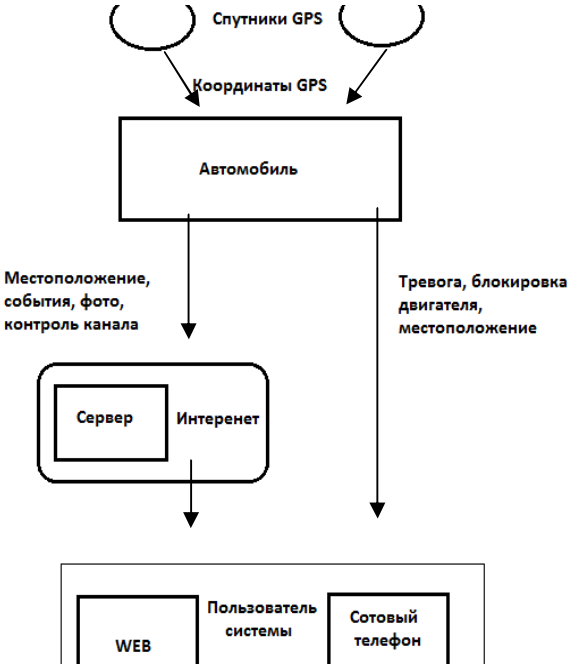
как спутниковую систему охраны или в качестве спутниковой сигнализации [1]. Система спутникового GPS-слежения дает неограниченную возможность контроля всех перемещений транспортного средства. Спутниковая система слежения и gps мониторинга транспорта широко применяется на предприятиях, занимающихся перевозкой грузов, и пассажирских перевозках (в службах такси), в жилищно-коммунальном хозяйстве, строительных фирмах [2].

На сегодняшний момент у системы GPS мониторинга транспорта самое широкое применение – именно в службах Министерства по чрезвычайным ситуациям [1].

Приемник GPS определяет географические координаты ТС и передает их микропроцессорному устройству. Микропроцессорное устройство обрабатывает полученные данные и с определенной частотой записывает их в энергонезависимую память. Информация с внешних датчиков, установленных на ТС, после обработки также записывается в энергонезависимую память прибора. Для передачи информации с прибора на центральный сервер используется GSM-сеть, а также передаёт информацию о любых изменениях в системе мониторинга хозяину автомобиля на мобильный телефон. Для этой цели в состав прибора включен GSM-модем. Информация может передаваться как в виде SMS, так и в пакетном виде GPRS (рис.). После получения информации на сервере она выводится на электронную карту [1].

Проведём сравнение нескольких устройств, таких как «Avtotraker B2», «Скаут» и «MS-PGSM 4».

Габариты и масса всех устройств практически одинаковы, находятся в пределах 190×90×40 мм, что позволяет установить прибор практически в любом месте автомобиля. Потребление тока меньше всего у «Avtotraker B2», в среднем оно составляет 20 мА/ч. Все устройства обладают отличной устойчивостью к вибрациям и перегрузкам, имеют резервный источник питания, а также «Avtotraker B2» и «MS-PGSM 4» имеют возможность подключения дополнительного источника питания. Рабочий диапазон температур у «Avtotraker B2» и «Скаут» практически одинаков и составляет –25…+55 °С, что отличает их от «MS-PGSM 4» рабочий диапазон температур которого составляет –45…+85 °С. Антенны у «Avtotraker B2» и «Скаут» выносные, у «MS-PGSM 4» антенны встроенные, что повышает скрытность прибора, так же он обладает встроенным датчиком наклона. «MS-PGSM 4» имеет комбинированное отключение питания различных модулей, что дает возможность реализовать ряд энергосберегающих алгоритмов при работе в режиме резервного питания, и имеет шину LAN для подключения противоугонного комплекса.



Принцип работы системы GPS GSM

Из представленных данных можно сделать вывод, что устройство «MS-PGSM 4» по многим техническим характеристикам превосходит свои аналоги.

Из-за недостатка более подробной информации о технических характеристиках приборов невозможно провести более тщательный анализ.

Научный руководитель – Д.Д. Зыков, к.т.н., доцент кафедры КИБЭВС ТУСУР.

ЛИТЕРАТУРА

1. Avtotreker B2 [Электронный ресурс]. http://www.auto-scan.ru/ index.php?p=gps_index

2. GPS [Электронный ресурс]. http://www.msk-gps.ru/page_21_1.htm

ТЕРМИНАЛЬНЫЕ СЕРВЕРЫ И БЕЗДИСКОВЫЕ СТАНЦИИ

С.Д. Литвинов, студент 5-го курса

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

В качестве терминального сервера можно использовать Microsoft Windows 2000 Server , Citrix MetaFrame, Microsoft Windows 2003 Server.

Поддерживаемые функции терминала

Возможные разрешения экрана для клиента: 1024×768, 800×600, 640×480, 1280×1024, 1600×1200. Возможна печать на локальный принтер и работа с локальными com-портами.

Программное обеспечение, установленное на слабой рабочей станции, выполняет только две функции: передача координат мыши и нажатия клавиш на терминальный сервер, а также прием и отображение изменений экрана, переданных терминальным сервером. Принимая во внимание скорость передачи в существующих локальных сетях (не менее 10 Мбит/с), обновления экрана могут отображаться на той самой маломощной локальной станции без сколько-нибудь заметных задержек. То есть набор текста, работа с табличными данными, электронной почтой или работа в сети интернет происходит полностью неотличимо от работы на современной рабочей станции.

Для работы самого сервера необходимо минимум 128 Mb RAM. Потребление памяти для одной рабочей сессии – 5–10 Mb.

Потребление памяти для приложений:

В тестовом варианте при загрузке на 2 клиентах MS Word , MS Excel , MS Access , MS Internet Explorer было определено по 50–60 Mb на одну сессию.

Ориентировочное потребление памяти сервера на одно запущенное приложение следующее:

1. MS Word 2000 – 10 mb.
2. MS Excel 2000 – 15 mb.
3. MS Access 2000 – 15 mb.
4. MS Internet Explorer – 10 mb.
5. MS Visio 2000 – 16 mb.

Также стоит отметить, что Windows 2000 на практике потребляет меньше ресурсов с ростом числа пользователей, т.е. при добавлении каждого следующего пользователя в систему необходимый прирост памяти сокращается с каждым новым пользователем. Предполагается, что в двухпроцессорной конфигурации для 30 пользователей может быть с успехом использован двухпроцессорный сервер с 2 Гб оперативной памяти.

Классический метод создания бездисковых станций – это первоначальная загрузка ядра операционной системы с сетевой поддержкой и последующее использование терминального клиента для доступа к терминальному серверу. Наиболее интересным представляется применение удаленной загрузки посредством использования сетевых карт с BootROM. Это позволяет разместить образ операционной системы на открытом ресурсе сервера и загрузить его по сети на клиентскую станцию. С целью снижения затрат на лицензирование рабочих станций и с

целью уменьшения размера образа загружаемой системы рекомендуется использование терминального клиента на базе операционной системы Linux. Такой образ системы занимает 5–10 Мб и вся загрузка терминальной станции занимает порядка 30 с. Вдобавок ко всему требования к аппаратному обеспечению клиентской станции резко снижаются. Например, данная конфигурация вполне работоспособной станции:

Processor: 486, RAM: 16MB (32 MB recommended), Network: 10 or 100 mbps, network card (any supported by kernel 2.4.x), Video card: All supported by Xfree86 4.3/3.3.6, Mouse: Serial, PS/2, USB.

Несмотря на все преимущества терминального режима, имеется ряд ограничений на используемые приложения. Приложения, использующие видеопотоки высокого разрешения и стереопотоки звука с высоким качеством, требуют для работы в терминальном режиме мощных сетей с пропускной способностью не менее 100 Мбит/с. Некоторые старые программные пакеты ненормально относятся к наличию нескольких копий себя в памяти. Такие приложения могут потребовать специального окружения или просто не будут работать в окружении терминального сервера. Старые DOS-приложения, требующие прямого доступа к аппаратной части компьютера, не могут работать на терминальном сервере.

Терминалами могут служить практически любые компьютеры, в том числе класса 486/Pentium 60, а также так называемые Windows-терминалы для Windows CE версий 2.12 или 3.0. Терминалы не нуждаются в модернизации. Терминальные решения снижают затраты на организацию рабочих мест: не требуются магнитные и оптические накопители, большие объемы памяти, высокие процессорные мощности и т.д. При использовании устаревшей техники стоимость рабочего места снижается до 200–300 долл., а в случае использования новых терминальных клиентов – до 300–400 долл. При работе в режиме терминала у пользователя намного меньше возможностей повлиять на стабильность работы ПО на своем рабочем месте. А при корректной настройке политик доступа к ресурсам у пользователя просто нет шансов вывести что-либо из строя. Даже разрушительное действие вирусов сводится только к возможному повреждению личных данных пользователя, но никак не повлияет на что-либо в сети или на терминальном сервере. Администрирование терминальной системы становится действительно централизованным. Так, если у пользователя возникла проблема с программным обеспечением, то администратор системы может со своего рабочего места подключиться в режиме терминала к сессии пользователя и помочь тому решить любую возникшую проблему. Администратор или менеджер с соответствующими полномочиями может в любой момент времени включить функции визуального контроля за работой того или

иного пользователя. Все ПО устанавливаются и обновляются исключительно на терминальном сервере, и появляются широкие возможности стандартизации программных средств в информационной системе предприятия. Поскольку доступ к терминальному серверу по RDP-протоколу не подразумевает передачи файлов и совместного доступа к файлам и каталогам на сервере, существенно уменьшается возможность несанкционированного доступа.

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Сети и системы связи (ООО «Антонюк-Консалтинг»). Архив по темам и номерам начиная с 2006.

СРАВНИТЕЛЬНЫЙ ОБЗОР SCADA-СИСТЕМ

А.В. Маркин, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, avm@sibnet.ru

SCADA – диспетчерский контроль и сбор данных (англ. Supervisory Control And Data Acquisition). SCADA-системы представляют собой специализированное программное обеспечение, ориентированное на визуализацию технологических процессов и коммуникацию с внешним миром [1].

В SCADA-системе контролируется работа всех инженерных систем и осуществляется согласованное функционирование отдельных систем управления. Передовая диспетчерская система позволяет сделать работу систем жизнеобеспечения максимально эффективной, свести к нулю процент нерационального использования ресурсов, обеспечить детальный контроль всех технологических участков и систем [2].

Помимо функций визуализации состояния технологического процесса, системы диспетчеризации обеспечивают регистрацию и архивацию значений технологических параметров, формирование, протоколирование и выдачу сигналов тревог (визуальных, звуковых), расчет текущих технико-экономических показателей и формирование оптимальных регламентов работы оборудования, которые передаются для исполнения на уровень управления процессом.

Для сравнения были выбраны следующие SCADA-системы: InTouch, Citect, FIX, Genesis, Factory Link, TraceMode, WinCC, PcVue.

Подавляющее большинство SCADA-систем реализовано на MS Windows-платформах. Именно такие системы предлагают наиболее полные и легко наращиваемые MMI-средства. Учитывая позиции

Microsoft на рынке операционных систем (ОС), следует отметить, что даже разработчики многоплатформенных SCADA-систем, такие как United States DATA Co (разработчик FactoryLink), приоритетным считают дальнейшее развитие своих SCADA-систем на платформе Windows NT. Некоторые фирмы, до сих пор поддерживавшие SCADA-системы на базе операционных систем реального времени (ОСРВ), начали менять ориентацию, выбирая системы на платформе Windows NT.

Одной из основных задач систем диспетчерского контроля и управления является обработка информации: сбор, оперативный анализ, хранение, сжатие, пересылка и т.д. Таким образом, в рамках создаваемой системы должна функционировать база данных.

Практически все SCADA-системы, в частности, Genesis, InTouch, Citect, используют ANSI SQL синтаксис, который является независимым от типа базы данных. Таким образом, приложения виртуально изолированы, что позволяет менять базу данных без серьезного изменения самой прикладной задачи, создавать независимые программы для анализа информации, использовать уже наработанное программное обеспечение, ориентированное на обработку данных.

Функционально графические интерфейсы SCADA-систем весьма похожи. В каждой из них существует графический объектно-ориентированный редактор с определенным набором анимационных функций. Используемая векторная графика дает возможность осуществлять широкий набор операций над выбранным объектом, а также быстро обновлять изображение на экране, используя средства анимации.

Большинство SCADA-систем имеют встроенные языки высокого уровня, VBasic-подобные языки, позволяющие генерировать адекватную реакцию на события, связанные с изменением значения переменной, с выполнением некоторого логического условия, с нажатием комбинации клавиш, а также с выполнением некоторого фрагмента с заданной частотой относительно всего приложения или отдельного окна.

Современные SCADA-системы не ограничивают выбора аппаратуры нижнего уровня, так как предоставляют большой набор драйверов или серверов ввода-вывода и имеют хорошо развитые средства создания собственных программных модулей или драйверов новых устройств нижнего уровня. Сами драйверы разрабатываются с использованием стандартных языков программирования.

Стоимость SCADA-систем, на первый взгляд, кажется достаточно высокой. При этом механизм определения цены у разных фирм-разработчиков различен: стоимость InTouch, например, зависит от количества переменных, используемых в разрабатываемой прикладной программе, стоимость PcVue определяется количеством каналов ввода/вывода, которые должна поддерживать система, а пакет FactoryLink

имеет высокую базовую стоимость, но не имеет ограничений по количеству каналов. При оценке стоимости SCADA-системы учитываются минимальные и рекомендуемые ресурсы компьютера, необходимые для ее установки. При этом в некоторых системах, например WinCC, число допустимых переменных напрямую зависит от количества доступного ОЗУ.

Современные SCADA-системы не ограничивают выбора аппаратуры нижнего уровня (контроллеров), так как предоставляют большой набор драйверов или серверов ввода/вывода и имеют хорошо развитые средства создания собственных программных модулей или драйверов новых устройств нижнего уровня.

Для подсоединения драйверов ввода/вывода к SCADA-системе в настоящее время используются следующие механизмы:

– ставший стандартом de facto динамический обмен данными (DDE);

– собственные протоколы фирм-производителей SCADA-систем, реально обеспечивающие самый скоростной обмен данными;

– новый OPC-протокол, который, с одной стороны, является стандартным и поддерживается большинством SCADA-систем, а с другой стороны, лишен недостатков протоколов DDE [3].

По функциональным возможностям все рассмотренные SCADA-системы в целом сравнимы. Технология программирования близка к интуитивному восприятию автоматизируемого процесса. Также мощное объектно-ориентированное программирование, используемое в большинстве этих пакетов, делает эти продукты легкими в освоении и доступными для широкого круга пользователей.

Все системы можно считать в той или иной степени открытыми, обеспечивающими возможность дополнения функциями собственной разработки, имеющими открытый протокол для разработки собственных драйверов, развитую сетевую поддержку, возможность включения ActiveX объектов и доступность к стандартным базам данных.

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

ЛИТЕРАТУРА

1. Все о SCADA: АСУ ТП и промышленная автоматика [Электронный ресурс]. Режим доступа: http://automation-system.ru/about-scada.html

2. ООО «ОЛИЛ»: Диспетчеризация – новое слово в современном доме! [Электронный ресурс]. Режим доступа: http://cybrotech.ru/article_64. html

3. Куцевич Н. А. SCADA-системы [Электронный ресурс] / ЗАО РТСофт. Режим доступа: http://www.asutp.ru/?p=600055.

АВТОМАТИЗИРОВАННОЕ ПОСТРОЕНИЕ ЗАЩИТЫ ОБЪЕКТА

А.А. Мельников, студент 5-го курса
г. Томск, ТУСУР, каф. КИБЭВС, mukamol@inbox.ru

Построение защиты объекта является одной из самых не автоматизированных областей. И если без ручных замеров никак не обойтись, то проведение расчётов о правильном расположении СЗИ является одной из самых кропотливых задач. Попытаемся автоматизировать данную задачу на программном уровне.

Предположим, что у нас имеется объект защиты – какое-либо помещение, для которого надо спроектировать систему защиты по заданному классу защищённости.

Для построения системы защиты помещения нам необходимо знать как минимум следующие параметры:

– план этого помещения;

– точное расположение дверей и их параметры;

– расположение окон и их параметры;

– расположение коммуникаций (батареи отопления, вентиляция, телефонные кабели, провода локальной сети, пожарной сигнализации, электропроводка);

– толщину стен и перекрытий;

а также от чего следует защищать это помещение, т.е. угрозы:

– проникновения;

– прослушивания;

– визуального наблюдения и т.п.

Система автоматизированного построения защиты объекта должна решать задачи по поводу оптимального набора СЗИ по данным параметрам и их расположения, таких как:

– камеры видеонаблюдения;

– вибро-акустические излучатели;

– акустические излучатели;

– пьезо-электрические излучатели.

а также способствовать принятию решения по поводу целесообразности применения тех или иных СЗИ (стоит ли менять деревянную дверь на железную, имеет ли смысл ставить камеры видеонаблюдения и т.д.).

Исходя из вышесказанного, АС должна иметь следующие модули:

– модуль интерфейса, обеспечивающий удобное взаимодействие пользователя и программы;

– графический модуль, позволяющий строить план помещения со всеми коммуникациями и располагать СЗИ на выбранных местах. Также на него выводится построенная система защиты объекта;

– модуль автоматизированного построения защиты, позволяющий анализировать объект и угрозы, выявлять уязвимости и принимать решения по поводу используемых СЗИ и их расположения;

– модуль работы с БД. Так как программа должна работать с огромным количеством СЗИ, то необходима БД для их хранения, а следовательно, необходим и модуль для работы с ней. Он должен позволять просматривать средства защиты, их характеристики и описания;

– модуль самодиагностики также должен присутствовать, т.к. в построенной системе защиты не должно быть уязвимостей из-за неверно обработанных или введённых данных. Через него должны проходить входные данные и команды пользователя.

На рисунке приведена схема потоков информации между модулями.

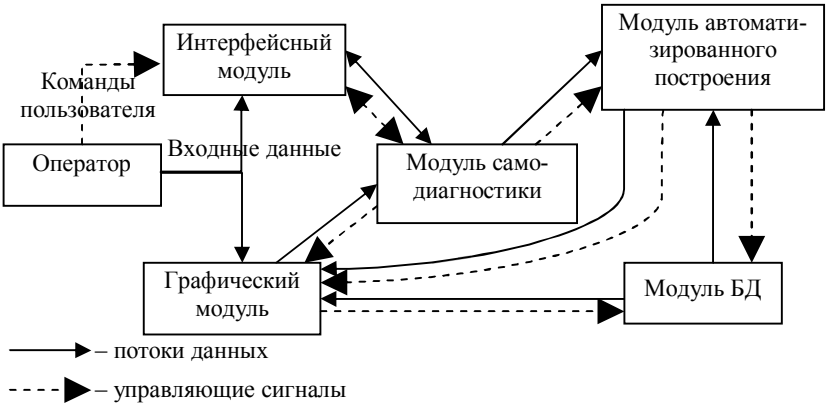


Схема потоков управляющих сигналов и данных между модулями АС

Оператор через интерфейс и графический модуль вводит изначальные данные (схема помещения, характеристики объектов) и команды (желаемый класс защищенности, угрозы, хочет ли он сам построить защиту объекта или желает, чтобы АС сама спроектировала её). Далее входные данные и команды пользователя попадают в модуль самодиагностики, где проверяются на корректность. Если пользователь желает, чтобы АС построила защиту объекта, то данные также отправляются в модуль автоматизированного построения. Модуль их анализирует, с помощью БД подбирает оптимальный набор и расположение СЗИ и строит защиту объекта, после чего выводит её на графический модуль. Далее пользователь может, проанализировав построенную систему защиты объекта, её отредактировать. Все команды пользователя при редактировании также проходят через модуль диагностики.

В дальнейшем к данной системе можно будет добавить модули для построения информационной защиты компьютерных систем, локальных сетей или модуль с образцами документов по организационному обеспечению информационной безопасности.

Научный руководитель – Е.М. Давыдова, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации. Томск: В-Спектр, 2006.

2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004.

МОДУЛЬ ВЗАИМОДЕЙСТВИЯ С МОБИЛЬНЫМ ПЕРСОНАЛОМ*

М.И. Мельников, аспирант;

М.О. Некрылова, И.Н. Шишкин, студенты 4-го курса

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

Беспроводные технологии уже сейчас готовы соревноваться в быстроте, защищенности и скорости со своим предшественником на примере сетей третьего поколения (3G) [1].

Развитие технологии не стоит на месте, а движется вместе с возрастающими потребностями людей. В современном обществе нельзя представить человека без мобильного телефона и компьютера. В целях создания современных машин используются инновационные технологии. Устройства, которые раньше занимали много места, теперь занимают лишь малую его часть. Так, создание беспроводных технологий позволяет изменить представление об их использовании.

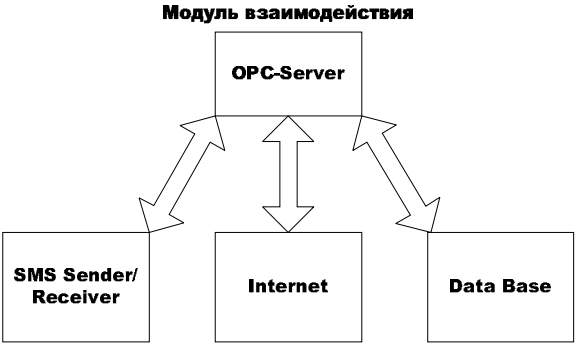
Модуль взаимодействия представляет собой инновационный комплекс программ, объединенных в систему [2].

Создание модуля взаимодействия с мобильным персоналом позволит повысить уровень управления в сфере мобильных работ.

Данный аппаратно-программный комплекс (см. рис.) является автономной системой для работы с мобильным персоналом и включает в себя OPC-сервер, средства для приёма и отправки SMS-сообщений, обмена данными с мобильными устройствами через Интернет, а также записи и чтения информации из базы данных. Данные о состоянии объ-

* Выполнено в рамках проекта ГПО КИБЭВС-0903 – Разработка системы управления на базе беспроводных технологий.

екта автоматизации модуль отслеживает с помощью OPC-сервера, использующего протокол OPC DA 3.0 [3]. В зависимости от входных данных программа автоматически обращается к базе данных для поиска информации. В случае возникновения аварии на объекте автоматизации модуль самостоятельно принимает решение об отправке мобильного персонала. При этом учитываются следующие факторы: состояние персонала («занят» или «свободен»), расстояние до места аварии, квалификация персонала.



Структура модуля взаимодействия

Взаимодействие с мобильным персоналом может осуществляться по двум каналам связи: основному и резервному. В качестве основного канала выступает Интернет, а резервного – GSM-сети (SMS-сообщения). Обмен информацией по строго определённому протоколу, который включает в себя следующие возможности: проверка состояния мобильного персонала («занят» или «свободен»), отправка и приём заявки, оповещение о прибытии на место аварии, тестирование объекта (после окончания работ), снятие заявки. Также предусмотрена возможность перенаправления заявки, в случае если первый получатель не подтвердил приём.

База данных обеспечивает хранение и запись новой информации, составление отчетов о работе персонала, системы и оборудования. Весь процесс поиска, добавления, обновления или удаления данных происходит с помощью SQL-запросов, что позволяет упростить внедрение модуля взаимодействия, так как программу не нужно будет переписывать под конкретную базу данных, а конечному пользователю нужно лишь составить свои запросы.

В комплекс программ входит программа для настройки модуля взаимодействия с удобным интерфейсом, в которой можно указать сле-

дующие параметры: установки GSM-модема, параметры подключения к базе данных.

Беспроводные технологии являются основным средством для работы с мобильным персоналом.

Возможность контролировать процесс работы и перемещения является одной из задач модуля взаимодействия. В целях достижения этой задачи используются беспроводные технологии, одним из таких устройств являются GSM-модемы.

Используя современные устройства, система может определить местоположение персонала. Координаты, получаемые системой, оформляются в отчет о передвижениях мобильного персонала.

Основным комплексом программ являются приложения для мобильных устройств (телефон, КПК [4]). Приложения позволяют пользователю расшифровать послание сервера.

ЛИТЕРАТУРА

1. Мельников М.И. Разработка автоматизированной системы управления распределённым лифтовым хозяйством на базе беспроводных технологий // Доклады ТУСУР 1(19). Ч. 2. Томск: ТУСУР, 2009. С. 81.

2. Особенности проектирования распределенных АСУ ТП: http://asutp.ru/?p=600406

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

4. Крелль Б. Windows Mobile. Разработка приложений для КПК. М.: ДМК, 2008. 352 с.

АУДИОМЕТР ПОРТАТИВНЫЙ, ОСНОВАННЫЙ НА ВОЗДУШНОЙ ПРОВОДИМОСТИ

Р.Ф. Нигматуллин, А.Г. Понизов, студенты 5-го курса

г. Томск, ТУСУР, каф. ПрЭ, rrafa@inbox.ru , ponizov_ne@sibmail.com

Болезни, связанные со слуховыми органами, были всегда, и, к сожалению, современная медицина по-прежнему бессильна против большинства проблем, таких как старческая тугоухость или врожденный дефект слуха. Но очень часто проблемы со слухом развиваются у молодых и здоровых людей, в таких случаях для оперативного и немедленного реагирования необходимо быстро и точно поставить диагноз. Именно в таких случаях специалистам отоларингологам помогает аудиометрия.

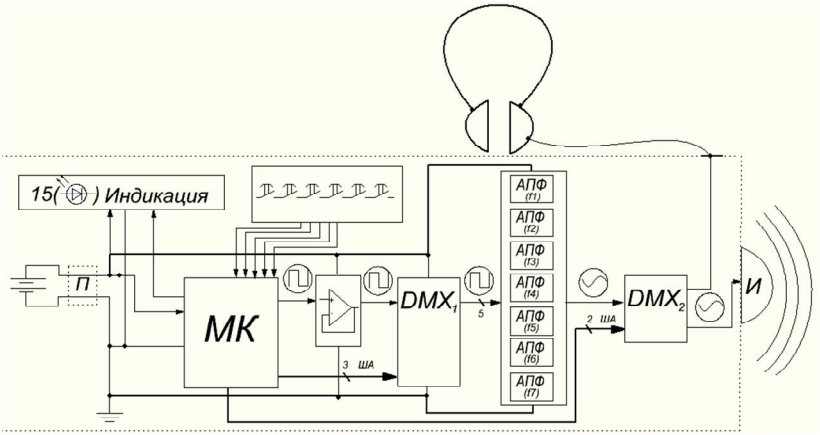
Аудиометрия (от лат. audio – слышу и греч. metron – мера) – исследование чувствительности слуха с помощью электроакустических приборов, аудиометров, которые позволяют строго дозировать интен-

сивность звуковых сигналов, осуществлять исследование на всех звуковых частотах, функциональные пробы по диагностике пороговой дифференциальной чувствительности, интенсивности, маскировки [1].

Результатом аудиометрии является аудиограмма, которая представляет собой характеристику зависимости остроты слуха от интенсивности звука и его частот, она изображается на бланке в виде кривых, отражающих состояние воздушной и костной проводимости. Наличие на аудиограмме значительного разрыва между кривыми воздушной и костной проводимости типично для кондуктивной тугоухости [2]. Следовательно, нельзя пренебрегать ни одним из видов исследований.

Аудиометр портативный, основанный на воздушной проводимости, проектируется на базе того же аудиометра, основанного на костной проводимости, путем добавления возможности получения частот в 125 и 250 Гц, а также добавления аудио выхода для наушников.

На рисунке показана функциональная схема аудиометра.



Функциональная схема аудиометра, основанного на воздушной проводимости, на базе аудиометра костной проводимости: *П* – преобразователь напряжения питания; *МК* – микроконтроллер; *АПФ* – активный полосовой фильтр; *И* – излучатель вибрации; *DMX* – Д-мультиплексор; *ША* – шина адреса

Алгоритм работы аудиометра:

1. Пользователь при помощи кнопок управления задает микроконтроллеру необходимость получения выбранного сигнала, выбирая между исследованием воздушной и костной проводимостью, а также задавая интенсивность и частоту сигнала.

2. Микроконтроллер на встроенном ЦАПе выдает импульсный сигнал с заданной частотой и заданным размахом напряжения.

3. Сигнал микроконтроллера попадает на повторитель напряжения для разделения силовой и управляющей части устройства.

4. На первом Д-мультиплексоре сигнал направляется на один из полосовых фильтров (в зависимости от частоты). Д-мультиплексором управляет контроллер, задавая необходимый адрес.

5. На активном полосовом фильтре высшие гармоники и постоянная составляющая импульсного сигнала отфильтровываются. На выходе получаем синусоиду, соответствующую основной гармонике неотфильтрованного сигнала (при необходимости ее можно усилить).

6. На втором Д-мультиплексоре сигнал направляется либо на костный вибратор, либо на аудиовыход, в зависимости от выбранного режима. Д-мультиплексором управляет контроллер, задавая необходимый адрес.

7. Частота и уровень выбранного сигнала отображаются на индикационной панели, состоящей из 15 светодиодов.

Создание портативного и дешевого аудиометра позволит избавить отоларингологов от зависимости от диагностического кабинета и даст возможность быстро и оперативно поставить диагноз пациенту, что является большим шагом в победе над болезнью.

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Словари и энциклопедии на Академике http://dic.academic.ru/ статья: Аудиометрия.

2. Кочкин Р.В. Импедансная аудиометрия. М.: МедЛит, 2006. 48 с.

РАЗРАБОТКА АЛГОРИТМОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБРАБОТКИ ФОРМООБРАЗУЮЩЕЙ МОДЕЛЬНОЙ ОСНАСТКИ

В.М. Давыдов, д.т.н., профессор. зав. кафедрой;
А.В. Никитенко, аспирант, А.А. Прокопенко, магистрант
каф. ТИИС; Чан Ен Нам, стажер, КНДР
г. Хабаровск, Тихоокеанский государственный университет

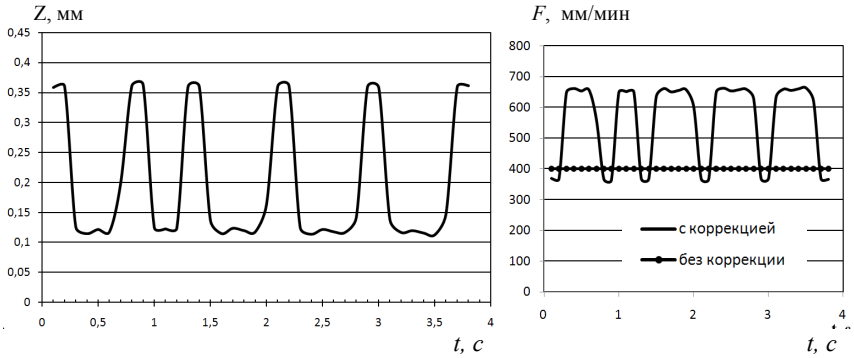
Повышение уровня автоматизации технологических процессов в машиностроительном производстве в значительной степени определяется использованием современных программных средств при проектировании технологических переходов обработки деталей на станках с числовым программным управлением [5]. Особенно это актуально для

формообразующих элементов модельной оснастки, обработка которой отличается повышенными требованиями к точности и производительности металлорежущего оборудования.

В работе предложена методика коррекции управляющих программ для станков с ЧПУ, позволяющая снизить время обработки, повысить качество обрабатываемых поверхностей и стойкость металлорежущего инструмента.

Формообразующие элементы технологической оснастки, используемой при производстве малогабаритных изделий методами точного литья, как правило, изготавливаются из модельных материалов методом гравирования. При этом послойная обработка, которая применяется при изготовлении крупногабаритной формообразующей оснастки, не находит применения в связи с низкой производительностью процесса гравирования. Однако сложность поверхностей приводит к тому, что величина срезаемого слоя в единицу времени оказывается непостоянной и имеет ряд пиков, связанных с резким изменением глубины обработки (рис. 1, *а*).

Высокая неравномерность припуска может привести к возникновению вибраций, снижению качества обработки и даже поломке инструмента [4]. Для снижения влияния неравномерности припуска предложена методика коррекции подачи в зависимости от глубины резания в текущей точки траектории (рис. 1, *б*). С учетом коррекции неравномерность величины срезаемого слоя в единицу времени снижается в 2 раза и более (рис. 2); время обработки также снижается на 10–50%. В основе алгоритма коррекции лежит анализ управляющей программы для станка с ЧПУ и модификация кода путем расчета более эффективной подачи режущего инструмента.



а *б*

Рис. 1. Зависимость глубины резания от времени на участке траектории (*а*); *б* – зависимость минутной подачи от времени

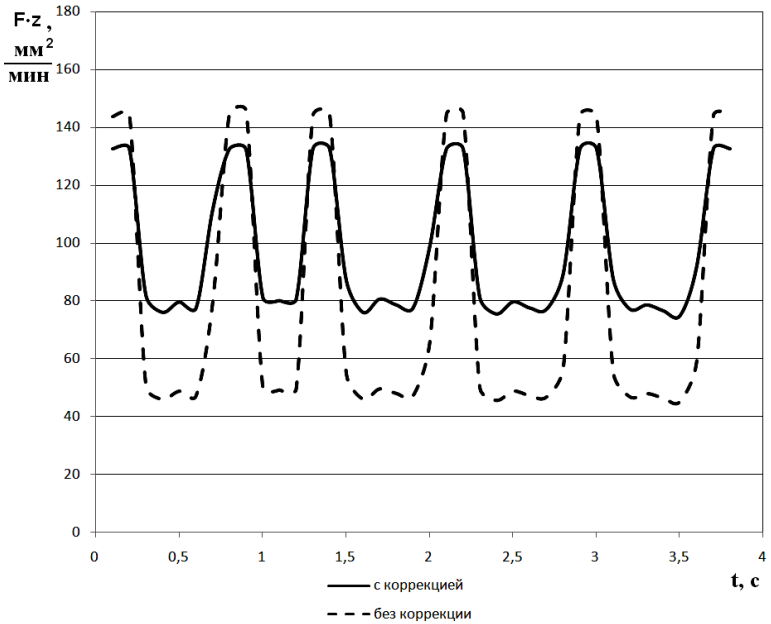


Рис. 2. Зависимость величины срезаемого слоя в единицу времени без коррекции подачи и с коррекцией подачи

Оценка эффективности предложенного алгоритма подтверждена экспериментами по измерению составляющих силы резания при обработке моделей из полиметилметакрилата на гравировально-фрезерном станке Alfa 30×30 фирмы Cielle (Италия). Снижение сил резания при использовании коррекции управляющей программы по сравнению с программой генерируемой CAM-системой составило около 40%.

Кроме экспериментальных методов большой интерес представляют имитационные модели, позволяющие предсказать поведение сложных динамических систем без проведения трудоемких экспериментов. Для характеристики динамических процессов часто используются методы нелинейной динамики, которые позволяют давать оценку устойчивости сложных процессов. Одним из наиболее важных показателей является показатель Ляпунова, который является точной характеристикой степени сложности хаотического поведения и структуры аттрактора в фазовом пространстве динамической системы. Показатель можно задать выражением [1, 2]:

$$\lambda_1 = \lim_{\substack{t\to\infty \\ d(0)\to 0}} \left(\frac{1}{t}\right) \log_2 \left[\frac{d(t)}{d(0)}\right].$$

Самым значимым является максимальный ляпуновский показатель, положительность которого свидетельствует о существовании хаоса в системе [3].

$$\lambda_{\max} = \sum_{k=0}^{k-1} \ln\left(\frac{\varepsilon'_k}{\varepsilon_k}\right) \Big/ \sum_{k=1}^{k} T_k . \qquad (1)$$

Для оценки динамических характеристик процесса обработки формообразующей модельной оснастки проведен анализ фазовой траектории компонент скорости подачи на трехкоординатном гравировально-фрезерном станке. Расчет старшего показателя Ляпунова производился по формуле (1). Для фазовой траектории компонент скорости подачи после коррекции управляющей программы показатель Ляпунова снизился с величины 2,67 до 2,09, что свидетельствует о снижении сложности хаотического движения и повышении динамической устойчивости системы.

ЛИТЕРАТУРА

1. Малинецкий Г.Г., Потапов А.Б. Современные проблемы нелинейной динамики. М.: Эдиториал УРСС, 2000. 336 с.

2. Мун Ф. Хаотические колебания. М.: Мир, 1990. 312 с.

3. Michael T. Rosenstein, James J. Collins. A practical method for calculating largest Lyapunov exponents from small data sets. Boston: University, 1992.

4. Биленко С.В. Повышение эффективности высокоскоростной механической обработки на основе подходов нелинейной динамики и нейронно-сетевого моделирования: Дис. … д.т.н. Комсомольск-на-Амуре, 2006. С. 163–169.

5. ArtCAM Pro – Artistic CADCAM Software [Электронный ресурс] / Delcam plc 2007. Режим доступа: http://www.artcampro.com/about/whatispro.htm , свободный. Загл. с экрана.

АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПОДСИСТЕМЫ АНАЛИЗА ТЕКСТОВОЙ ИНФОРМАЦИИ СИСТЕМЫ «ПУАРО»*

М.А. Молчанов, О.О. Осипова, студенты 4-го курса

г. Томск, ТУСУР, каф. КИБЭВС, scintilla@mail2000.ru

В рамках группового проектного обучения разрабатывается система «Пуаро». Это автоматизированная система поиска, анализа и принятия решений, необходимая для предоставления информации пользователям и помощи в принятии решений в каком-либо вопросе, исходя из полученной информации в сети Интернет.

* Выполнено в рамках проекта ГПО КИБЭВС-0701 – Автоматизированная система поиска, анализа и принятия решений «Пуаро».

Данная система представляет собой сложный механизм, включающий в себя ядро программы, базу данных для хранения найденной информации, модуль анализа данных и модуль принятия решений. Принцип работы «Пуаро» заключается в следующем: система обращается с запросом пользователя в сеть Интернет, полученную информацию сравнивает с тематическими словарями, анализирует по необходимым критериям (синтаксис предложений, тональность текста). Затем следует процесс принятия решений, который подразумевает сложный алгоритм анализа имеющейся информации.

Под сложным алгоритмом понимается включение в него достаточного количества методов анализа текстовой информации, чтобы подготовить данные для принятия решений.

Важным фактором для анализа информации является тональность текста. Тональность является комплексной текстовой категорией первой степени, представленной парадигмой основных стилистических тональностей (лирической, драматической и т.п.). данный подход позволяет распознать позитивное или негативное отношение автора текста к описываемому объекту и выявить составляющие образа объекта в тексте, которые формируют определенную окраску по признаку «позитив/негатив».

Метод анализа тональности текста содержит в себе следующие шаги:

1) Распознавание всех упоминаний о целевом объекте в тексте, включая его полные, краткие, косвенные, местоименные и другие обозначения.

2) Отсев и полный синтаксический разбор конструкций, в которых отражаются все события и признаки, связанные с целевым объектом.

3) Выделение и классификация конструкций, в которых явно выражается тональность и описываются эмоционально-коннотативные события.

4) Для каждой конструкции принятие решения о тональности «позитив/негатив» с учетом мест, которые занимают в ее составе эмоционально-коннотативные, тональные и нейтральные слова, а также средства выражения отрицания и инверсии смысла «Х якобы не отказался от авантюрной идеи».

5) Заключительный шаг – обработка результатов. Основным утилитарным результатом является формирование частотного портрета всех позитивных и негативных событий, связываемых с образом объекта в информационном поле.

Существует ряд схем проведения оценки тональности текста. К ним относятся явная тональная характеристика, прямая эмоционально-коннотативная характеристика, ассоциированный эмоциональный коннотат.

Далее будет предложена методика принятия решений о тональности. Она включает в себя следующие шаги:

1) При наличии хотя бы одного слова с негативной тональностью общая тональность участника негативна; в противном случае общая тональность позитивна, если присутствует хотя бы одно слово с позитивной тональностью.

2) При оценке тональности каждого участника ситуации необходимо учесть наличие при нем слов, которые инвертируют тональность: частиц, наречий, прилагательных и некоторых глаголов. Показатели инверсии часто могут употребляться совместно, причем четное количество инверсий эквивалентно отсутствию таковой, а нечетное есть инверсия.

3) В ситуациях, выраженных предикативной конструкцией, показатели тональности и отрицание могут быть выражены не при главном, а при дополнительном предикате (который и сам по себе может выражать отрицание).

4) Влияние показателей отрицания на тональность отдельных слов необходимо просчитывать до применения указанного выше принципа получения результирующей тональности участников факта. Исключением является случай, когда показатель инверсии стоит на самом целевом объекте: «*не президент отвечает за*...», что инвертирует общую окончательную оценку тональности ситуации.

Данная методика позволит существенно облегчить задачу принятия решений. Реализация данного алгоритма находится в стадии разработки.

ЛИТЕРАТУРА

1. «Проект ВААЛ»: http://www.vaal.ru/

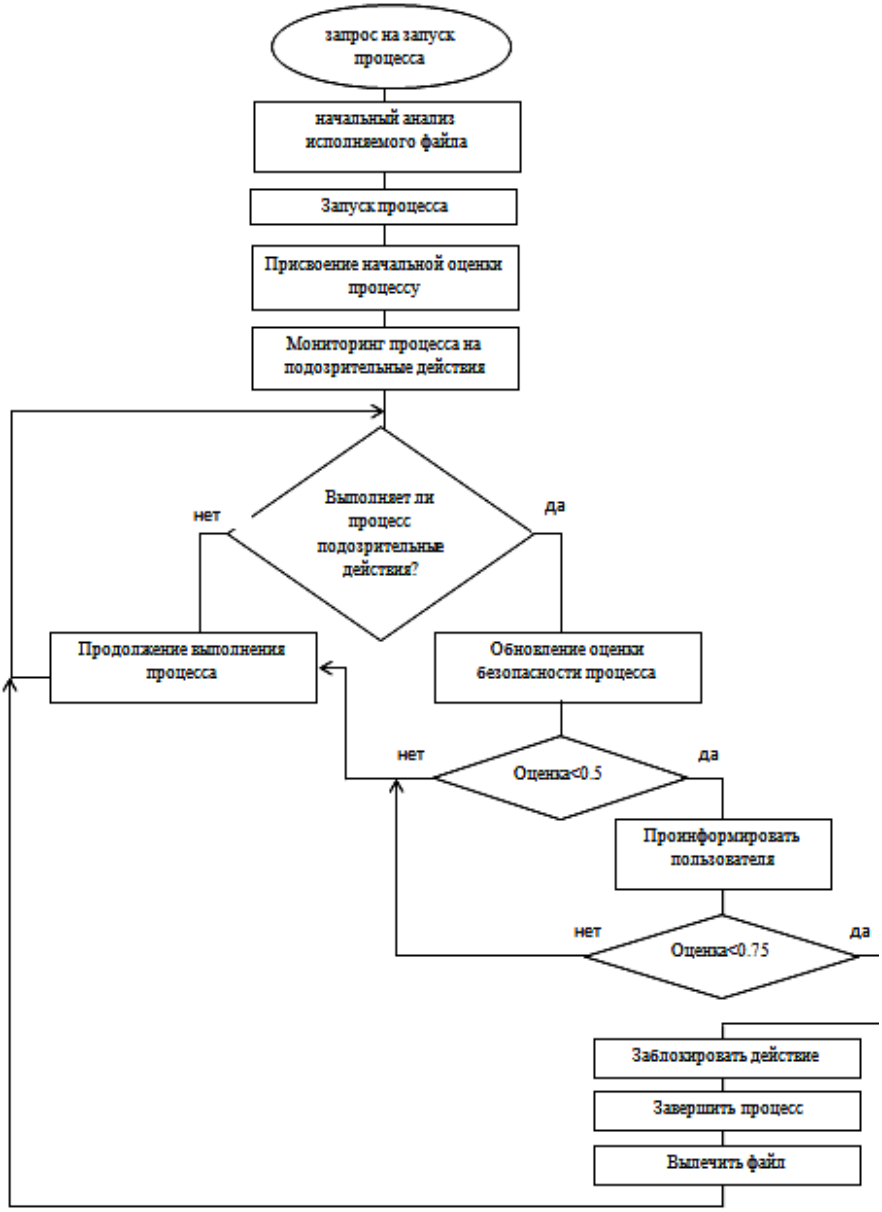
ЭКСПЕРТНАЯ СИСТЕМА ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ И АНТИВИРУСОВ

Ю.А. Парфенов, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, maelstrom254@gmail.com

Эвристический анализ – это механизм обнаружения вирусов и программных закладок, при котором антивирусный сканнер контролирует все действия, выполняемые потенциальной вредоносной программой. В процессе эвристического анализа проверяются потенциально опасные действия, характерные для вирусов и программных закладок.

Алгоритм антивирусной защиты приведен на рисунке.



Алгоритм мониторинга работы процессов

В современных компьютерах предусматриваются программные средства защиты как прикладного программного обеспечения, так и операционных систем. Большинство известных антивирусных систем используют эвристический механизм антивирусного мониторинга, основанный на контроле выполняемых программами операций при их запуске на исполнение, а также механизм антивирусного сканирования, сводящийся к поиску в программных файлах известных вирусов по их сигнатурам.

Методы эвристического анализа не обеспечивают гарантированной защиты от новых, отсутствующих в сигнатурном наборе компьютерных вирусов, что объясняется использованием в качестве объекта анализа сигнатур ранее известных вирусов, а в качестве правил эвристической проверки – знаний о механизме полиморфизма сигнатур. Невозможно полностью исключить ложные срабатывания, поскольку этот метод поиска базируется на эмпирических предположениях.

В основу развиваемой в данном проекте системы антивирусной защиты положена так называемая технология «интеллектуального сканирования» опасных функций программного обеспечения, основывающаяся на методическом аппарате эвристического анализа и искусственного интеллекта.

Технология подразумевает:

– экспертный анализ системой искусственного интеллекта файлов программного обеспечения на предмет наличия в них опасных функций, а также вирусов и программных закладок;

– проверку выявленных опасных функций программного обеспечения на основе соответствующей базы знаний;

– формирование логического вывода об обнаруженных свойствах вирусов и программных закладок;

– автоматическое формирование алгоритмов лечения файлов.

В отличие от известных антивирусных программ, разрабатываемая экспертная система основывается не на поиске известных вирусов и анализе процесса выполнения программ, а на качественно новой концепции – анализе функций программ без их выполнения.

Научный руководитель – Е.М. Давыдова, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Нейлор К. Как построить свою экспертную систему. М.: Энергоатомиздат, 1991. 345 с.

2. Нильсон Н. Д.. Искусственный интеллект. Методы поиска решений. М.: Мир, 1973. 412 с.

3. Сафонов В.О.. Экспертные системы – интеллектуальные помощники специалистов. СПб.: Санкт-Петербургская организация общества «Знания» России, 1992. 337 с.

4. Таунсенд К., Фохт Д. Проектирование и программная реализация экспертных систем на персональных ЭВМ. М.: Финансы и статистика, 1990. 345 с.
5. Убейко В. Н.. Экспертные системы. М.: МАИ, 1992. 218 с.

СОЗДАНИЕ ИНТЕРНЕТ-АНАЛОГОВ ЛОКАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

М.Д. Пудалов, аспирант
г. Томск, ТУСУР, каф. АСУ, maksim-pudalov@yandex.ru

Облачная обработка данных – это парадигма, в рамках которой информация постоянно хранится на серверах в сети Интернет и временно кэшируется на клиентской стороне.

Подобная архитектура обеспечивает ряд преимуществ как для конечного пользователя, так и для производителя программного обеспечения, среди которых:

1. Снижение расходов на установку и сопровождение программного обеспечения, устанавливаемого на компьютер пользователя.
2. Отсутствие зависимости от операционной системы.
3. Высокая степень защиты от нелицензионного использования программного обеспечения.
4. Возможность предоставления гибких тарифов оплаты.
5. Пользователь всегда имеет доступ к последней версии программного обеспечения, не обновляя его.

Хотя использование подобной архитектуры ведет за собой явные преимущества и такие крупные компании, как Google и Microsoft, уже начали активно её использовать, тем не менее есть ряд проблем, мешающих повсеместному распространению Cloud Computing. И хотя самые насущные из них не относятся к сфере программирования и не являются предметом данной работы, есть ряд технических проблем. Одной из них является возможность создания веб-приложений, полностью повторяющих функции программных продуктов, устанавливаемых на компьютеры пользователей. На этой проблеме остановимся подробнее.

Для начала проанализируем инструменты, находящиеся в распоряжении современного веб-разработчика. На стороне сервера мы можем использовать большое количество языков программирования, среди которых C++, Java, PHP, C#, а также любое программное обеспечение, которое сможем установить. Таким образом, серверная часть не накладывает существенных ограничений на функционал конечного программного продукта.

Однако с клиентской частью всё обстоит несколько иначе.

Разрабатывая интерфейс пользователя, мы вынуждены ориентироваться на популярные тонкие клиенты, предназначенные для работы с сетью Интернет, среди которых Internet Explorer 6,7, Mozilla Firefox 3.x, Opera 9.x, Google Chrome. Они способны работать с языком гипертекстовой разметки HTML, каскадными таблицами стилей CSS и скриптовым языком программирования JavaScript. Данные передаются и принимаются по протоколам http [2] и HTTPS.

Первой и наиболее очевидной проблемой является избыточность языка HTML. Обновляя страницу, пользователь, помимо полезных, получает большое количество паразитных данных, касающихся отображения информации на странице. Частично эту проблему можно решить, активно используя CSS, поскольку файл, в котором содержатся таблицы стилей, загружается один раз, после чего кэшируется браузером. Однако процент служебной информации всё равно будет достаточно большим.

Полное решение проблемы заключается в использовании JavaScript и AJAX – запросов, которые позволяют получить информацию с сервера, не обновляя страницу. После получения информации, используя JavaScript, мы можем изменить страницу любым образом. Для передачи данных мы можем использовать как какой-либо собственный формат, так и достаточно экономичный формат JSON.

Вторая проблема – это защита информации. По протоколу HTTP данные передаются в открытом виде и могут быть перехвачены. Решением этой проблемы является использование протокола HTTPS, который предоставляет достаточно возможностей для безопасной передачи данных между клиентом и сервером.

Третий подводный камень – это различная интерпретация браузерами HTML, CSS, JavaScript кода. Данная проблема решается использованием современных стандартов HTML, таких как XHTML [3, 4] 1.0, 1.1, и использованием таких JavaScript-framework'ов, как jQuery.

Из всего вышеперечисленного можно сделать вывод, что все, или подавляющее большинство технических проблем, связанных с созданием Интернет-аналогов локального программного обеспечения, являются решаемыми и распространение концепции Cloud Computing сдерживают только проблемы, не связанные с техникой, такие как доверие к подобным системам или различные юридические вопросы.

ЛИТЕРАТУРА

1. Cloud computing [Электронный ресурс] / Википедия. Свободная энциклопедия. 2009. Режим доступа: http://en.wikipedia.org/wiki/Cloud_computing, свободный.

2. HTTP – Hypertext Transfer Protocol Overview / w3c. Режим доступа: http://www.w3.org/Protocols/, свободный

3. XTML 1.0: The Extensible HyperText Markup Language (Second Edition) / w3c. Режим доступа : http://www.w3.org/TR/xhtml/, свободный

4. XTML 1.1 – Module – based XHTML / w3c. Режим доступа: http://www.w3.org/TR/xhtml1/, свободный.

ПРИМЕНЕНИЕ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ ПРИ ОРГАНИЗАЦИИ ПРОИЗВОДСТВЕННОГО ПРОЦЕССА НА ПРЕДПРИЯТИИ

Е.А. Родин, инженер ФГУП «НИИ Квант»

г. Москва, ФГУП «НИИ Квант», earodin@rambler.ru

В настоящее время современные вычислительные системы и компьютерные сети позволяют накапливать большие массивы данных для решения задач обработки и анализа. К сожалению, сама по себе машинная форма представления данных содержит информацию в скрытом виде и для ее извлечения нужно использовать специальные методы анализа данных [1].

Информационно-аналитическая система (ИАС) – это система, обладающая средствами ввода, хранения и анализа данных, относящихся к определенной предметной области, с целью поиска решений (рис. 1).

Постоянное накопление данных приводит к непрерывному росту их объема. В связи с этим на систему ложится задача обеспечения надежного хранения больших объемов информации. Также на систему могут быть возложены задачи предотвращения несанкционированного доступа, резервного хранения, архивирования и т.п.

По степени «интеллектуальности» обработки данных при анализе выделяют три основных класса задач анализа:

– информационно-поисковый – система осуществляет поиск необходимых данных, характерной чертой такого анализа является выполнение заранее определенных запросов;

– оперативно-аналитический – система производит группирование и обобщение данных в любом виде, необходимом аналитику, в отличие от информационно-оискового анализа в данном случае невозможно заранее предсказать необходимые аналитику запросы;

– интеллектуальный – система осуществляет поиск функциональных и логических закономерностей в накопленных данных, построение моделей и правил, которые объясняют найденные закономерности.

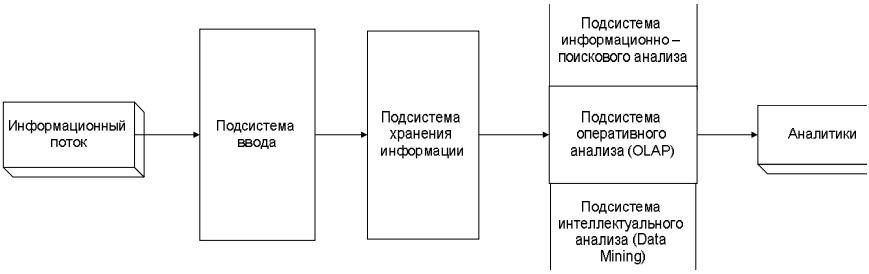


Рис. 1. Архитектурная схема ИАС

Подсистема анализа может быть построена на основе:

– подсистемы информационно-поискового анализа на базе реляционных СУБД и статистических запросов с использованием языка SQL;

– подсистемы оперативного анализа, для реализации таких подсистем применяется технология оперативной аналитической обработки данных OLAP (процесс анализа данных в реальном масштабе времени), использующая концепцию многомерного представления данных;

– подсистемы интеллектуального анализа, данная подсистема реализует методы и алгоритмы Data Mining.

Knowledge Discovery in Databases (KDD) – это процесс поиска полезных знаний в «сырых» данных [2]. KDD включает в себя вопросы подготовки данных, выбора информативных признаков, очистки данных, применения методов «раскапывания данных» (Data Mining), а также обработки и интерпретации полученных результатов.

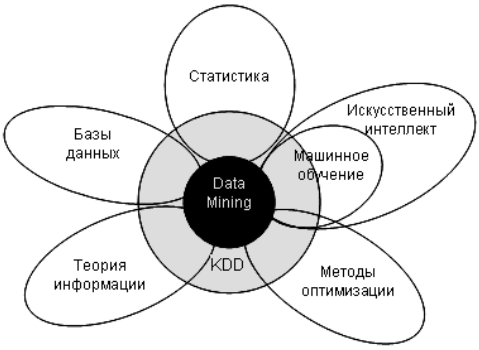


Рис. 2. Мультидисциплинированность ИАД

Центральным элементом этой технологии являются методы Data Mining, позволяющие обнаруживать знания при помощи математических правил.

ИАД стал очередной ступенью после OLAP в развитии анализа в реляционных базах данных и информационных хранилищах [3] (рис. 2).

Появившиеся методы ИАД позволяют проводить глубинные исследования больших объёмов данных с целью поиска и выведения скрытых и неочевидных закономерностей. В отличие от OLAP, где за-

дается определенный параметр поиска или проверяется заранее установленное предположение, ИАД позволяет находить новые, еще неизвестные, но существующие гипотезы и взаимосвязи [4].

В основу современной технологии ИАД положена концепция шаблонов (паттернов), отражающих фрагменты многоаспектных взаимоотношений в данных [5]. Эти шаблоны представляют собой закономерности, свойственные подвыборкам данных, которые могут быть компактно выражены в понятной человеку форме. Поиск шаблонов производится методами, не ограниченными рамками априорных предположений о структуре выборки и виде распределений значений анализируемых показателей.

В целом технологию добычи данных достаточно точно определяет Григорий Пиатецкий-Шапиро [6] – один из основателей этого направления. Добыча данных – это процесс обнаружения в сырых данных.

ИАД является мультидисциплинарной областью, возникшей и развивающейся на базе достижений прикладной статистики, распознавания образов, методов искусственного интеллекта, теории баз данных и др.

ЛИТЕРАТУРА

1. Барсегян А.А., Куприянов М.С., Степаненко В.В., Холод И.И. Методы и модели анализа данных: OLAP и Data Mining. СПб.: БХВ-Петербург, 2004. 336 с.

2. Дюк В.А., Самойленко А.П. Data Mining: Учеб. курс. СПб.: Питер, 2001. 368 с.

3. Han J., Kamber M. Data Mining: Concepts and Techniques, Morgan Kaufmann Publishers. Chapter 1. 2000.

4. Буров К. Обнаружение знаний в хранилищах данных // Открытые системы. 1999. №05–06.

5. Карпов Л.Е., Юдин В.Н. Методы добычи данных при построении локальной метрики в системах вывода по прецедентам / РАН. 2007. http://www.citforum.ru/consulting/BI/data_mining/.

6. Fayyad U., Piatetsky-Shapiro G., Smyth P. «From Data Mining to Knowledge Discovery: An Overview // Advances in Knowledge Discovery and Data Mining (Eds. U.M. Fayyad, G. Piatetsky-Shapiro, P. Smyth). Cambridge, Mass: MIT Press, 1996. P. 1–34.

СОЗДАНИЕ ИССЛЕДОВАТЕЛЬСКОГО РОБОТА*

И.И. Шиляев, студент 3-го курса
г. Томск, ТУСУР, каф. КИБЭВС, virtualist@sibmail.com

Проблема роботов в человеческом мире возникла сразу же с появлением первого робота. Футуристические фантазии рисовали различные варианты интеграции роботов в человеческий мир, от войны с роботами до слияния робота и человека в единое целое. Но даже с развитием технологий такой конфликт до сих пор кажется далеким и недостижимым.

Создание любого робота является интересной, творческой задачей. Мы же поставили перед собой задачу создать исследовательского робота, который позволит понять основные принципы робототехники, а также поможет учащимся в учебном процессе. Для этой цели достаточно создать программируемого робота с несколькими датчиками. Кроме того, создание такого робота позволит понять и изменить других роботов как на программном, так и на конструктивном уровне.

Но все-таки интересно представить план создания практически любого робота.

Простейшую модель робота может собрать практически любой человек, обладающий лишь небольшими навыками в построении конструкций РЭС. Простота технологического процесса может вызвать удивление у тех, кто впервые столкнулся с такой задачей, ведь даже механизм, собранный из пары резисторов и одной микросхемы, с парой-ройкой движущих элементов, уже может быть назван роботом. Правда, такая модель не умеет думать и реагировать на какие-либо изменения.

Более сложные системы содержат и более сложные конструкции, и программируемые элементы. Так, внедрение всего одного микроконтроллера позволит значительно расширить функциональность робота и спектр задач, выполняемых с его помощью. Такой робот умеет думать, но по-прежнему безучастен к окружающему миру.

Программирование процессоров робота производится посредством различных программ и приложений. Это могут быть и несложные оконные программы, и различные языки программирования различных уровней. Наиболее популярными являются RoboBasic и RobotC, которые являются двойниками бэйсика и C++, с небольшими модификациями, но и любители языка типа Ассемблер смогут найти несколько программ, которые позволят не переучиваться на C++. Кроме того, в

* Выполнено в рамках проекта ГПО КИБЭВС-0845 – Управление объектами с использованием мобильной связи.

последнее время выходит множество приложений, которые позволяют программировать действия робота без каких-либо знаний языков программирования.

К недостатку программных приложений следует отнести их труднодоступность, так, за достаточно простую программу придется серьезно потратиться, что делает их недоступным широкому кругу конструкторов.

Но ведь только двигаться, пусть и по программе, недостаточно. Робот должен владеть некой самостоятельностью, а для этого он должен иметь «органы восприятия». Эта задача решается достаточно просто, стоит лишь добавить в конструкцию несколько датчиков, и робот начинает «видеть», «слышать», «осязать» и даже разговаривать. Простейшие конструкции лишь распознают уровень звука, степень освещенности и наличие прикосновения, нажатия. Более сложные датчики распознают речь, различают цвета и даже могут оценить расстояние до объекта [1].

Более сложные модификации роботов чуть ли не дублируют человека, или же являются сложными механическими устройствами узкого радиуса применения, например промышленные роботы.

Создание такого робота может послужить и поводом и толчком для создания робота узкой специализации, который сможет помочь человеку или заменить его в какой-либо профессиональной деятельности.

Нами уже разработан и собран прототип робота на одной микросхеме. Кроме того, разработана модель робота на микропроцессоре. Ведется поиск идей для создания датчиков и окончательной модели робота.

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

ЛИТЕРАТУРА

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

ОБЗОР КОНТРОЛЛЕРОВ ДЛЯ СИСТЕМЫ «УМНЫЙ ДОМ»

Д.С. Сиргаева, И.С. Бузмаков, студенты 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, bagira162@mail.ru

Умный дом (Smart House) – это интеллектуальная система управления, обеспечивающая согласованную и автоматическую работу всех инженерных сетей дома. Такая система грамотно распределяет ресурсы, снижает эксплуатационные затраты и обеспечивает понятный ин-

терфейс контроля и управления. Главным элементом системы является контроллер [1].

Системы «Умный дом» строятся на базе промышленных свободно программируемых логических контроллеров. Идея такой системы состоит в том, чтобы снять интеллектуальные функции с оконечных устройств автоматики «Умного дома» (датчиков и активаторов) и использовать одно интеллектуальное устройство для множества простых и дешёвых устройств (обычных выключателей, обычных реле и т.д.). За счёт этого приобретаем экономическую выгоду и возможность применения сложных алгоритмов, доступных ранее только в промышленности. Программируемый логический контроллер (ПЛК) – специализированный цифровой компьютер, используемый для автоматизации технологических процессов. В отличие от компьютеров общего назначения, ПЛК имеют развитые устройства ввода-вывода сигналов датчиков и исполнительных механизмов, приспособлены для длительной работы без серьёзного обслуживания, а также для работы в неблагоприятных условиях окружающей среды. ПЛК являются устройствами реального времени [2].

На российском рынке широко представлены программируемые логические контроллеры, используемые для автоматизации зданий, различных производителей. Рассмотрим контроллеры следующих компаний: Honeywell, Johnson Controls, Siemens и WAGO.

Линейка контроллеров Honeywell представлена как несложными по своей функциональности контроллерами, решающими определённые локальные задачи, так и мощными контроллерами с распределённой системой ввода-вывода сигналов.

Отказавшись от шины CCBus собственной разработки, компания стала поддерживать широко распространённую шину LonWorks. Такое решение позволило использовать её контроллеры с устройствами других производителей, совместимыми с шиной LonWorks.

Johnson Controls (JC) – американская компания с многолетней историей деятельности в области автоматизации зданий. В связи с тем, что политика JC подразумевает полное неразглашение информации о своих технических продуктах, говорить о каких-либо «плюсах» и «минусах» контроллеров не представляется возможным. Ясно одно – внесение больших изменений в функции или перечень подключаемого оборудования потребует серьёзной переработки проекта, может даже повлечь необходимость выезда представителей фирмы на объект для перенастройки оборудования и изменения архитектуры. Это, в свою очередь, повлечёт за собой немалые денежные затраты заказчика. Фактически покупатель приобретает чёрный ящик с набором входов и выходов, что не может не настораживать. Кроме того, практически все

датчики, выпускаемые JC, невозможно использовать совместно с оборудованием других производителей.

В АСУ ТП давно и широко применяются контроллеры Siemens семейств SIMATIC S7 и LOGO!. Они хорошо зарекомендовали себя благодаря высокой надёжности, гибкости и простоте программирования. Эти универсальные контроллеры применяются и для автоматизации зданий, как правило, для решения сложных задач управления крупными инженерными системами торговых и производственных помещений. В то же время корпорация Siemens предлагает гамму изделий, специально предназначенных для автоматизации зданий. Направлением автоматизации инженерных и офисных систем зданий занимается подразделение Siemens Building Technologies, которое в настоящее время активно продвигает систему автоматики и управления для зданий DESIGO™. Эта система может быть подразделена на три уровня: уровень оборудования, уровень автоматизации, уровень управления. Благодаря идеологии распределённой системы управления каждый уровень может функционировать как отдельно, так и в составе комплексной системы.

Семейство контроллеров DESIGO™ PX представлено свободно программируемыми контроллерами двух типов: компактными с интегрированными входами и выходами и модульными с внешними сигнальными модулями. Также в системе есть панели оператора, интернет-контроллеры и специализированные контроллеры для интеграции контроллеров других производителей.

Система на базе контроллеров WAGO I/O имеет концепцию построения, характерную скорее для промышленной автоматики, чем для систем автоматизации зданий. Эта концепция подразумевает использование как программируемых, так и пассивных базовых контроллеров со свободно формируемым набором сигнальных модулей. Программируемые и пассивные базовые контроллеры могут связываться с системой диспетчеризации при помощи самых разнообразных интерфейсов: Ethernet TCP/IP, PROFIBUSSDP, LonWorks, ModBus, CANbus и пр. Гибкость системы позволяет минимизировать затраты на реализацию, так как нет необходимости приобретать отдельные специализированные элементы для управления тем или иным оборудованием.

Контроллеры и сигнальные модули компактны, что позволяет компоновать весьма сложные системы автоматики в шкафах небольших размеров.

Несомненным плюсом систем WAGO I/O является возможность сопрягать контроллеры практически с любым оборудованием сторонних производителей как нижнего, так и верхнего уровней [3].

В заключение можно сказать, что на рынке автоматизации зданий ещё распространены закрытые решения, ничем не оправданные «фир-

менные» секреты, за которыми зачастую скрывается просто техническое несовершенство продукции. Выбирая аппаратную платформу, необходимо не только смотреть на рекламные заявления типа «Мы – лидеры рынка автоматизации зданий», а внимательно проверять полноту и доступность технической информации и технической поддержки.

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

ЛИТЕРАТУРА

1. Компания «Intellecthouse»: Автоматизация вашего дома [Электронный ресурс]. Режим доступа: http://www.intelecthouse.ru/

2. Википедия [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/Программируемый_логический_контроллер

3. Журнал «Современные технологии автоматизации» [Электронный ресурс]. Режим доступа: http://cta.ru/

ИНТЕРФЕЙС ЛАБОРАТОРНОГО ПРАКТИКУМА НА ПЛАТФОРМЕ ОС LINUX

Д.М. Слепнёв, студент 5-го курса;
Л.А. Торгонский, науч. рук., доцент
г. Томск, ТУСУР, каф. КИБЭВС, slepnev88@mail.ru

Одним из направлений снижения потерь времени на организационные этапы выполнения работ является рациональная организация рабочего места исполнителя. Для работ, выполняемых с применением компьютера, а лабораторный цикл по дисциплине «Микропроцессорные ЭВС» [1] на базе учебного стенда SDK-1.1 [2] не может быть исполнен без персонального компьютера (ПК) по принципу постановки, необходима удобная сервисная среда, так называемый дружественный интерфейс для исполнителя. Разнообразие аппаратных ресурсов учебного стенда в сочетании со спецификой состава сопутствующего резидентного программного обеспечения актуализирует задачи разработки сервисной среды проведения лабораторного цикла по дисциплине.

Выполнение лабораторных работ связано с процессами подготовки, редактирования программ управления, трансляции текстов программ, устранения ошибок, подготовки, загрузки исполняемого кода в память стенда, отладки программ с отменами и повторами запуска. Материалами, применяемыми в процессе выполнения работ, являются текстовые описания, сведения и сами модули исходных текстов, из которых может компоноваться исходный текст программ к трансляции. Штатные ресурсы стенда предусматривают загрузку программ в память стенда по протоколу RS232C через последовательный порт компьютера

с помощью инструментальных средств T167B (либо T2), работающих в среде DOS. Анализ и декомпозиция задач интерфейса лабораторного практикума позволяют сделать вывод о целесообразности разделения графических форм на две группы;

– управляющие;

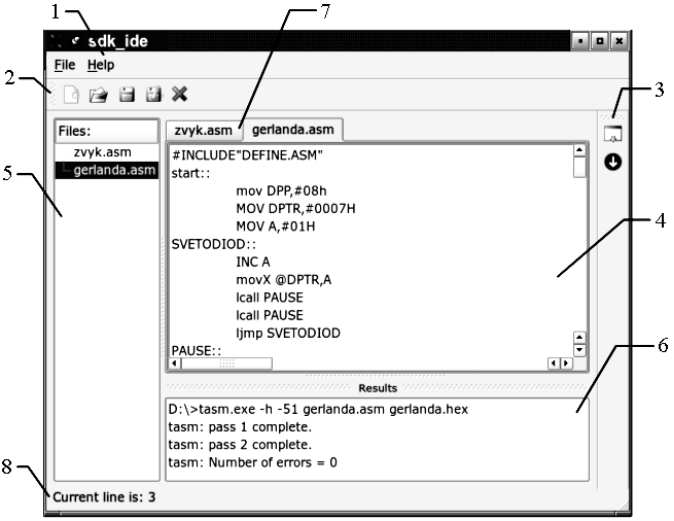
– информационно-справочные.

К первой группе относятся кнопки перехода по перечисленным ранее процессам с использованием справок помощи, взаимодействия с библиотекой рабочих материалов.

Во вторую группу относятся кнопки выбора справочных материалов в библиотеке материалов или подсказок по составу практикума, по расположению описаний, пояснения по необходимости и т.д.).

В связи с рядом обстоятельств, не обсуждаемых в работе, в качестве операционной системы (ОС) для проектирования интерфейса принята ОС Linux.

Форма графического интерфейса лабораторного практикума изображена на рисунке. Предложения формы, представленные восемью полями, поддерживают необходимые операции по процессу выполнения лабораторного практикума. Поле *1* содержит меню кнопок «File», «Help».



Интерфейс лабораторного практикума

Поле кнопок *2* дублирует операции с файлами, имеющимися в ниспадающем меню предложений по нажатии кнопки «File» (– кнопка создания нового файла текста программы; – кнопка откры-

тия имеющегося файла программы;  – кнопка сохранения редактируемого файла;  – кнопка сохранения файла под другим именем;  – кнопка закрытия редактируемого файла). Поле *3* с кнопками ( – трансляции редактируемого файла и  – загрузки программы в стенд) для действий по трансляции и загрузке программ в стенд. Поле *4* отведено для работы с редактируемым текстом программы. В поле *5* формы отображается список открытых файлов. В поле *6* отображаются результаты трансляции и загрузки программы. Поле *7* отведено под вкладки для переключения (по сигналу от кнопки мыши) между редактируемыми файлами. Поле *8* содержит строку состояния, в которой отображается номер строки во время редактирования текста программы, а также подсказки о назначении кнопок при наведении на них курсора мышью.

В результате предварительного анализа требуемых ресурсов взаимодействия с DOS-программами под управлением ОС Linux выбран пакет программ «Dosemu» для эмуляции MSDOS. Этот пакет позволяет не просто выполнять DOS-программы, в среде которых функционирует штатная инструментальная программа Т167В, но и предоставлять доступ к файловой системе и устройствам ПК.

При создании интерфейса использовались: операционная система Debian GNU/Linux, графическая библиотека Qt4, среда программирования QDevelop [5], язык программирования С++.

В процессе работы по этой теме был приобретен опыт установки ОС Linux на ПК.

Работа по рассматриваемой теме позволила приобрести практические навыки самостоятельных проектных работ с ОС Linux и создать проект приложения для отработки принятой технологии постановки практикума. Сведения об информационно-справочных материалах лабораторного практикума и доступ к ним вследствие ограничений объёма публикации планируется представить в материалах доклада на сессии.

ЛИТЕРАТУРА

1. Торгонский Л.А. Проектирование центральных и периферийных устройств ЭВС-2: Метод. указания по лабораторным работам. Томск: Изд-во ТУСУРа, 2007. 75 с.

2. Учебный стенд SDK-1.1: Руководство пользователя. М.: ООО «ЛМТ», 2006. 100 с.

3. Debian – Универсальная операционная система [Электронный ресурс]. http://www.debian.org/ Загл. с экрана.

4. Qt – Википедия [Электронный ресурс].http://ru.wikipedia.org/wiki/Qt – Загл. с экрана.

5. QDevelop – Википедия [Электронный ресурс].http://ru.wikipedia.org/wiki/QDevelop – Загл. с экрана.

ПРОЕКТИРОВАНИЕ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Д.Н. Вечерина, студентка 5-го курса
г. Томск, ТУСУР, каф. КИБЭВС, vedahsa@sibmail.com.

В данной статье будут рассмотрены основные моменты процесса проектирования локальной вычислительной сети.

За последнее десятилетие по мере появления новых технологий и роста потребностей бизнеса дизайн локальной вычислительной сети (ЛВС) непрерывно усложнялся. В настоящий момент приложения и средства коммуникаций, такие как IP-телефония, IP-видео и электронное обучение, позволяют компаниям повышать производительность.

Архитектура взаимодействия компьютеров в локальной вычислительной сети строится на стандарте Open Systems Interconnection (OSI). Каждому уровню отводится конкретная специализированная задача. Соглашения для связи одного уровня с другим называют протоколом. Процесс проектирования ЛВС условно можно разбить на составляющие, каждой из которых будет соответствовать один из первых трех уровней модели семиуровневой модели OSI.

Уровень 1 – физический, определяет параметры среды передачи данных. При проектировании ЛВС для данного уровня необходимо выбрать среду передачи данных. Это может быть витая пара, оптоволоконный кабель, коаксиальный кабель, беспроводная сеть. Исходя из небольшой стоимости, достаточно высокой пропускной способности, защищенности среды передачи, для небольших предприятий и офисных помещений наиболее часто в качестве среды передачи используется витая пара категорий 5e,6,7, что в итоге позволяет передавать информацию на скорости от 100 Мбит/с до 10 Гбит/с. Для кабельной среды передачи данных разработан стандарт кабельной сети – структурированная кабельная система – универсальная кабельная сеть, предназначенная как для построения компьютерной сети, так и для работы иных систем, например телефонной сети, пожарной и охранной сигнализации. Для СКС разработаны и внедрены ряд стандартов, на территорию России распространяется действие стандарта ISO/IEC 11801, поскольку Россия входит в состав Международной организации по стандартизации (ISO).

После выбора среды передачи выбирается топология соединения компонентов сети. Наиболее распространено 3 топологии: звезда, кольцо, общая шина. В настоящее время наиболее распространена в мире и реализована в протоколах Ethernet топология «звезда». Среда передачи и топология сети связана с уровнем 2 модели OSI-канальным. Канальный уровень отвечает за формирование кадров, управление доступом к среде. От выбранной среды передачи и топологии сети зависит протокол канального уровня. При использовании витой пары и топологии «звезда» используются протоколы Ethernet. Ethernet – наиболее

распространенный стандарт ЛВС. Сейчас спецификация Ethernet содержится в стандарте IEEE 803.3. Все протоколы IEEE 802.3 определяют параметры среды передачи данных, алгоритм доступа к среде и скорость передачи данных.

Уровень 3 – сетевой, отвечает за маршрутизацию, управление потоками данных. В настоящее время стандартом дефакта является протокол IP (internet Protocol). Другие используемые протоколы все более заменяются протоколом IP.

Далее необходимо выбрать используемое активное сетевое оборудование, поддерживающее выбранные протоколы и среду передачи, а также построить логическую схему сети, т.н. архитектуру. Множество крупных компаний, таких как IBM и Cisco, рекомендуют придерживаться иерархической или многоуровневой архитектуры ЛВС. Иерархическая (сегментированная) сеть состоит из объединенных между собой блоков, которые можно легко дублировать или изменять. Таким образом, по мере добавления или удаления одного из модулей, не нужно проектировать заново всю сеть. Благодаря тому, что сеть сегментирована, легче ею управлять, отыскивать и устранять неисправности становиться гораздо легче.

Иерархическая модель сети включает в себя три функциональных уровня: доступа (access layer), распределения (distribution layer) и магистрали (core layer).

Уровень доступа (Access Layer) образуется коммутаторами, работающими на втором уровне согласно модели OSI, а также конечными устройствами: компьютерами, телефонами, принтерами. Сетевое оборудование должно создавать виртуальные подсети, обеспечивать проверку подлинности подключаемых конечных устройств, поддерживать сервис QoS (качество обслуживания).

Уровень распределения (Distribution Layer) образуется коммутаторами, работающими на втором и третьем уровнях модели OSI. На уровне распределения обеспечивается многоуровневая коммутация между уровнем доступа и магистралью: изменение среды передачи данных, объединение множества низкоскоростных каналов в высокоскоростные магистральные каналы, проверка прав доступа рабочих групп или департаментов, резервное соединение с сетевым оборудованием уровня доступа. Кроме того, оборудование уровня распределения должно предоставлять следующие сервисы: фильтрацию проходящего трафика по адресам и портам, разделение между динамическими и статическими протоколами маршрутизации, сервис QoS (качество обслуживания).

Уровень ядра (Core Layer) образуется коммутаторами и маршрутизаторами, работающими на втором и третьем уровнях модели OSI. Уровень ядра предназначен для коммутации пакетов на максимально

возможных скоростях. Здесь должны обеспечиваться: резервирование, как информационных каналов, так и сетевых устройств, балансировка нагрузки, масштабируемость.

Объединение различных уровней иерархии на одном физическом устройстве, например уровня доступа с уровнем распределения и уровня распределения с уровнем ядра, вполне допустимо. В случае построения небольших ЛВС оно является экономически выгодным.

Для обеспечения надежности и отказоустойчивости локальных вычислительных сетей используются различные методы, как в самой топологии сети, так и при выборе телекоммуникационного оборудования. Как правило, при построении ЛВС для связи между различными уровнями в топологии сети предусматривают резервные подключения между телекоммуникационным оборудованием, причем для передачи трафика используются оба канала – основной и резервный. Кроме того, в топологии сети предусматривают установку дублирующих центральных коммутаторов уровня ядра, которые обеспечивают работу сети в случае отказа одного из коммутаторов.

В заключение можно сказать, что локальные вычислительные сети стали неотъемлемой частью современного бизнеса. При корректном проектировании ЛВС может значительно повысить эффективность бизнеса и уменьшить операционные расходы.

Научный руководитель – Г.А. Праскурин, старший преподаватель каф. КИБЭВС ТУСУР.

ЛИТЕРАТУРА

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учеб. для вузов. СПб.: Питер, 2007. 960 с.

2. Таненбаум Э. Компьютерные сети. Питер, 2007. 992 с.

АВТОМАТИЗИРОВАННЫЙ КОНТРОЛЬ ЭЛЕКТРИЧЕСКИХ ПАРАМЕТРОВ ПРИ ПРОИЗВОДСТВЕ МОНОЛИТНЫХ ИНТЕГРАЛЬНЫХ СХЕМ

М.А. Яковлев, магистрант ФЭТ

г. Томск, ТУСУР, sunman@ms.tusur.ru

Монолитная интегральная схема (МИС) – это очень сложный продукт полупроводниковой промышленности, при производстве которого перед технологами встает большой объем работы по решению различных задач.

Одной из таких задач является контроль процесса производства интегральных схем. Система тестирования в современном производстве МИС является одной из главных составляющих. Каждая её часть отвечает за контроль определенного типа параметров, например: кон-

троль параметров технологических процессов, контроль параметров структур на подложках, финальные СВЧ-измерения готовых чипов.

Особенностью производства интегральных схем является массовость изготовления. На одной полупроводниковой пластине могут находиться тысячи чипов, производство которых необходимо контролировать.

Для контроля электрических параметров используют специализированные чипы, содержащие тестовые структуры. Process control monitor (PCM) – это специальные тестовые структуры, расположенные на одном чипе, дающие информацию о параметрах изготавливаемой схемы. Тестовые данные собираются и анализируются, если данные удовлетворяют заранее определенным значениям, то пластина признается годной к дальнейшей обработке. Таких чипов намного меньше, что позволяет сократить процесс измерения. Однако объем измерений все равно большой, и его необходимо автоматизировать.

В качестве одного из решений этой задачи можно использовать полуавтоматическую зондовую станцию, которая может проводить измерения тестовых структур в автоматическом режиме. Для этого необходимо разработать специальный чип с PCM структурами, предназначенный для автоматизированного измерения на зондовой станции.

В результате проделанной работы был спроектирован требуемый чип. Был использован набор PCM структур, представленный в таблице.

Тестовые структуры

№ п/п	Название структуры	Измеряемый параметр
1	Dual tracks	Сопротивление металла, ток утечки
2	Via chains	Контактное сопротивление
3	Split cross bridge resistors	Поверхностное сопротивление
4	Конденсаторы	Емкость, напряжение пробоя
5	Резисторы	Сопротивление
6	Interdigitated layer	Ток утечки между слоями
7	Транзисторы	Параметры транзистора
8	TLM	Сопротивление омических контактов
9	Mesa test	Сопротивление изоляции

Данные структуры располагаются на чипе в виде модулей. Существуют модули для активных и пассивных элементов МИС. Контактные площадки упорядочены в виде двенадцатиэлементных двухрядных массивов.

ЛИТЕРАТУРА

1. May, Gary S., Costas J. Spanos. Fundamentals of semiconductor manufacturing and process control. Wiley-Interscience, 2006. 481 p.

2. Wong Kok Sun. Process control monitor testing for integrated passive device wafers. KGD Packaging & Test Workshop, September 9–12, 2007. Napa, California.

3. Шур М. Современные приборы на основе арсенида галлия. М.: Мир, 1991. 632 с.

УНИВЕРСАЛЬНЫЙ МОДУЛЬ ВИЗУАЛИЗАЦИИ РАСЧЁТНЫХ ДАННЫХ

Е.П. Каратаев, студент 4-го курса; С.Ю. Дорофеев, аспирант; М.А. Песков, аспирант

г. Томск, ТУСУР, каф. КСУП, Karataev.Evgeny@gmail.com

Особенностью современного этапа развития радиоэлектроники является все более широкое освоение СВЧ диапазона, ведущее к появлению качественно новых радиоэлектронных и телекоммуникационных систем с улучшенными характеристиками.

В Томском государственном университете систем управления и радиоэлектроники в лаборатории интеллектуальных компьютерных систем ведется разработка программы анализа и синтеза СВЧ-устройств Indesys [1]. Для отображения научных и расчётных данных, для визуального анализа и реализации визуальных интерактивных методик необходимо их графическое представление, что позволяет в десятки раз повысить скорость восприятия информации и снизить степень утомляемости пользователя, снизить количество совершаемых ошибок.

Таким образом, необходим модуль отображения результатов моделирования в виде различных видов графиков (прямоугольный график, полярный график, диаграмма Вольперта-Смита, в виде таблиц).

Входными данными здесь являются результаты вычисления функции на наборе входных аргументов. На выходе необходимо в наглядной и доступной форме отобразить зависимость функции от аргумента.

На данный момент не существует готовых модулей отображения графиков функций, удовлетворяющих всем требованиям системы Indesys. Поэтому было решено реализовать модуль для отображения графиков в Visual Studio на языке программирования .NET C# с использованием графической библиотеки GDI+ [2]. На рис. 1 представлена общая схема модуля.

Пакет классов «Данные» содержит классы, отвечающие за хранение результатов вычислений. С помощью классов из этого пакета можно хранить как простые, так и сложные структуры входных данных. Пакет классов «Элементы графика» – это пакет, хранящий основные классы для отображения и описания отображенных данных: системы координат, оси. Пакет классов «График» включает в себя классы для отображения системы координат, легенды, плавающего маркера и текстовых подписей. Пакет классов «Элементы управления» включает в себя классы, описывающие диалоги настроек и пользовательского интерфейса.

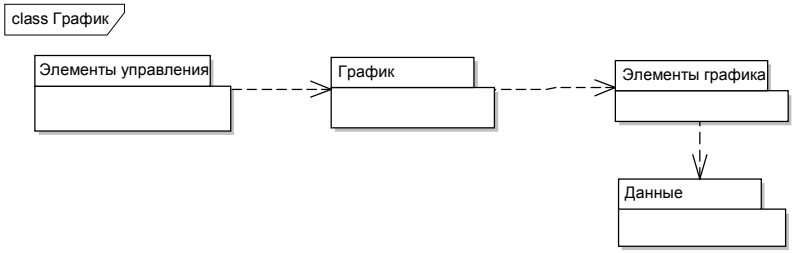


Рис.1. Общая схема модуля

На рис. 2 представлен результат отображения графика функции в прямоугольной системе координат, на котором отображены основные элементы графика.

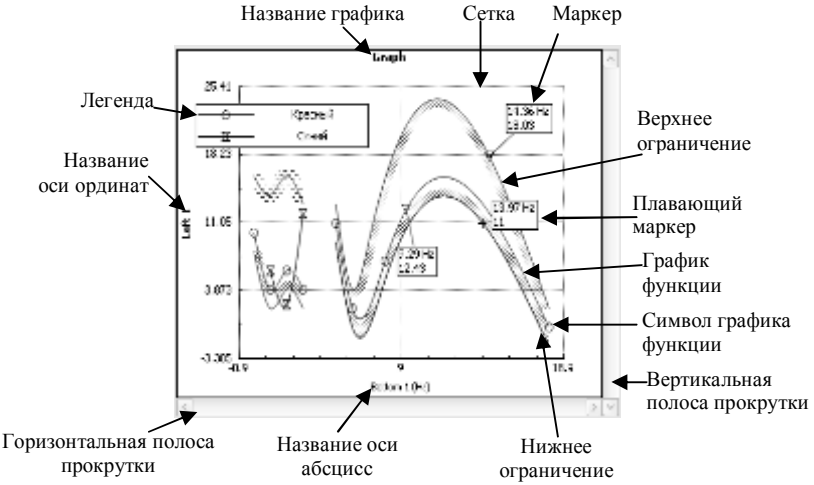


Рис. 2. Результат отображения графика в прямоугольной системе координат

Единый программный интерфейс задания данных позволяет абстрагироваться от способа их визуализации. Возможности модуля:

– возможность отображения нескольких графиков на одной координатной плоскости;

– возможность добавления нескольких абсцисс и ординат для прямоугольных графиков и привязки функций к ним;

– настройки сетки для диаграммы Смита (обычный/расширенный);

– отображение ограничений в виде линий со штриховкой;

– изменение формата числовых меток на осях;

– учёт системы измерений, в которой отображаются данные (данные на график подаются в системе СИ, но отображаться могут в любой системе измерения);

– использование интерполяции при выводе графиков;

– дополнительные настройки графика (цвет, тип и толщина линий, тип маркеров);

– установка шрифтов текста;

– масштабирование;

– плавающий маркер с отображением значений координат;

– копирование графиков в векторном и растровом форматах в буфер обмена.

Модуль для отображения графиков в системе Indesys, позволяет представить численные данные в наглядной и удобочитаемой форме, что в свою очередь позволяет повысить эффективность работы проектировщика. Кроме того, при проектировании графического модуля была заложена структура, предполагающая дальнейшее расширение функциональных возможностей, а большое количество настроек дает возможность пользователю настроить отображение графиков так, как удобно именно ему.

Данная работа была профинансирована грантами «Бизнес-Старт с Microsoft», INTAS, У.М.Н.И.К., РФФИ в рамках работы над системой Indesys.

ЛИТЕРАТУРА

1. Дорофеев С.Ю., Песков М.А., Барышников А.С., Кошевой С.Е. Бабак Л.И. INDESYS – интеллектуальная система автоматизированного проектирования СВЧ-устройств // Фестиваль Microsoft в ТПУ. Технологии Microsoft в теории и практике программирования: Секция: Системы автоматизированного проектирования. VI Всерос. науч.-практ. конф. студентов, аспирантов и молодых учёных.

2. Петцольд Ч. Программирование для Windows на C#. В 2 т. Т. 2. / Пер. с англ. М.: Изд.-торговый дом «Русская Редакция». 2002. 624 с.

СЕКЦИЯ 14

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Председатель секции – **Шелупанов А.А.**, проректор по НР ТУСУР, зав. каф. КИБЭВС, д.т.н., проф.;*
*зам. председателя – **Мещеряков Р.В.**, к.т.н., доцент, зам. зав. каф. КИБЭВС по НР*

АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО АДМИНИСТРАТОРА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА СИБИРИ ТУСУР

Г.Н. Абрамов, студент 5-го курса; В.Д. Зыков, аспирант
г. Томск, ТУСУР, каф. КИБЭВС, abramovgosha@mail.ru

В современном мире большинство информации хранится и обрабатывается в электронном виде. Для придания юридической значимости электронным документам в соответствии с действующим законодательством [1] необходимо использовать технологию электронной цифровой подписи (ЭЦП). Для обеспечения конфиденциальности передаваемой информации используется шифрование.

Функции формирования, проверки ЭЦП, шифрования, расшифрования данных и хранения ключей в соответствии с российскими криптографическими алгоритмами [2–4], реализуются с помощью криптопровайдеров (Cryptographic Service Provider, CSP) – программных модулей, содержащих библиотеку криптографических функций со стандартизованным интерфейсом. Они могут быть использованы различными интерфейсными приложениями.

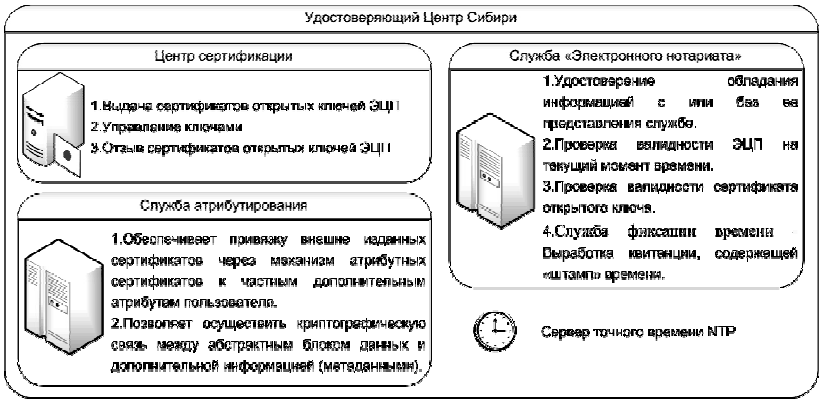
Каждый субъект защищенного информационного взаимодействия должен иметь сертификат открытого ключа подписи и соответствующие ему ключевые пары. Функции управления сертификатами и ключами выполняют специальные организации – удостоверяющие центры (УЦ). В Томске, на базе Института системной интеграции и безопасности ТУСУРа, существует Удостоверяющий центр Сибири.

Кроме функций управления сертификатами и ключами, Удостоверяющий центр Сибири реализует сервисы «Доверенной третьей сторо-

ны» (ДТС). Сервисы ДТС являются основной платформой для развертывания различных высокотехнологичных сервисов и услуг, в том числе относящихся к «электронному правительству».

В роль Доверенной третьей стороны (ДТС) входит предоставление гарантий участникам взаимодействия, что сообщения и сделки своевременно и точно передаются предполагаемому получателю с обеспечением целостности, подлинности и авторства и что в случае возникновения любых споров существуют определенные методы для создания и предоставления необходимых фактов, подтверждающих совершение действий и ход событий.

Сервисы ДТС Удостоверяющего центра Сибири включают: фиксацию времени (time stamping), электронную нотариальную службу и службу атрибутирования (рис.).



Сервисы ДТС Удостоверяющего центра Сибири

Кроме того, Удостоверяющий центр Сибири имеет статус Доверенного удостоверяющего центра Пенсионного фонда России (ПФР) и Доверенного удостоверяющего центра Федеральной налоговой службы России (ФНС России), что позволяет предоставлять возможность своим клиентам и сторонним удостоверяющим центрам присоединиться к системе электронного документооборота с ФНС России и ПФР.

Выполнение данных функций Удостоверяющим центром Сибири влечет за собой ряд соответствующих технических мероприятий, выполняемых администраторами УЦ. В настоящий момент ряд мероприятий не автоматизирован, что приводит к значительным временным затратам.

Для сокращения временных затрат администраторов УЦ разрабатывается программный продукт, реализующий следующие функции:

– функции криптографического менеджера: формирование ЭЦП, проверка ЭЦП, шифрование и расшифрование данных;

– проверка действительности сертификата по списку отозванных сертификатов или через OCSP [5];

– автоматическое получение актуальных списков отозванных сертификатов сторонних УЦ;

– отслеживание срока действия сертификатов, кросс-сертификатов;

– функции почтового клиента с возможностями защищенной электронной почты по протоколу S/MIME [6];

– взаимодействие с сервисами ДТС;

– создание запросов на сертификаты с поддержкой шаблонов запросов на сертификаты.

Таким образом, разрабатываемый программный продукт позволит автоматизировать все необходимые действия с сертификатами (отслеживание срока действия, создание запросов на сертификаты, получение актуальных списков отозванных сертификатов, проверка действительности сертификатов), реализовать криптографические операции с файлами и сообщениями электронной почты (с использованием встроенного почтового клиента) и обеспечить взаимодействие с сервисами ДТС. Объединение данного функционала в единое комплексное программное решение «Автоматизированное рабочее место администратора Удостоверяющего центра Сибири ТУСУР» позволит оптимизировать работу и сократить временные затраты администраторов УЦ.

Научный руководитель – В.Д. Зыков, аспирант каф. КИБЭВС.

ЛИТЕРАТУРА

1. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (в ред. Федерального закона от 08.11.2007 N 258-ФЗ).

2. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

3. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

4. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

5. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, RFC 2560, June 1999.

6. Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted – S/MIME J. Galvin, S. Murphy, S. Crocker, N. Freed, RFC 1847, October 1995.

РЕАЛЬНЫЕ ЗАТУХАНИЯ

Р.Ф. Акчурин, Е.Н. Анищенко, В.А. Трошин – студенты 4-го курса;
А.П. Зайцев, науч. рук., к.т.н., профессор
г. Томск, ТУСУР, каф. КИБЭВС, nurka12@rambler.ru

Защита информации является одной из наиболее важных задач для любого государства, предприятия, фирмы.

С развитием информационных технологий большая часть информации обрабатывается на электронно-вычислительных машинах. В свою очередь при обработке и передаче информации ЭВМ и линиями связи, по которым передается информационный сигнал, возникает электромагнитное поле, которое может быть использовано в целях получения информации злоумышленниками.

Эти паразитные электромагнитные излучения радиодиапазона, создаваемые в окружающем пространстве устройствами, специальным образом для этого не предназначенными, называются побочными электромагнитными излучениями (ПЭМИ). При излучениях элементами технических средств обработки, хранения и передачи информации (ТСПИ) информационных сигналов возникают наводки электромагнитных излучений [1]. В качестве антенны, принимающей такие наводки, могут выступать линии связи, средства коммуникаций, пожарные и охранные сигнализации и т.д. Но распространение сигналов в любых физических средах происходит с затуханием.

Затухание определяет относительное уменьшение амплитуды или мощности сигнала при передаче по каналу передачи сигнала определенной частоты. Коэффициенты затухания оказывают влияние на соотношение сигнал/шум на границе контролируемой зоны, где возможно снятие информативного сигнала средствами технической разведки. Поэтому точное определение этих коэффициентов имеет важное практическое значение.

Наша группа провела исследование по определению реальных коэффициентов затухания и определения радиуса опасных зон для конкретного объекта. Была собрана экспериментальная линия, исследования проводились по схеме, представленной на рисунке.

Измерение реального затухания в исследуемой линии проводилось отдельно для каждой частоты сигнала.

На каждой *j*-й частоте в исследуемую линию длиной 9 м вблизи СВТ подавался информативный сигнал с частотой 45 и 90 МГц и амплитудой напряжения 500 мВ от вспомогательного источника. Напряжение этого сигнала измерялось пробником напряжения в двух точках: вблизи СВТ в точке *1* и на границе контролируемой зоны в точке *2*.

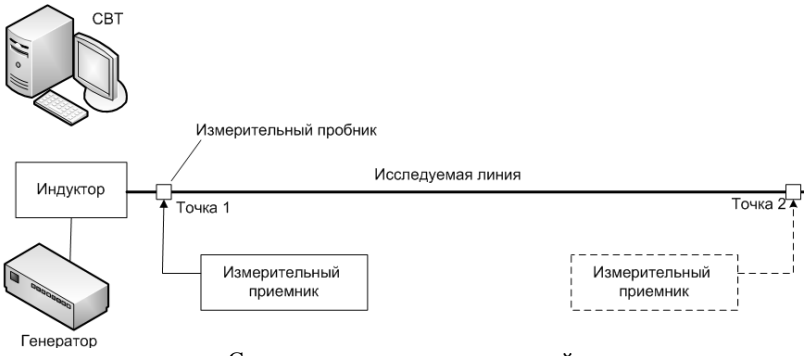


Схема проводимых исследований

При помощи измерительного приемника были получены данные для расчета реального коэффициента затухания, который вычислялся по формуле [2]:

$$K_{\text{Л}j} = 10 \cdot \lg \frac{U_{2uj}}{U_{1uj}} \text{ [дБ]},$$

где $K_{\text{Л}j}$ – коэффициент затухания на j-й частоте; U_{1uj}, U_{2uj} – напряжения, полученные пробником напряжения в точках *1* и *2* соответственно.

Результаты измерений и вычислений погонного коэффициента затухания $K_{\text{п}}$ представлены в таблице.

Полученные измерения и расчеты

Выход		Точка *A*	Точка *B*	l_{AB}, м	$R_{\text{н}}$, Ом	$K_{\text{п}}$, дБ/м
f, МГц	U, мВ	$U_{\text{тс}}$, мВ	$U_{\text{тс}}$, мВ			
45	500	500	450	9	56	0,102
90	500	400	300	9	56	0,278

По полученным результатам коэффициентов затуханий определяются радиусы опасных зон, по которым можно судить об эффективности применения активных средств защиты в случае, если радиус контролируемой зоны оказывается меньше допустимого.

Научный руководитель – А.П. Зайцев, к.т.н., профессор.

ЛИТЕРАТУРА

1. Зайцев А.П., Шелупанов А.А. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Томск: Изд-во Том. гос. ун-та систем управления и радиоэлектроники, 2004. 197 с.

2. Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации: Учеб. пособие. Томск: В-Спектр, 2008. 228 с.

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ РЕЧЕВОЙ ИНФОРМАЦИИ

Е.П. Аншакова, студентка 5-го курса;
Д.В. Кутузов, доцент каф. информационных систем
г. Астрахань, Астраханский государственный университет,
d_kutuzov@aspu.ru

В настоящее время актуальность защиты речевой информации от утечки по техническим каналам неоспорима. Особенно это касается обсуждения информации ограниченного доступа при проведении совещаний, переговоров и т.п. в коммерческих и государственных структурах. Однако при многообразии и широком ассортименте на российском и международном рынках технических средств защиты, различных по качеству, сложности и стоимости, единых методик по выбору оптимального комплекса средств защиты и оценке эффективности реализованных мер не существует.

В данной статье предлагается методика организации защиты речевой информации от утечки по техническим каналам для помещений, в которых эта информация циркулирует.

Первым этапом методики проведения мероприятий по защите помещений от утечки речевой информации по техническим каналам является определение риска утечки информации. Оценка рисков и выражение их в денежной форме необходимы, прежде всего, для принятия решения о целесообразности внедрения мер по обеспечению безопасности, их состава и направленности.

Вероятность реализации угрозы может быть оценена по статистическим данным, если на предприятии ведется статистика по нарушениям информационной безопасности.

При отсутствии статистических данных зачастую трудно определить вероятности того или иного события. Большинство предприятий не ведет учета нарушений безопасности и не имеет данных, характеризующих эти нарушения. Поэтому при оценке вероятности нарушения безопасности целесообразно использовать косвенные методы оценки. В качестве таких оценок могут выступать, например, метод ALE (Annualized Loss Expectancy), метод компании IBM [1] и т.п.

На втором этапе необходимо оценить вероятность использования злоумышленником того или иного технического канала утечки информации (ТКУИ). Она может быть оценена по статистическим данным (если таковые имеются) либо с применением одного из методов оценки с привлечением экспертов. В данной методике предлагается использовать метод анализа иерархий [2].

При осуществлении третьего этапа проводится оценка разборчивости речи в местах вероятного расположения средств съема речевой информации. Для этого используется инструментально-расчетный метод, основанный на результатах экспериментальных исследований [3], проведенных Н.Б. Покровским, при котором числовое значение словесной разборчивости рассчитывается на основе измерения отношения уровней речевого сигнала и шума в местах предполагаемого расположения датчиков аппаратуры акустической разведки.

На четвертом этапе формируется множество методов защиты. В качестве примера, предлагается использовать методы защиты, изложенные в работах [4, 5].

Пятый этап осуществления методики предполагает выбор оптимальных средств защиты и осуществляется изложенным выше методом анализа иерархий. В этом случае в роли альтернатив выступают средства защиты, которые оцениваются по набору критериев, определенных для этой задачи.

Критериями выбора средств защиты могут быть: стоимость; эффективность; наличие сертификации ФСТЭК; совместимость; удобство установки и использования и т.п.

Заключительный шестой этап предполагает, что после интегрирования системы защиты для оценки эффективности реализованных мер, проводится повторная оценка вероятности утечки речевой информации. Для акустических каналов проводится расчет вероятности утечки речевой информации путем измерения разборчивости речи. Для оценки вероятности использования других ТКУИ может использоваться один из методов экспертных оценок, например ALE. Далее может быть оценен уровень снижения вероятности утечки и рисков, связанных с утечкой речевой информации.

Предложенные рекомендации разработаны на основе анализа многочисленных известных методов и могут найти практическое применение в области защиты информации, а также быть полезны руководителям коммерческих организаций, которых волнуют вопросы защиты коммерческой тайны при проведении переговоров.

Научный руководитель – Д.В. Кутузов, доцент каф. информационных систем АГУ.

ЛИТЕРАТУРА

1. Семкин С.Н.,Беляков Э.В.,Гребенев С.В., Казачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации. М.: Гелиос АРВ, 2005. 186 с.

2. Саати Т. Принятие решений: метод анализа иерархий: Пер. с англ. М.: Радио и связь, 1993. 278 с.

3. Хорев А.А., Макаров Ю.К. К оценке эффективности защиты акустической (речевой) информации. // Специальная техника. 2000. №5.

4. Торокин А.А. Основы инженерно-технической защиты информации. М.: Ось-89, 1998. 336 с.

5. Хорев А.А. Защита информации от утечки по техническим каналам. Ч. 1. Технические каналы утечки информации
http://www.analitika.info/kanalutechki.php

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВУЗА

И.В. Аютова, ассистент каф. радиоэлектроники

г. Сургут, Сургутский государственный университет,
vishenka786@mail.ru

Рынок образовательных услуг – совокупность существующих и потенциальных покупателей и продавцов товара. Образовательные услуги пользуются большим спросом – статья образования у россиян среднего класса входит в тройку первостепенных статей расхода. Расходы на образование составляют 5% совокупных потребительских расходов этого слоя населения [1].

Конкуренцию на рынке образовательных услуг усиливают: введение единого государственного экзамена, сложная демографическая ситуация, внедрение образовательных кредитов и государственных именных финансовых обязательств.

Вузы, конкурируя за определенные сегменты рынка, как экономические субъекты, стремятся обеспечить собственную безопасность от внешних и внутренних угроз.

Основная проблема по обеспечению информационной безопасности вуза – это значительное отличие процессов, ресурсов и характера информационных потоков, характерных для типовой компании (предприятия, организации).

В силу своей специфики в вузе хранится и обрабатывается огромное количество информации, связанной с обеспечением учебного процесса, внеучебной деятельности, научных разработок, международного сотрудничества, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация.

Вуз как объект защиты обладает рядом особенностей [2], таких как публичность, непостоянство аудитории, широкое внедрение средств вычислительной техники, территориальная разобщенность отдельных объектов, использование современных информационных технологий, развитие различных форм дистанционного обучения, значительные наработки в области интеллектуальной собственности.

Вышеперечисленные особенности приводят к неконтролируемому росту количества уязвимостей, увеличению числа угроз со стороны внешних и внутренних злоумышленников и, соответственно, трудно предсказуемым потенциальным материальным, финансовым, моральным и другим видам потерь.

Многочисленные исследования показывают, что более 70% всех нарушений в современных компаниях приходится на долю внутренних нарушителей [3]. К внутренним нарушителям вуза можно отнести студентов, преподавателей, сотрудников, технический персонал. Доступ к наиболее ценным активам вуза имеют преподаватели и сотрудники. В условиях все более жесткой конкуренции вузов и на фоне экономического кризиса этим нарушителям необходимо уделять более пристальное внимание. Такая группа нарушителей, как студенты, в силу своего возраста и свойственного им азарта и желания самоутвердиться, реализует угрозы не для личной выгоды, а из желания опробовать свои знания и произвести впечатление на окружающих. Исключением являются угрозы, связанные с контролем знаний и закачкой данных. Перечисленные источники угроз – потенциальные причины финансовых и нематериальных потерь вуза [4], таких как ущерб, связанный с восстановлением ресурсов после реализации угроз, ущерб, связанный со срывом учебного процесса или НИР, снижение конкурентоспособности вуза на рынке образовательных услуг, ущерб репутации вуза, снижение качества образования, нарушение эмоционально-психологического состояния коллектива.

Рассмотрим результаты глобального исследования статистики по инцидентам, связанным с утечками информации компании InfoWatch [5].

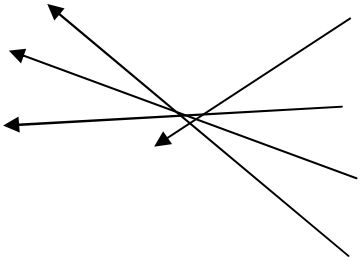
Доли умышленных и случайных утечек

Вид утечек	1-е полугодие 2009		2-е полугодие 2008	
	Кол-во	%	Кол-во	%
Умышленные	231	55,9	133	48,7
Случайные	161	39,0	105	38,5
Не установлено	21	5,1	35	12,8

Из таблицы видно, что доля умышленных утечек практически в полтора раза больше случайных утечек, и этот показатель в 1-м полугодии 2009 г. заметно вырос по сравнению со 2-м полугодием 2008 г.

Все предприятия и организации, в которых произошли утечки, ставшие публичными, эксперты InfoWatch подразделяют на три катего-

рии: государственные учреждения, коммерческие предприятия, а также учебные заведения и общественные, некоммерческие структуры.



Распределение источников утечек по видам организаций
в 1-м полугодии 2009 г.

Как видно из диаграммы, в 1-м полугодии 2009 г. доля утечек конфиденциальных данных в учебных заведениях и общественных, некоммерческих структурах составляет 11%, т.е. каждая 10 утечка информации происходит в этом секторе. На конец февраля 2010 г. эта цифра выросла более чем в 2 раза.

Проблемой многих вузов также является ведение бумажного документооборота или частичный переход на электронный документооборот при отсутствии единой защищенной базы данных. Так, например, персональные данные студента дублируются: в журнале группы, в личной карточке студента в деканате, в карточке читателя библиотеки, в студенческом отделе кадров, на выпускающей кафедре, после распределения по специальностям, в бухгалтерии, при обучении на бюджетной основе, в договорном отделе, при обучении на коммерческой основе.

Аналогичная ситуация и с профессорско-преподавательским составом. В таких структурных подразделениях, как бухгалтерия, и отдел кадров, существует определенный уровень защиты информации, но, к примеру, кафедра и деканат, характеризуются постоянным скоплением студентов, преподавателей, посетителей и низким уровнем защиты информации.

Вопрос обеспечения информационной безопасности в вузе не столь однозначен, как это кажется на первый взгляд. Принятое нами представление о вузе как о храме науки, открытом каждому, на сего-

дняшний момент изменилось, вузы как поставщики услуг на рынке борются за свой сегмент рынка. Нетиповая структура, открытость для посетителей, большой круг пользователей внутри вуза не позволяют однозначно формализовать процессы, протекающие в нем. Но этому вопросу необходимо уделить более пристальное внимание, в связи с более жесткой конкуренцией. Потенциальные угрозы, которые могут быть реализованы в вузе, могут привести как к существенным финансовым затратам, так и к ущербу репутации вуза, снижению качества образования, снижению конкурентоспособности вуза на рынке образовательных услуг.

Научный руководитель – В.А. Майстренко, д.т.н., профессор, академик Международной академии информатизации.

ЛИТЕРАТУРА

1. Владимирова С.А. Экономика региональной системы образования как объект исследования // Вестник Казанского технологического университета. 2008. №3. С. 178–184.

2. Васильев В. И. Построение нечетких когнитивных карт для анализа и управления информационными рисками вуза / В.И. Васильев, И.А. Савина, И.И. Шарипова // Вестник Уфимского государственного авиационного технического университета. Сер. Управление, вычислительная техника и информатика. 2008. Т. 10, №2. С. 199–209.

3. Цыбулин А.М. Математическая модель злоумышленника в корпоративной сети / Цыбулин А.М., Шипилев А.В // Управление большими системами: Сб. трудов. 2007. №19. С. 127–133.

4. Кудрявцева Р.Т. Управление информационными рисками с использованием технологий когнитивного моделирования: Дис. … канд. техн. наук. Уфа, 2008. 159 с.

5. Глобальное исследование утечек. Первое полугодие 2009 [Электронный ресурс]. Режим доступа: http://www.infowatch.ru/threats_and_risks/analytical_reports/2811/, свободный.

ОБЕСПЕЧЕНИЕ КАЧЕСТВА И ЦЕЛОСТНОСТИ ДАННЫХ В ГЕОИНФОРМАЦИОННЫХ ФОНДАХ

В.А. Белькович, студент 6-го курса,
каф. информационной безопасности
г. Тюмень, ТГУ, belkovichva@mail.ru

В настоящее время в IT-индустрии прослеживается тенденция к созданию различных общих баз знаний, хранилищ и информационных фондов, содержащих большие объемы данных. В том числе такой подход оказался актуальным и для геоинформационных фондов, аккуму-

лирующих в себе точный картографический материал. Высокая себестоимость и быстрое «устаревание» картматериала объясняют общую тенденцию совместного использования геоданных несколькими компаниями (группами пользователей). При этом пользователи являются как потребителями данных, так и их поставщиками. То есть пользователь может беспрепятственно получить интересующую его информацию или внести новую. Схема потоков данных в этом случае во многом схожа со схемой в открытых сетях. Поэтому многие угрозы присущие различным социальным сетям, торрент-трекерам и т.д., также актуальны и для геоинформационных фондов, например:

1. Наполнение геоинформационного фонда некачественными данными (засорение). Тем самым серьезно страдает критерий доступности информации, снижается «полезность» системы.

2. Желание пользователей являться лишь «потребителем» информации, но никак не ее поставщиком.

Далее приведены мероприятия по устранению этих угроз. Во-первых, сохраняя данные в фонд, пользователь может выбрать из списка тех, кто вообще не будет иметь доступ к этой информации («черный лист»). Во-вторых, что касается картографических данных, то нельзя получить всю карту целиком. Можно выделить необходимый район работ фиксированной площади и сохранить его. Размер площади доступной для сохранения, также определяет пользователь, выкладывающий карту. Бывают ситуации, когда необходимо сохранить район работ, площадь которого все же больше той, что доступна. В этом случае пользователю, выложившему карту, отсылается запрос. Если он отвечает на запрос положительно, то сохранение разрешается, иначе нет. Конечно, ответ на запрос может прийти не сразу. Да и пользователь вместо одного может сохранить несколько районов работ, частично перекрывающих друг друга. Поэтому важно не то, сколько кто скачивает, а то, как именно он это делает.

Вторая существенная угроза – это случайное или намеренное сохранение в фонд искаженных, некорректных или вообще бесполезных данных. В этом случае страдают актуальность и достоверность общего картографического фонда. Традиционным способом решения данной проблемы является комментирование другими пользователями такой информации. Но в целом этот способ проблему не решает – выявить некорректные данные на карте довольно сложно.

Для решения данных проблем автором предлагается использовать сервис оценки профессиональной репутации. Эта оценка во многом схожа с рейтингом пользователей в социальных сетях. Принципиальным различием является то, что сервис предназначен для конкретной предметной области и учитывает ее особенности (например, какой

именно картматериал интересует пользователя, как он сохраняет соседние районы работ, с наложением или без и т.д.). Данный сервис призван помочь выявить недобросовестных пользователей, а также поощрить тех, кто работает в системе много и качественно. Для каждого пользователя сервис высчитывает оценку, его профессиональную репутацию. Чем выше оценка, тем большими привилегиями обладает пользователь. Например, можно без дополнительных запросов скачать район работ, площадь которого превышает заданную.

В формировании репутации не обойтись без «человеческого фактора». Этим фактором являются экспертные оценки, выставляемые за сохраненные документы.

Далее приведена математическая модель профессиональной репутации, на которой основывается предложенный сервис:

$$p = \frac{\sum_{e \in E} f(e)}{|E|},$$

E – множество документов, за которые ответствен пользователь; $f(e)$ – оценка соответствия конкретного документа.

$$f(e) = \frac{\sum_{r \in R} r}{6|R|} + \frac{1 - \frac{1}{a^x}}{3},$$

R – множество документов оцененных экспертами; r – принимает целые значения от 0 до 4; x – количество просмотров конкретного документа.

В дальнейшем планируется развивать описанную модель с учетом предметной области.

Научный руководитель – О.В. Желудкова, к.т.н., доцент каф. информационной безопасности.

ЛИТЕРАТУРА

1. ГОСТ Р 52155-2003. Географические информационные системы. Федеральные, региональные, муниципальные. Общие технические требования.

2. ГОСТ Р 52573-2006. Географическая информация, метаданные.

3. Грищенко В.С. Исчисление мнений // Известия Уральского государственного университета. Сер. Компьютерные науки и информационные технологии. 2006. №42. С. 139–153.

4. Грищенко В. С. Метрики репутации и борьба за релевантность // Безопасность информационного пространства: Матер. междунар. науч.-практ. конф. студентов, аспирантов и молодых ученых. Екатеринбург: Изд-во УрГУПС: 2006. – С. 89.

5. Selcuk A.A., Uzun E., Pariente M.R. A reputation-based trust management system for p2p networks // 4th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGrid 2004). Chicago, USA, 2004. April.

АВТОМАТИЗАЦИЯ ОЦЕНКИ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИХ ЗАЩИТЫ

Э.Р. Бейбутов, аспирант каф. КБ
г. Москва, РГГУ, flash-best@mail.ru

Понимая важность и ценность информации о человеке, а также заботясь о соблюдении прав своих граждан, государство требует от организаций и физических лиц обеспечить надежную защиту персональных данных. Требования Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» были конкретизированы в подзаконных актах Правительства РФ, Министерства связи и массовых коммуникаций РФ, нормативно-методических документах ФСТЭК России, ФСБ России и Роскомнадзора.

Документы, разработанные федеральными службами, вызвали неоднозначную реакцию экспертов в области информационной безопасности и юридических лиц, подпадающих под действие нового законодательства [1]. При обсуждении проектов по защите персональных данных перед операторами встает ряд проблем

− каким образом проводить работы по определению текущей обстановки по обеспечению безопасности персональных данных в организации;

− по каким критериям оценивать выполнение требований множества руководящих документов федеральных служб;

− в какой последовательности необходимо устранять несоответствия требованиям;

− какие рекомендации по реализации требований имеются в «лучших практиках»;

− возможно ли автоматизировать процесс оценки соответствия обработки персональных данных требованиям законодательства в области их защиты.

Настоящая статья посвящена описанию предлагаемых автором решений ряда поставленных проблем.

Формирование перечня этапов работ по оценке соответствия проводилось с учетом документов [2–4], в связи с чем автор предполагает, что разработанный подход может являться альтернативой до появления официальных регламентов проверок всех федеральных служб. В соответствии с разработанным регламентом проведение работ состоит из этапов, перечисленных ниже:

− организация проведения оценки соответствия;
− документарная проверка;
− выездная проверка;
− подготовка отчета по оценке соответствия;

− подготовка плана мероприятий с рекомендациями по устранению выявленных несоответствий;

− бюджетная оценка стоимости устранения несоответствий;

− завершение работ.

В общем случае под критериями оценки понимается совокупность политик ИБ, процедур или требований, установленных федеральными законами и подзаконными нормативно-правовыми актами и/или стандартами и нормативами, с которыми сравнивается свидетельство соответствия. Свидетельство соответствия при этом определяется как записи, изложения фактов или другой информации, связанной с критериями оценки, которая может быть перепроверена. Любые свидетельства соответствия, в том числе свидетельства, содержащие информацию об инцидентах ИБ, должны быть доступны для членов экспертной группы.

Разработанный автором регламент проведения оценки соответствия предполагает наличие двух групп критериев:

− критерии оценки выполнения требований при документарной проверке;

− критерии оценки выполнения требований при выездной проверке.

Первая группа критериев содержит наборы показателей для оценки соответствия состава и содержания организационно-распорядительных документов, локальных нормативно-правовых актов и форм документов оператора организационным и юридическим требованиям законодательства в области защиты ПДн.

Вторая группа критериев содержит наборы показателей для оценки выполнения и полноты реализации методов и систем защиты ПДн техническим и эксплуатационным требованиям законодательства в области защиты ПДн.

Ввиду необходимости формирования и развития инструментального программного обеспечения (ПО) с учетом совершенствования нормативного обеспечения безопасности ПДн в ИС, автором был разработан программный комплекс (ПК), позволяющий автоматизировать процесс оценки соответствия обработки ПДн требованиям законодательства в области их защиты.

Разработанный программный комплекс позволяет решить ряд поставленных перед операторами задач, таких как:

1) автоматизировать проведение работ по определению текущей обстановки по обеспечению безопасности персональных данных в организации;

2) накапливать и использовать рекомендации по устранению несоответствий в планах работ по защите персональных данных в организации;

3) автоматизировать разработку плана мероприятий по устранению несоответствий.

Создание программного комплекса потребовало от автора разработки регламента проведения работ по оценке соответствия обработки персональных данных требованиям законодательства в области их защиты, определяющим:

1) участников оценки, их цели и распределение ответственности между ними;

2) подход и общий порядок оценки соответствия информационных систем (ИСПДн) требованиям безопасности информации.

Документарная и выездная проверки, определенные упомянутым регламентом, потребовали выработки кортежей критериев и наборов показателей оценки соответствия обработки персональных данных требованиям законодательства в области их защиты.

Научный руководитель – А.А. Грушо, д.ф.-м.н., профессор каф. КБ.

ЛИТЕРАТУРА

1. Бейбутов Э. Защита персональных данных. Выход есть // Открытые системыэ 2009. № 6. С. 32–33. Электронный адрес статьи: http://www.osp.ru/os/2009/06/10069191.

2. Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных. Утвержден приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 01.12.2009 № 630.

3. Концепция аудита информационной безопасности систем информационных технологий и организаций (проект), ФСТЭК России. http://www.fstec.ru/_licen/016.doc.

4. Положение по аттестации объектов информатизации по требованиям безопасности информации, Утверждено председателем Гостехкомиссии России от 25 ноября 1994 г.

ОБУЧАЮЩАЯ СИСТЕМА ПО СУБД FIREBIRD*

А.О. Битюцкая, студентка 4-го курса

г. Томск, ТУСУР, каф. КИБЭВС, bao_89@mail.ru

В рамках проекта ГПО «Инженерия баз данных», проводимого на кафедре КИБЭВС, было принято решение создать обучающую систему по СУБД Firebird.

* Выполнено в рамках проекта ГПО 0842 – Инженерия баз данных.

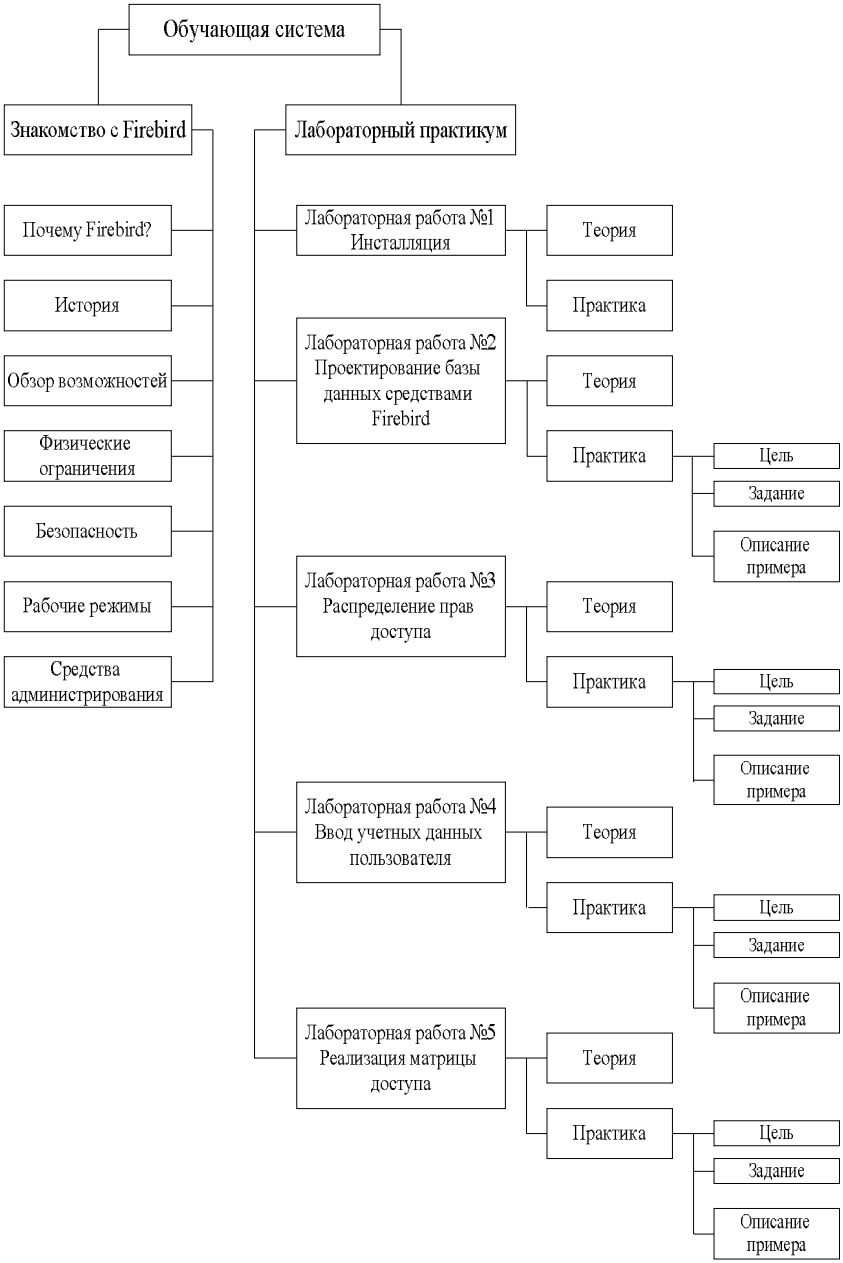


Рис. 1. Структура системы

В настоящее время все больше приложений разрабатывается с помощью СУБД Firebird, так как данная СУБД распространяется бесплатно и не имеет лицензионных ограничений.

Задача данного проекта состоит в том, чтобы создать систему, которая позволяет научиться работать в СУБД Firebird, а именно создавать базы данных и защищать их средствами самой СУБД.

В ходе анализа предметной области и изучения работы алгоритмов было принято решение, что система будет работать по схеме, показанной на рис. 1.

Обучающая система состоит из двух основных разделов: теория и практика.

В теоретическом разделе «Знакомство с Firebird» обучающийся может узнать больше о данной СУБД, а именно: историю, возможности, ограничения на размеры базы данных, безопасность. Этот раздел позволяет быстро и понятно ознакомиться с программой.

Чтобы приступить ко второму разделу «Лабораторный практикум», предполагается, что обучающийся уже знаком с курсом «Безопасность систем баз данных», т.е. уже выполнил анализ предметной области и подготовил модель базы данных.

В разделе «Лабораторный практикум» пользователь учится работать в СУБД Firebird, выполняя лабораторные работы, в которых подробно и поэтапно расписаны все действия. Изучив этот раздел и выполнив все задания, он сможет самостоятельно спроектировать, создать базу данных и защитить ее средствами СУБД.

Для реализации оболочки обучающей системы был выбран язык разметки HTML.

На рис. 2 показан пример работы в данной системе.

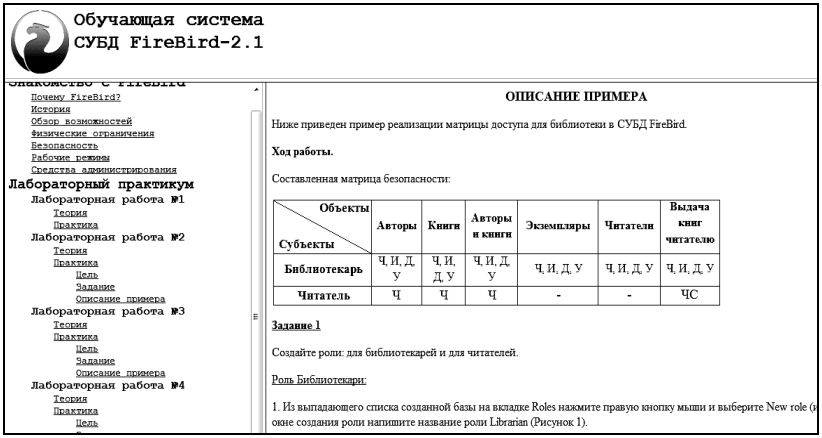


Рис. 2. Обучающая система по СУБД Firebird

Данная система позволяет обучающемуся самостоятельно ознакомиться с теоретическим материалом и научиться применять на практике полученные знания.

Для работы с данной программой достаточно навыков работы с web-документами. К достоинствам системы можно отнести легкое и понятное освоение материала, описание примеров практической реализации.

Научный руководитель – Н.А. Новгородова, старший преподаватель каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Хелен Борри Firebird. Руководство разработчика баз данных. СПб.: БХВ-Петербург, 2006. 1104 с.

2. Черемных С.В., Семенов И.О., Ручкин В.С.: Моделирование и анализ систем // IDEF-технологии: Практикум – Финансы и кредит, 2005. 192 с.

3. Давыдова Е.М., Новгородова Н.А. Базы данных: Учеб. пособие. Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2008. 127 с.

4. Петюшкин А.В. HTML. Экспресс-курс. СПб.: БХВ-Петербург, 2003. 256 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ NOTARY PRO, КРИПТО ПРО УЦ И MICROSOFT CA

В.А. Черемнов, студент 5-го курса; В.Д. Зыков, аспирант

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

Бурное развитие компьютерных технологий и повсеместное внедрение их в бизнес с использованием Интернета, коренным образом изменяют устоявшиеся способы ведения бизнеса.

Для многих участников предпринимательской деятельности вопрос об использовании электронной цифровой подписи (ЭЦП) уже давно решен. Предпочитая обмениваться электронными документами, заключать договоры и подписывать акты на расстоянии, организации различных форм собственности применяют в своей деятельности криптографические средства защиты информации, пользуясь преимуществами, которые дает ЭЦП.

Наиболее распространенными сферами использования ЭЦП являются: сдача отчетности, электронная торговля, банкинг, корпоративный документооборот, здравоохранение, образование и др. Так, например, банки для привлечения клиентов и автоматизации обслуживания предлагают систему «Банк–Клиент». С помощью дистанционного банковского обслуживания клиент может осуществлять расчеты через сеть Интернет, что ускоряет процесс проведения расчетов.

В соответствии с Федеральным законом «Об электронной цифровой подписи», для проверки подлинности ЭЦП используется сертификат ключа подписи, который выдается специализированной организацией – удостоверяющим центром (УЦ) [1].

В настоящее время существует множество программных комплексов, реализующих функции УЦ, среди которых: Notary Pro, Крипто Про УЦ, Microsoft CA и др. Каждый из них выполняет основную функцию – выпуск сертификатов открытых ключей и обладает различными особенностями и свойствами.

Программный комплекс Notary Pro реализует алгоритмы ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 и ГОСТ 28147-89, выполнен с использованием сертифицированного ФСБ СКЗИ «Крипто-КОМ 3.2» и может использоваться для защиты информации, не содержащей сведений, составляющих государственную тайну. Совместим с другими криптопровайдерами и криптобиблиотеками, поддерживающими международные стандарты RFC 4357, 4490, 4491.

Программный комплекс Крипто Про УЦ, так же как и Notary Pro, реализует криптографические алгоритмы ГОСТ 28147-89, ГОСТ Р34.10-94, ГОСТ Р34.10-2001, сертифицирован ФСБ России по классу КС1 (КС2 при использовании совместно с сертифицированным средством защиты от НСД) и может использоваться для защиты информации, не содержащей сведений, составляющих государственную тайну.

Основные функциональные возможности данных УЦ идентичны. С их помощью возможно построение как централизованной, так и распределенной схем получения электронной цифровой подписи. Важным отличием программных комплексов являются типы поддерживаемых операционных систем.

Удостоверяющий центр Microsoft CA является одной из служб операционной системы (ОС) Windows Server 2000/2003/2008. Его особенностью являются поддержка подачи заявок на сертификаты и их отзыв в различных масштабируемых средах, в том числе с использованием Active Directory.

Сравнительный анализ данных трех комплексов удостоверяющих центров показал, что Крипто Про УЦ и Notary Pro реализуют сертифицированными средствами российские криптографические алгоритмы и могут использоваться для обеспечения юридической значимости систем электронного документооборота государственных учреждений. В отличие от них – в Microsoft CA для поддержки российских криптографических алгоритмов необходимо устанавливать соответствующий криптопровайдер. С использованием Microsoft CA в коммерческих организациях можно реализовать: технологию защищенной электронной почты (S/MIME), безопасный протокол передачи данных (SSL/TLS),

защищенные беспроводные сети, виртуальные частные сети (VPN), протокол IPsec, шифрованную файловую систему (EFS), вход в операционную систему с помощью смарт-карт.

Программные комплексы Крипто Про УЦ и Notary Pro необходимо приобретать и устанавливать отдельно, уже после установки операционной системы. А Microsoft CA является одной из служб ОС Windows Server, что дает пользователю возможность применять имеющиеся возможности его ОС без дополнительных затрат.

Научный руководитель – В.Д. Зыков, аспирант каф. КИБЭВС.

ЛИТЕРАТУРА

1. Федеральный закон от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи» (в ред. Федерального закона от 08.11.2007 № 258-ФЗ).

ПОДСИСТЕМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ USB FLASH DRIVE

И.С. Черепанов, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, Banshik299@mail.ru

Идентификация и аутентификация – это первая линия обороны информационного пространства.

Идентификация – это процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации – каждый субъект или объект системы должен быть однозначно идентифицируем. Аутентификация – это проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы.

Парольная аутентификация. Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым. Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации и далеко не всегда после установки системы производится их смена. Ввод пароля можно подсмотреть. Иногда для подглядывания используются оптические приборы.

Также необходимо отметить, что сервис идентификации и аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Компьютер, который проводит идентификацию, имеет список имен пользователей и паролей. Когда пользователь входит под своим именем и паролем, компьютер сравнивает введенные данные с записями, хранящимися в его списке. Если пользователь ввел данные, имеющееся в списке, то происходит авторизация, в противном случае пользователь получает отказ.

В разрабатываемой системе в качестве внешнего аппаратного ключа выступает персональный flash накопитель, при этом он не теряет свойств устройства хранения и переноса информации. Каждое устройство, использующее USB-интерфейс, имеет уникальный идентификатор, который будет являться ключевой информацией для осуществления идентификации и аутентификации. В каждой системе идентификации и аутентификации изначально необходимо провести процедуру регистрации. При дальнейшей авторизации клиент будет подтверждать свою подлинность. В разрабатываемой системе данная процедура осуществляется с использованием асимметричного алгоритма шифрования RSA.

Подсистема идентификации и аутентификации состоит из:

– модуля считывания идентификатора USB-накопителя, данный модуль позволяет получить уникальный номер устройства, который ему был присвоен при изготовлении;

– модуля хеширования, в данном модуле реализован алгоритм хеширования ГОСТ Р 34.11 – 94;

– модуля реализации алгоритма шифрования данных ГОСТ 28147-89, данный модуль предназначен для проведения аутентификации;

– модуля реализации асимметричного алгоритма шифрования данных RSA, данный модуль предназначен для проведения регистрации.

Для регистрации пользователю необходимо скопировать на свой flash-накопитель программное обеспечение, так как оно не содержит секретной информации, то является общедоступным для любого пользователя. Далее пользователь запускает программу в режиме регистрации, ему будет предложено ввести PIN-код (не менее 5 знаков). Запущенная программа считывает уникальный идентификатор и с помощью криптографического алгоритма хеширования ГОСТ Р 34.11 – 94 преобразует его в 256-битовое хэш-значение. Данный хэш будет являться ключом к алгоритму шифрования данных ГОСТ 12847–89. Далее для

получения уникального значения, по которому будет происходить поиск зарегистрированного пользователя, мы объединяем введенный PIN-код с идентификатором flash-накопителя и также вычисляем хэш-значение с помощью алгоритма ГОСТ Р 34.11 – 94. Таким образом, мы получаем два уникальных значения, первое из которых будет являться ключом для проведения аутентификации, а второе – для поиска пользователя в базе данных (идентификации).

Научный руководитель – Ю.М. Филимонов, к.ф.-м.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Щеглов А.Ю. Задача идентификации и аутентификации. Постановка в общем виде и подходы к решению. http://www.npp-itb.spb.ru

2. ГОСТ 28147–89. Алгоритм криптографического преобразования данных.

3. Шефановский Д.Б. ГОСТ Р 34.11 – 94. Функция хеширования. Краткий анализ. М.: Учебный центр «ИНФОРМЗАЩИТА»; 2001. 158 с.

4. Двуреченский П.А. Алгоритм шифрования данных ГОСТ 28147–89. http://pavel.przone.ru

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ АНАЛИЗА ПАРАМЕТРОВ РЕЧЕВОГО СИГНАЛА*

Д.В. Черных, В.С. Хлебников, студенты 4-го курса

г. Томск, ТУСУР, каф. КИБЭВС, dmit-cher@mail.ru

Для создания программ, позволяющих производить такие действия над речевым потоком, как выделение ключевых слов, распознавание речи и др., необходимо знать ключевые параметры отдельных фонем, по которым их можно было бы различать.

Для поиска и изучения таких параметров был создан программный комплекс для исследования речевых сигналов, который разбит на девять модулей, где каждый модуль отвечает за свою функцию (рис. 1):

– модуль определения номеров каналов и интенсивностей гармоник;

– модуль определения номеров каналов границ заданного частотного окна;

– модуль определения номеров каналов и интенсивностей гармоник в заданном частотном окне;

– модуль вычисления суммарной интенсивности по каналам;

* Выполнено в рамках проекта ГПО КИБЭВС-0841 – Распознавание слуховых образов.

– модуль вычисления относительных интенсивностей (относительно частоты основного тона);

– модуль сортировки гармоник по интенсивностям;

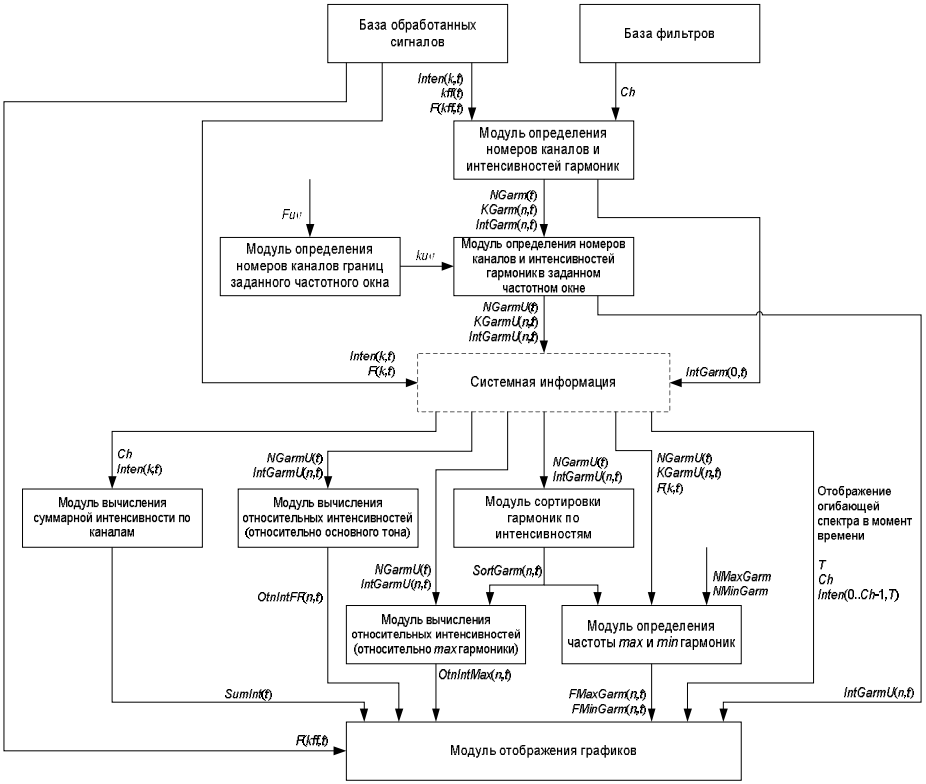
– модуль вычисления относительных интенсивностей (относительно максимальной гармоники);

– модуль определения частоты максимальной и минимальной гармоник;

– модуль отображения графиков.

Разработанный программный комплекс позволяет разбивать речевой сигнал на вокализованный и невокализованный и другие участки, которые соответствуют заданным параметрам.

Для удобства использования, а также для повышения гибкости комплекса все математические алгоритмы были скомпилированы в виде динамических библиотек (рис. 1).



Структура исследовательского комплекса

Основные возможности комплекса:

– свертка речевого сигнала с фильтром;

– автоматическая сегментация сигнала в соответствии с параметрами;

– сравнение результатов автоматической сегментации с результатами ручной сегментации;

– отображение графической информации (зависимость интенсивности от частоты, интенсивности от времени и др.).

В результате создания такого комплекса была получена возможность с высокой степенью точности разделять слитную речь на сегменты, соответствующие фонетическим классам звуков. При этом параметры речевого сигнала выделяются на основе собственных алгоритмов применительно к каждому классу звуков.

Научный руководитель – А.А. Конев, к.т.н., доцент каф. КИБЭВС ТУСУРа.

О ПРИМЕНЕНИИ ФАКТОРНОГО АНАЛИЗА В ЗАДАЧАХ ОЦЕНКИ ЗАЩИЩЕННОСТИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Е.А. Данилова, аспирант

г. Красноярск, СибГАУ, каф. БИТ, omni86@mail.ru

Различают множество принципов факторного анализа [1]. Для выполнения поставленной задачи используется детерминированный многофакторный анализ.

Чтобы решить задачу учета всего множества факторов, влияющих на информацию, циркулирующую в системе электронного документооборота (СЭД), предлагаем разбить ее на основные составные элементы. При этом для каждого элемента определим возможные состояния, которые он может принимать, затем рассмотрим сочетания этих состояний, создавая базовую модель описания всех возможных частных функций полезности и моделируя функцию риска в динамике развития системы на основе минимального набора исходных данных.

Пусть существует информационная система *IS*, которая состоит из *N* числа элементов *E*, каждый из которых состоит из *K* составляющих. Составляющая каждого элемента в определенный промежуток времени может принимать *x* состояний *s* с вероятностью *r*:

$$IS=\{E_i\},\ E_i=\begin{Bmatrix} s_1^1 & s_2^1 & \dots & s_{x1}^1 \\ s_1^2 & s_2^2 & \dots & s_{x2}^2 \\ \dots & \dots & \dots & \dots \\ s_1^k & s_2^k & \dots & s_{xk}^k \end{Bmatrix},\ \text{здесь } i \in [1\dots N].$$

Назовем x количеством степеней свободы элемента. Очевидно, что используя подобную модель системы, можно воспользоваться методом морфологического ящика Цвикки (например, см. [2, с. 196] в различных вариантах. При этом рассчитать количество причинно-следственных связей между состояниями элементов информационной системы можно, рассчитывая их как число размещений с повторениями:

$$k_{\text{сост}}=\left(\sum_{i=1}^{N}\sum_{j=1}^{K} x_{s_{ij}}\right)^n.$$

Принимая во внимание, что в данной работе поставлена цель оценки защищенности элементов СЭД, структура которой организационно, технически и с помощью функционально-логических моделей может быть относительно легко описана, основной задачей, определяющей эффективности интегральной оценки, становится описание составляющих элемента.

На основании определения АС [3] можно выделить четыре основные составляющие каждого элемента АС, а именно: технические средства, программное обеспечение, персонал и организационные меры обработки и защиты информации (различного типа инструкции, регламенты и приказы).

Пусть, учитывая ограничения модели, способность элемента АС выполнять заданные функции описывается статичным набором состояний: 1) работоспособное; 2) неработоспособное: отказ; сбой; ошибка.

Зададим способ формирования морфологического ящика как исследование сочетаний перечисленного набора состояний. Для проведения оценки защищенности необходимо определить те сочетания, которые могут негативно повлиять на изменение состояния защищенности информационной системы, и исключить сочетания, не влияющие на изменение интегрального показателя риска или частной функции полезности элемента.

В данном случае получаем 128 сочетаний, которыми можно описать все множество воздействий на элемент АС, при этом довольствуясь минимумом исходных данных, каковыми являются интенсивности отказов отдельных составляющих элемента АС. Полнота и достоверность выявленных связей между состояниями элементов АС, воздействующих или могущих воздействовать на информацию, достигаются

путем рассмотрения множества состояний всех составляющих элемента АС и, как следствие, всех факторов, воздействующих на все элементы АС и на всех этапах обработки информации [4].

Если нам известны вероятности наступления каждого из состояний для всех составляющих элемента АС $P_{sx}(E_i)$, тогда вероятность наступления связанного события P_s можно представить как совместную:

$$P_s = r_{si} r_{sj}, \text{ здесь } i, j \in [1 \ldots x].$$

Исследовав зависимости выбранных состояний друг от друга, формируем частную функцию полезности элемента на основе факторов:

$$u^*_{E_i} = F_1 \cap F_2 \cup F_3 \cap F_4 \cup F_5 \cap F_6 \cap F_7 \cup F_8 \cap F_9 \cap F_{10}, \quad (1)$$

где $u^*_{E_i}$ – частная функция полезности элемента АС; F_1, $F_2 \ldots F_{10}$ – факторы, влияющие на изменение состояния АС; $\cap$ – символ пересечения – между факторами есть зависимость; $\cup$ – символ объединения – между факторами нет явной зависимости.

Используя методы математической логики, (1) можно представить в виде $u^*_{E_i} = F_1 F_2 + F_3 F_4 + F_5 F_6 F_7 + F_8 F_9 F_{10}$.

Для проведения факторного анализа информационных рисков необходимо объект исследования рассмотреть с точки зрения логической, технической и структурной схем обработки информации в организации. При факторном анализе может использоваться как отдельно каждая из этих схем, так и все в совокупности, что даст более полную информацию для расчета результирующего показателя, т.е. уровня риска каждого элемента исследуемого объекта. При этом уровень риска каждого из элементов исследуемого объекта представляется в разрезе факторных показателей. На основании этих данных можно сделать вывод не только о том, какой из элементов наиболее уязвим, но и указать конкретную причину, снижающую уровень информационной безопасности.

Применение предложенного подхода учитывает причинно-следственные связи процессов обработки информации, влияющие на уровень защищенности информационных ресурсов. Использование факторного анализа является шагом к получению объективных количественных результатов в процессе управления информационной безопасности.

Научный руководитель – В.В. Золотарев, к.т.н., заместитель директора ИИТК.

ЛИТЕРАТУРА

1. Сафонов А.А. Теория экономического анализа: Учеб. пособие / Под ред. Л.В. Моисеевой. Владивосток: Изд-во Владивост. гос. ун-та эконом. и сервиса, 64 с.

2. Волкова В.Н., Денисов А.А. Теория систем и системный анализ: Учеб. для вузов. М.: Юрайт, 2010. 679 с.

3. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

4. Жуков В.Г., Золотарев В.В., Заблоцкая Н.С. и др. Применение факторного анализа и эволюционного алгоритма оптимизации для решения задачи управления информационными рисками систем электронного документооборота // Системы управления и информационные технологии. Воронеж: Научная книга, 2009. №3(37). С. 41–50.

УПРАВЛЕНИЕ И МОНИТОРИНГ РАБОЧИХ СТАНЦИЙ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ИЦ УВД ПО ТОМСКОЙ ОБЛАСТИ

М.А. Девяткин, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, max5252@vtomske.ru

Информационный центр (ИЦ) при Управлении внутренних дел по Томской области является самостоятельной структурной единицей, непосредственно подчиненной УВД по Томской области.

В данном подразделении эксплуатируется ЛВС, которая включает в себя более 70 ПЭВМ и более 10 программно-технических комплексов по различным направлениям служебной деятельности.

Таким образом, наличие в ИЦ такого большого количества компьютеров, распределенных на большой площади, требует постоянного контроля со стороны администратора, который должен поддерживать работоспособность всех рабочих станций в ЛВС и оперативно реагировать на любые изменения. При этом нельзя полагаться лишь на внимание системного администратора, необходимы автоматические и непрерывно действующие средства контроля. К тому же с ростом количества компьютеров сложность в осуществлении контроля возрастает.

Для того чтобы администратору не нужно было бегать от компьютера к компьютеру, проверять состояния отдельных служб и приложений, ждать оповещений от недовольных пользователей и тратить при этом большое количество времени, необходимо наличие централизованной системы управления и мониторинга. При этом основной задачей такой системы является повышение уровня информационной безопасности, благодаря осведомленности о состоянии рабочих станций и возможности осуществлять управленческие действия [1, 2].

Подобная система должна обладать следующими свойствами:

– управлять и осуществлять мониторинг рабочих станций централизованно, без непосредственного доступа к этим станциям;

– предоставлять администратору свежую информацию о состоянии всех компьютеров;

– иметь централизованную базу данных, в которую стекается собранная с рабочих станций информация;

– контролировать работу антивирусного программного обеспечения;

– иметь механизм создания отчетности для принятия управленческих решений;

– иметь возможность добавлять дополнительную информацию о каждом компьютере и его пользователе;

– обнаруживать изменения в конфигурации компьютеров;

– осуществлять резервное копирование данных;

– предоставлять простой пользовательский интерфейс.

При этом информация, получаемая от рабочих станций, нужна не только администратору, но и руководителю подразделения, а также инженеру по эксплуатации средств электронно-вычислительной техники. Использование таких программ позволяет повысить эффективность использования аппаратного и программного обеспечения и снизить вероятность возникновения сбоев в системе, что особенно важно для госструктур.

Недостатком большинства программ централизованного управления и мониторинга рабочих станций является их высокая стоимость, что оказывается очень важным фактором, поскольку для госструктур существуют бюджетные ограничения. К тому же подобное программное обеспечение зачастую весьма ограничено по функционалу [1].

Научный руководитель – Д.С. Анфиногенов, заместитель начальника ИЦ при УВД по Томской области.

ЛИТЕРАТУРА

1. Кустов Н.Т. Администрирование информационно-вычислительных сетей: Учеб. пособие. Томск: Том. гос. ун-т, 2004. 247 с.

2. Методы мониторинга и обеспечения безопасности для поддержания работоспособности корпоративной сети [Электронный ресурс]. Режим доступа: http://www.securitylab.ru

КЛЕТОЧНЫЕ АВТОМАТЫ В ЗАДАЧАХ ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ

О.О. Евсютин, аспирант; С.К. Росошек, науч. рук., к.ф.-м.н., доцент

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

Теория клеточных автоматов была разработана достаточно давно. Но традиционно клеточные автоматы использовались для моделирования физических процессов, при решении комбинаторных и вычислительных задач, задач прикладной кибернетики. Так, например, извест-

ный многим клеточный автомат под названием «Жизнь» описывает популяцию стилизованных организмов, развивающуюся во времени под действием противоборствующих тенденций размножения и вымирания.

Подробно клеточные автоматы описаны в [1]. Там даются все необходимые определения и рассматривается возможность моделирования физических явлений с помощью клеточных автоматов.

Упрощенно процесс развития клеточного автомата можно представить следующим образом. Есть некоторый клеточный автомат с решеткой заданного размера, клетки которой принимают значения из конечного множества. Выберем окрестность и сформируем таблицу правил, которая будет определять новое значение клетки для всех значений клеток окрестности. Зададим начальное состояние решетки клеточного автомата. После этого в течение нужного числа шагов будем изменять состояние решетки согласно таблице правил.

Данный процесс можно условно разбить на следующие этапы: мы берем некоторые начальные данные и представляем их в удобном для нас виде (начальное состояние решетки клеточного автомата); преобразуем эти данные по определенному алгоритму (правило клеточного автомата); получаем измененные данные (конечное состояние решетки клеточного автомата).

Таким образом, клеточные автоматы могут представлять интерес как средство решения различных задач преобразования информации, к которым можно отнести, в частности, шифрование и сжатие данных.

В данной статье рассматривается возможность построения алгоритма сжатия данных на основе клеточных автоматов. Выбор такого направления исследований связан с тем, что, несмотря на быстрое развитие средств вычислительной техники, проблема сокращения объема передаваемых и хранимых данных по-прежнему актуальна, в особенности применительно к звуковой, фото- и видеоинформации.

Идея построения алгоритма сжатия данных на основе клеточных автоматов заключается в предварительном преобразовании исходных данных с помощью клеточного автомата к виду, который обеспечит большую степень сжатия по сравнению с исходными данными. Естественно, что для этого должны использоваться прежде всего обратимые клеточные автоматы.

Таким образом, первоначальной задачей является исследование обратимых клеточных автоматов разных типов на предмет того, возможно ли построить на их основе эффективный алгоритм сжатия данных. Для этого необходима их программная реализация в виде машины клеточных автоматов. Кроме того, необходимо детально изучить существующие подходы к сжатию данных и, возможно, определить ту об-

ласть, в которой наиболее применимыми могут оказаться клеточные автоматы.

ЛИТЕРАТУРА

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

СИСТЕМА КОНТРОЛЯ ДОСТУПА К ТЕЛЕКОММУНИКАЦИОННЫМ ШКАФАМ

П.А. Галицкий, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, pavel.galitskiy@gmail.com

Системы управления и контроля доступом в настоящее время являются неотъемлемой частью многих современных систем безопасности. Они позволяют контролировать движение сотрудников и посетителей по охраняемой территории, не допускать посторонних и разграничивать доступ в ответственные помещения.

Томское производственное объединение «КОНТУР» выпускает телекоммуникационные шкафы различного назначения. Внутри монтажных конструктивов, как правило, устанавливается дорогостоящее оборудование, в том числе и оборудование, предназначенное для передачи информации (коммутаторы, маршрутизаторы и т.д.), поэтому необходимо обеспечить высокий уровень защиты от несанкционированного доступа.

Доступ обеспечивается при совпадении какого-либо идентификационного признака с тем, который установлен в качестве разрешенного. В зависимости от идентификационного признака (ИП) существуют различные устройства ввода ИП (УВИП). Они могут быть механические, оптические, акустические, электронные, биометрические, комбинированные [1]. Широкое распространение нашли электронные носители идентификационных признаков – идентификаторы доступа или просто идентификаторы. Эти устройства представляют собой переносные носители информации, на которые тем или иным способом записан код, являющийся идентификационным признаком. Распространены электронные идентификаторы, используемые как при контактном, так и при дистанционном вводе ИП. Наиболее перспективными являются бесконтактные карты Proximity и ключ-брелоки Touch memory.

В проектируемой системе в качестве идентификатора используется электронный ключ Touch memory, другое название – iButton. iButton – это микросхема, заключённая в стандартный круглый корпус из нержа-

веющей стали. Микросхема является постоянным запоминающим устройством, содержащим 6-байтный серийный номер, являющийся уникальным для каждого устройства.

Система контроля доступа является совокупностью различных компонентов (механических, электрических, программных и т.д.). Основные составляющие типичной системы контроля доступа:

– устройства, преграждающие управляемые (УПУ) в составе преграждающих конструкций и исполнительных устройств;

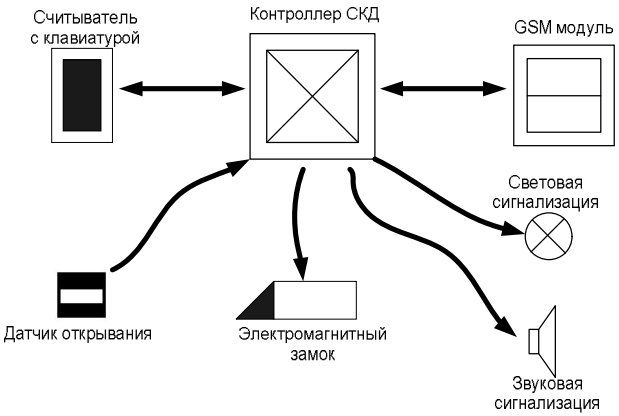
– устройства ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов;

– устройства управления (УУ) в составе аппаратных и программных средств.

В качестве УПУ выступают: двери, турникеты, электромагнитные и электромеханические замки, шлагбаумы и т.д. Устройства управления представлены в виде контроллеров СКУД и различных внешних аппаратных и программных средств.

В проектируемой системе для оповещения администратора необходимо использовать отправку SMS-сообщений. Для этого в составе СКД должен присутствовать GSM-модуль. Также в состав СКД входят: датчики открывания двери, световая и звуковая сигнализации, клавиатура для набора кода, электромагнитный замок.

На рисунке приведена структурная схема СКД.



Структурная схема проектируемой СКД

Использование GSM модуля позволяет не только оповещать о состоянии датчиков, но и управлять системой дистанционно. В результате проектируемая система гибка в настройке и использовании.

ЛИТЕРАТУРА

1. ГОСТ Р 51241–98. Технические средства защиты и охраны. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

2. ГОСТ 26139–84. Интерфейс для автоматизированных систем управления рассредоточенными объектами. Общие требования.

3. РД 78.36.002 – 99. Технические средства систем безопасности объектов. Обозначения условные графические элементов систем.

АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ АВТОРСТВА ТЕКСТА

А.О. Гальвас, студент 4-го курса

г. Томск, ТУСУР, каф. КИБЭВС, galart@t-sk.ru

В настоящее время существует несколько методов определения авторства текста и ни один не может отличаться стопроцентной эффективностью. Данная проблема достаточно актуальна, потому что до сих пор стоит вопрос об авторстве некоторых литературных произведений. Первая попытка создания методики для определения автора текста была сделана еще в самом начале XX в. Морозовым, который в своём исследовании использовал лингвистические спектры. Метод Морозова позднее был подвергнут критике и не приобрел дальнейшего развития.

В настоящий момент в связи с бурным развитием вычислительной техники встает вопрос о попытках автоматизировать процесс определения авторства. В частности, математиком Хетсо была предложена методика, основанная на методах математической статистики, использующая следующие параметры:

- Средняя длина слова в буквах, вычисляемая на основании выборок размером 500 текстовых слов.
- Общее распределение длины слова.
- Средняя длина предложения в словах, вычисляемая на основании выборок размером в 30 предложений.
- Общее распределение длины предложения.
- Лексический спектр текста на уровне словаря.
- Лексический спектр текста на уровне текста.
- Индекс разнообразия лексики.

В исследовании Хетсо используется общий принцип применения статистических методов. Для каждого метода определялась критическая граница $\alpha_{кр}$ и для каждой статьи определялся числовой параметр α, проверялись две гипотезы: H_1 – {если $\alpha < \alpha_{кр}$, то статья скорее всего принадлежит данному автору}; H_2 – {если $\alpha > \alpha_{кр}$, то статья скорее всего не принадлежит данному автору} и формулировалось заключение [2].

Позднее Д.В. Хмелев предложил методику определения авторства текста с использованием буквенной и грамматической информации, которая использует формальную математическую модель последовательности букв (и любых других элементов) текста как реализации цепи Маркова. Хмелев в исследовании использовал различные литературные произведения 82 авторов. Элементы текста кодировались числами от 0 до 32. Код 0 всегда соответствовал разделителю. Пусть у нас есть W писателей, у каждого из которых есть N_w текстов, где $w = 0,..., W–1$. В первую очередь подсчитывается Q_{ij}^{wn} – количество переходов из буквы i в букву j в тексте n ($n = 0, ..., N_w–1$) автора w ($w = 0, ..., W–1$). Чтобы найти предсказание автора текста $\hat{n}$ (известного автора $\hat{w}$) с использованием информации об авторстве всех остальных текстов всех авторов (включая автора $\hat{w}$), мы подсчитываем

$$Q_{ij}^{k} = \sum_{n=0}^{N_w-1} Q_{ij}^{kn}, \qquad Q_i^k = \sum_j Q_{ij}^k .$$

Для авторов $k \neq \hat{w}$, а для автора $\hat{w}$ мы исключаем текст $\hat{n}$ из обучающей выборки

$$Q_{ij}^{\hat{w}} = \sum_{n \neq \hat{n}} Q_{ij}^{\hat{w}n}, \qquad Q_i^{\hat{w}} = \sum_j Q_{ij}^{\hat{w}} .$$

Теперь вычисляем

$$\Lambda_k(\hat{w},\hat{n}) = -\sum_{i:Q_i^k>0} \sum_{j:Q_{ij}^k>0} Q_{ij}^{\hat{w}\hat{n}} \ln \frac{Q_{ij}^k}{Q_i^k}$$

и

$$\Lambda_{\hat{w}}(\hat{w},\hat{n}) = -\sum_{i:Q_i^{\hat{w}}>0} \sum_{j:Q_{ij}^{\hat{w}}>0} Q_{ij}^{\hat{w}\hat{n}} \ln \frac{Q_{ij}^{\hat{w}}}{Q_i^{\hat{w}}} .$$

Если отвлечься от вырожденных случаев $Q_{ij}^k = 0$ и $Q_i^k = 0$, то легко увидеть, что каждая $\Lambda_{\hat{w}}(\hat{w},\hat{n})$ – минус логарифм вероятности реализации текста $\hat{n}$ писателя $\hat{w}$ при условии, что он является реализацией марковской цепи с переходными интенсивностями $P_{ij}^k = Q_{ij}^k / Q_i^k$. Обоснование для отбрасывания вырожденных слагаемых дают результаты об оптимальной оценке максимума правдоподобия. Также определяется ранг $R_k(\hat{w},\hat{n})$ как ранг $\Lambda_k(\hat{w},\hat{n})$ среди $\{\Lambda_k(\hat{w},\hat{n}), k = 0,...,W-1\}$. Если текст соотнесен правильному автору, то ранг $R_{\hat{w}}(\hat{w},\hat{n}) = 0$. Если текст

соотнесен какому-либо другому автору, а правильный оказался на втором месте, то $R_{\hat{w}}(\hat{w},\hat{n})=1$, и т.д. [1].

Хмелев также предложил алгоритм, использующий сжатие данных. Дадим теперь «идеальное» определение относительной сложности в духе определения колмогоровской сложности: относительная сложность $K(A \mid B)$ текста A относительно текста B – это длина наименьшей программы в двоичном алфавите, которая переводит текст B в текст A. К сожалению, $K(A \mid B)$ невычислима, и неясно, как можно ее использовать на практике.

Некоторое грубое приближение к ней можно получить с помощью алгоритмов сжатия данных. Определим относительную сложность $C(A \mid B)$ текста A по отношению к тексту B следующим образом. Сожмем текст B в текст B' и текст $S = B{\cdot}A$ в текст S'. Теперь положим $C(A \mid B) = |S'| - |B'|$.

Нас будет интересовать применение функции $C(A \mid B)$ в задаче определения авторства. Предположим, что у нас имеются тексты n авторов. Отберем у каждого автора по контрольному тексту $U_1,...,U_n$. Все остальные тексты у каждого автора объединим в один текст $T_i,...,T_n$. Для каждого контрольного текста i авторство определяется следующим образом. Сначала определяется ранг R_i числа $C(U_i \mid T_1)$ в наборе чисел $\{C(U_i \mid T_i),..., C(U_i \mid T_n)\}$. Ранги принимают значения от 0 до $n - 1$. Если ранг R_i равен 0, то авторство i-го контрольного текста определено верно [1].

В заключение стоит отметить, что при большой длине текста описанные выше алгоритмы являются достаточно эффективными, что подтверждается результатами исследований.

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Кукушкина О.В., Поликарпов А.А., Хмелёв Д.В. Определение авторства текста с использованием буквенной и грамматической информации. 2001.

2. Хетсо Г. Принадлежность Достоевскому: к вопросу об атрибуции Ф.М. Достоевскому анонимных статей в журналах «Время» и «Эпоха». SOLUM FORLAG A.S.: OSLO 1986.

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ОТРАБОТКИ НАВЫКОВ ЗАЩИТЫ СЕРВЕРА*

И.Г. Ганюшкин, В.Е. Шильненков, студенты 3-го курса
г. Томск, ТУСУР, каф. КИБЭВС, GanyushkinIG@mail.ru

В условиях рыночной экономики информация имеет цену и ее утечка может повлечь различного рода потери, в первую очередь финансовые. Развитие информационных технологий и их повсеместное внедрение привели к упрощению процесса обработки информации пользователем, одновременно с этим усложнились информационные системы. Как известно, чем сложнее система, тем больше в ней потенциальных уязвимостей. Уязвимость-параметр, характеризующий возможность нанесения описываемой системе повреждений любой природы теми или иными внешними средствами или факторами [1].

Создание программного комплекса – тренажера, структура которого представлена на рис. 1, позволит приобрести и отработать навыки устранения уязвимостей информационной системы. В основе разрабатываемого комплекса лежит принцип работы программных средств, выполняющих диагностику готовности системы к защите информации. К таким технологиям относят ликтест (leaktest, тест на утечку данных) и чекеры (checker – система для поиска уязвимостей) [2, 3].

Рис. 1. Структура тренажера

Принципиально важным элементом тренажера является библиотека уязвимостей, схема обращения к которой представлена на рис. 2. Библиотека представляет собой хранилище специально созданных уязвимостей.

Для приближения к реальным ситуациям предполагается реализация функции, позволяющей проводить тренировку в форме соревнований. Схема возможной реализации подобного рода конкурсов представлена на рис. 3.

С помощью данного комплекса предполагается решение следующих задач:

* Выполнено в рамках проекта ГПО КИБЭВС-0905 – Специализированный сервер для взлома.

• допуск к работе лиц, удовлетворяющих соответствующим квалификационным требованиям в сфере IT-безопасности;

• обеспечение проведения подготовки и аттестации работников предприятий и учреждений в области IT-безопасности;

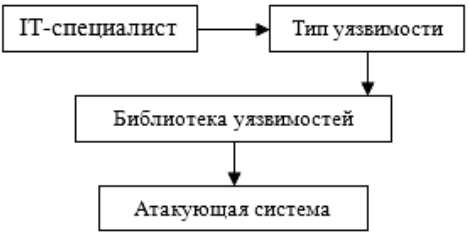


Рис. 2. Загрузка уязвимостей

Рис. 3. Структура соревнований

• отработка основных приемов в критических или чрезвычайных ситуациях;

• обучение работников служб безопасности действиям при критических или чрезвычайных ситуациях.

• анализ причин возникновения инцидентов и принятия мер по устранению выявленных причин;

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Ломакин П., Шрейн Д. Антихакинг. М.: Майор, 2002. 510 с.

2. Ликбез по ликтестам [Электронный ресурс]. Режим доступа: http://www.agnitum.ru/ news/securityinsight/issues/october2008, свободный. Загл. с экрана.

3. Серверный скрипт для поиска и проверки прокси серверов [Электронный ресурс]. Режим доступа: http://www.proxy-tool.net/, свободный. Загл. с экрана.

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ Wi-Fi-СЕТЕЙ К АТАКАМ ТИПА «EVIL TWIN». ИССЛЕДОВАНИЕ АТАКИ НА ПРИМЕРЕ Wi-Fi-СЕТИ ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ. МЕТОДЫ ЗАЩИТЫ

Д.В. Гаврилов, студент 4-го курса;
г. Томск, ТУСУР, каф. КИБЭВС, rs24@yandex.ru

В наше время получили развитие беспроводные сетевые технологии, такие как Wi-Fi, Bluetooth. Данные технологии достаточно удобные для передачи данных там, где нет возможности прокладывать ЛВС, а также очень удобны пользователям, так как большинство компьютеров оборудуются беспроводными сетевыми картами.

Однако проблема заключается в безопасной передачи данных по беспроводным сетям. В данной статье, пойдет речь об атаке на беспроводные сети «Evil Twin».

Суть атаки заключается в подмене «правильной» точки доступа, на пользовательскую точку доступа, для перехвата пользовательской информации.

Программные и аппаратные средства:

1. Ноутбук.
2. Wi-Fi-адаптер выполняющий режим AP (режим точки доступа).
3. Необходимое программное обеспечение.

Для того чтобы исследовать атаку, необходимо изменить SSID нашего адаптера на SSID оригинальной точки доступа (SSID: tusur).

Протестировано, что после подмены SSID все пользовательские адаптеры Wi-Fi переключаются на новую точку доступа без предупреждения, что найдена новая Wi-Fi-сеть, даже если Mac-адреса точек доступа совершенно разные.

Цель атаки заключается в перехвате пользовательской конфиденциальной информации, а именно логинов и паролей к системе. Чтобы перехватить пользовательские данные, применим фишинг-атаку.

Для этого установим web-сервер (Apache+PHP+MySQL) и создадим точную копию сайта http://vkontakte.ru . Почему был выбран именно этот ресурс? Потому что для аутификации в системе используется логин и пароль, логином является E-mail пользователя, а так как многие пользователи используют один и тот же пароль к разным системам, несложно догадаться, что после получения логина и пароля будет возможен вход и на E-mail адрес пользователя.

Была создана страница, которая сообщала пользователю, что на серверах производятся технические работы, и предлагала перейти к необходимому сайту (рис. 1).

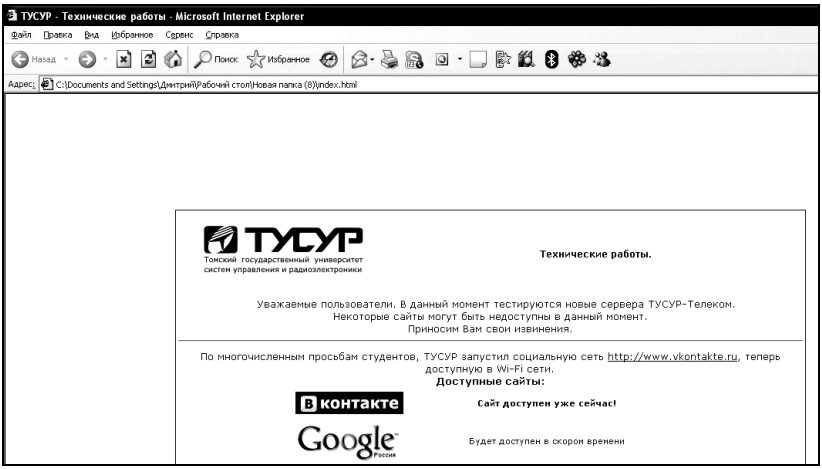


Рис. 1. Переадресация всех запросов на страницу

Когда пользователь переходил на сервис vkontakte.ru, он успешно «прощался» со своим логином и паролем к системе, простейший скрипт-сниффер (позволяющий сохранить введенные данные в форму, в СУБД Mysql) сообщал пользователю, что его пароль неверный, это позволяло точно удостовериться в правильности ввода логина и пароля (рис. 2). Замечу, что в адресной строке браузера адрес был, как у оригинального сайта, что вызывало большее доверие к сайту.

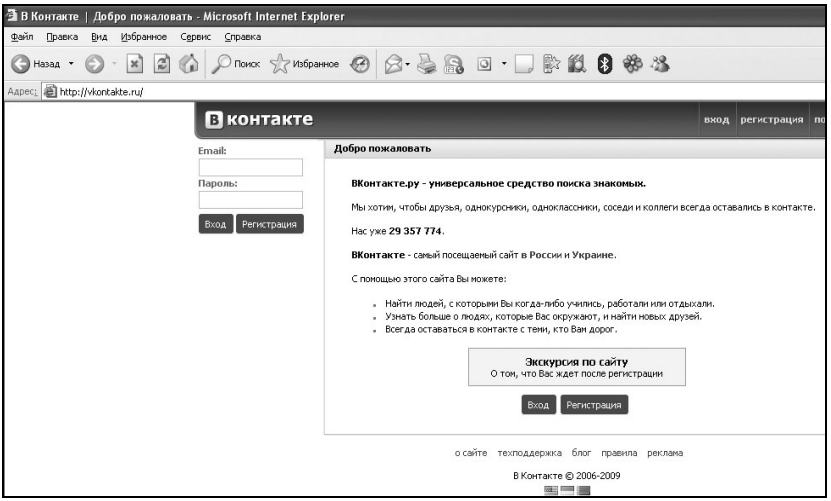


Рис. 2. Точная копия сайта

Для проверки работоспособности системы, были введены данные – E-mail и пароль, после этого просмотрена база данных, в которой сохранились эти данные.

Методы защиты. Пользовательские адаптеры узнавали как «родную» поддельную точку доступа, что можно считать непозволительно для организации сети.

Пора бы уже начать ставить сертификаты на сайты, в которых зарегистрировано большое количество людей, это бы решило проблему фишинга сайтов в сети Интернет.

Необходимо задумываться, в той ли сети находится человек, или если что-то вызвало подозрение, прекратить использование данной сети.

Научный руководитель – Ю.М. Филимонов, к.ф.-м.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. IEEE 802.11a стандарт протокола Wi-Fi.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ САЙТОВ

Д.С. Гордин, студент 4-го курса

г. Томск, ТУСУР, каф. КИБЭВС, gordan@docsis.ru

Современный мир невозможно представить без Всемирной паутины, а Всемирную паутину, в свою очередь, невозможно представить без ее главных составляющих – сайтов. Информационная защита сайтов в наше время должна быть основополагающим критерием при проектировании сайта. Но на деле это не так. Часто можно услышать тревожные сообщения в СМИ о том, что на днях хакерами был взломан интернет-ресурс крупной компании, и эта компания понесла большие убытки из-за взлома. Множество компаний каждый день все больше интегрируются в сеть Интернет, начиная от простого размещения информации о компании и заканчивая ведением всех стадий бизнеса, используя только Сеть. Сообщения о взломах сайтов появляются с завидной регулярностью, и со временем частота их появления растет. Это не говорит о том, что с каждым днем грамотность веб-программистов падает. Это говорит о том, что сложность проектируемых веб-систем с каждым годом, да что тут говорить – с каждым месяцем, растет. Из-за этого роста уследить за всеми потенциальными уязвимостями системы становится все сложнее.

Цель моего научного проекта – создать некое веб-приложение (сайт), которое в автоматическом режиме сможет показать информа-

цию и возможные уязвимости другого интернет-ресурса. Эта информация сможет упростить дальнейшую оценку информационной безопасности этого сайта. Ниже приведен список данных, которые могут помочь в аудите информационной безопасности.

Информация о сервере:

- ip;
- OS (по возможности);
- версия веб-сервера;
- другая информация (версия СУБД, интерпретатора и т.д.) (по возможности).

Информация о домене:

- full whois (из нескольких источников).

Информация о сайте:

- файловая структура сайта;
- открытые пути;
- версия CMS;
- версия и, насколько возможно, точный порядковый номер версии;
- установленные модули и плагины;
- список возможных паблик уязвимостей для данной версии и список возможных эксплоитов;
- уязвимые скрипты;
- sql-injection;
- xss;
- php-инклудинг.

В ходе выполнения работы список, возможно, будет меняться. В результате это будет веб-система, то есть это будет полностью серверное приложение. Должен заметить, у этого веб-приложения будет база данных, содержащая информацию о способах проведения атак (sql-injection, xss, php-инклудинг), и информацию, позволяющую правильно идентифицировать установленную CMS и установленные плагины к этой CMS. Эффективность работы создаваемого приложения будет зависеть исключительно от актуальности этой базы.

Само же приложение возможно будет написано на нескольких серверных языках программирования (пока PHP и Perl). Все будет зависеть от простоты и возможности реализации и дальнейшей модернизации некоторых функций на определенном языке. У проектируемого мною веб-приложения есть аналоги, но они часто специализированы только на одной области, например ищут только sql-injection и xss. В большинстве это клиентские приложения, и результат работы этих приложений зачастую оставляет желать лучшего. Это можно понять, ведь объем работ, который нужно провести для автоматизации поиска

уязвимостей, разновидности которых появляются, чуть ли не каждый день, должен быть колоссальным.

Любая компания должна заботиться о безопасности своих сайтов. Ведь, в первую очередь, это престиж компании, который долго зарабатывается и легко теряется.

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Фленов М.Е. PHP глазами хакера. СПб.: БВХ-Петербург, 2005. 304 с.

СИСТЕМА АУТЕНТИФИКАЦИИ ЧЕЛОВЕКА ПО РЕЧИ CAPTCHA

К.О. Изотов, студент 5-го курса;
Р.В. Мещеряков, науч. рук., к.т.н., доцент
г. Томск, ТУСУР, каф. КИБЭВС, enykeev@gmail.com

Тест Тьюринга – эмпирический тест, предложенный британским ученым Аланом Тьюрингом в 1950 г. Целью данного теста является ответ на вопрос: «Может ли машина мыслить?» Стандартная интерпретация этого теста звучит следующим образом: «Человек взаимодействует с одним компьютером и одним человеком. На основании ответов на вопросы он должен определить, с кем он разговаривает: с человеком или компьютерной программой. Задача компьютерной программы – ввести человека в заблуждение, заставив сделать неверный выбор» [1].

Существует и иная разновидность теста Тьюринга, в которой одну или более ролей машины и человека поменяли местами. Таким образом, задачей компьютера будет определить, с кем он беседовал: с человеком или же с другим компьютером. Одной из наиболее популярных интерпретаций такой разновидности теста Тьюринга является CAPTCHA (от англ. «Completely Automated Public Turing test to tell Computers and Humans Apart» – полностью автоматизированный публичный тест Тьюринга для различия компьютеров и людей), появившаяся в 2000 г. Основная идея теста: предложить пользователю такую задачу, которую может решить человек, но которую крайне трудно научить решать компьютер. В основном это задачи на распознавание символов.

Интересное решение было предложено в 2005 г. Луисом Ван Ан, профессором университета Карнеги – Меллона, Питтсбург, США. Он предложил использовать обратный тест Тьюринга для распознавания

старых книг и аудиозаписей. В связи с процессом старения и низким качеством печатной (записывающей) аппаратуры данные исходные материалы обладают реалистичной картиной шумов, делающей невозможным автоматическое распознавание, и, одновременно, легко воспринимаются человеком. Созданный им проект reCAPTCHA обрабатывает более 200 миллионов запросов в сутки, что эквивалентно 500 распознанным книгам или 36 тысячам человеко-часов, потраченных на их распознавание [2].

Слабым местом reCAPTCHA является функция аудиотестирования. Построенный на основе отрывков английской речи, данный тест невозможно пройти человеку без уверенного знания английского языка.

Целью работы является создание русскоязычного аналога проекта reCAPTCHA, полностью совместимого с оригиналом (идентичные форматы обмена информацией, схожие внешний вид клиентских модулей и механизмы работы). Такого рода совместимость повысит отказоустойчивость системы и позволит пользователю самостоятельно выбрать удобный для него язык тестирования, повысит привлекательность проекта для веб-разработчиков.

Схема клиент-серверного взаимодействия приведена на рисунке.

В процессе создания собственного ресурса веб-разработчик регистрируется в системе, вводит список доменов, для которых он планирует использовать АС, и получает для каждого из них публичный и приватный ключ. Также разработчик должен скачать и подключить к своему ресурсу javascript-модуль (в котором должен быть указан публичный ключ) и backend-модуль (с приватным ключом) либо написать их самостоятельно на основе предоставленного API.

Рис. 1. Схема клиент-серверного взаимодействия

При входе пользователя на страницу, требующую прохождения теста, браузер пользователя запрашивает и отрисовывает форму, а также получает аудиофрагмент и идентификатор сессии, соответствующий выданному фрагменту. Пользователь вводит требуемые данные и отправляет их на сервер приложений, который, в свою очередь, отправляет ответ пользователя, ключ его сессии и приватный ключ на сервер верификации. Сервер верификации сравнивает полученные от пользователя данные с соседними выданному, ранее распознанными фрагментами и, если совпадение найдено, возвращает TRUE. При получении положительного ответа сервер приложений возвращает пользователю информацию и/или выполняет определенные действия, для которых было необходимо прохождение теста.

Проблема определения человека особо остро встала с момента появления первых сайтов социальной направленности и до нынешнего времени не решена окончательно. Недобросовестные пользователи всё чаще прибегают к услугам автоматизированных систем для рассылки сообщений рекламного характера, разработчики таких систем всё чаще встраивают в свои программы механизмы распознавания изображений и аудиозаписей на основе генетических алгоритмов и нейронных сетей.

Приведенный в работе способ защиты благодаря использованию записей речи большого количества людей, взятых из разных источников, позволяет свести эффективность вредоносных автоматизированных систем к минимуму. При этом, в отличие от многих схожих решений, он не вызывает затруднений даже у людей с дефектами зрения.

Отдельным преимуществом данной системы является распознание речи – функции, так и не реализованной достаточно хорошо для использования в промышленных масштабах, хотя необходимость в ней назрела уже давно.

Разработанная система подлежит реализации в виде публичного веб-сервиса, позволяющего интегрировать функцию тестирования в модули аутентификации сайтов-посредников.

ЛИТЕРАТУРА

1. Тьюринг А.М. Вычислительные машины и разум // Хофштадер Д., Деннет Д. Глаз разума. Самара: Бахрах-М, 2003. С. 47–59.

2. reCaptcha. About Us. [Электронный ресурс]. Режим доступа: http://recaptcha.net/aboutus.html

ПРИВЕДЕНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ЗАО АКБ «СИБИРЬГАЗБАНК» В СООТВЕТСТВИЕ С ТРЕБОВАНИЯМИ ЗАКОНОДАТЕЛЬСТВА «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

В.В. Компанец, студент 5-го курса;
Н.А. Новгородова, науч. рук., ст. преп.
г. Томск, ТУСУР, каф. КИБЭВС, memfis_tm@mail.ru

Все мероприятия по приведению ИСПДн в соответствие с требованиями законодательства о персональных данных можно разделить на организационные и технические. К организационным мероприятиям можно отнести написание различных положений, инструкций, актов, а к техническим – анализ существующих средств защиты информации, внедрение новых средств защиты информации, выявление каналов утечки информации [1].

В настоящее временя в ЗАО АКБ «Сибирьгазбанк» (Банк) эксплуатируются три информационные системы, обрабатывающие персональные данные:

– «Банковский информационный комплекс ЦФТ – Банк – Платформа развития на базе Oracle» (ЦФТ – Банк);

– «Универсальная система автоматизации банковских сервисов 3Card-R» (3Card-R);

– «Программно-технологический комплекс DepoNet Pro» (DepoNet).

Для защиты данных ИСПДн используются организационные, программные и инженерно-технические средства.

Основной задачей при приведении ИСПДн Банка в соответствие с требованиями законодательства «О персональных данных» было выполнение классификации трех ИСПДн, составление для них моделей нарушителя и моделей угроз, а также проведение анализа соответствия трех ИСПДн требованиям руководящих документов ФСТЭК. По окончании анализа соответствия необходимо составить список мероприятий и документов, которые необходимы для соответствия требованиям приказов и руководящих документов в области защиты персональных данных.

В ходе классификации все три ИСПДн были признаны специальными и согласно Приказу ФСТЭК/ФСБ/Мининформсвязи России от 13 февраля 2008 г. №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» присвоение класса ИСПДн выполняется по построенной модели угроз. Также в ходе классификации было установлено, что ИСПДн ЦФТ-Банк и 3Card-R являются распределенными, а ИСПДн DepoNet – локальной [2].

В ходе построения моделей нарушителя было установлено, что для всех трех ИСПДн актуальными являются внешние нарушители, а также

внутренние нарушители первой и второй категории. Для ИСПДн ЦФТ-Банк и 3Card-R актуальными являются еще и внутренние нарушители третьей категории.

В ходе построения моделей угроз было установлено, что актуальными для всех трех ИСПДн являются следующие угрозы:

– угрозы, реализуемые в ходе загрузки операционной системы;

– угрозы, реализуемые после загрузки операционной системы;

– угрозы выявления паролей;

– распространение файлов, содержащих несанкционированный исполняемый код;

– комбинированные угрозы, представляющие собой сочетания актуальных угроз.

К угрозам, реализуемым в ходе загрузки операционной системы, можно отнести загрузку с отчуждаемых носителей, изменение исходной процедуры загрузки операционной системы или файлов, используемых при загрузке. Посредством реализации данной угрозы возможно получить доступ к хранимым на жестких дисках базам данных, содержащим персональные данные, к компьютерам, на которых обрабатываются персональные данные. Данная угроза в Банке является актуальной и не реализуемые меры по ее предотвращению являются недостаточными.

К угрозам, реализуемым после загрузки операционной системы, можно отнести различные угрозы, результатом которых может явиться утечка персональных данных по возможным несанкционированным каналам. Предотвращение данной угрозы возможно посредством устранения возможных каналов утечки. Данная угроза в Банке является актуальной, но реализуемые меры по ее предотвращению являются достаточными.

Угроза выявления пароля может быть направлена как на операционную систему, так и на саму информационную систему, в которой выполняется непосредственная обработка персональных данных. Данная угроза в Банке является актуальной, но реализуемые меры по ее предотвращению являются достаточными.

Угроза распространения файлов, содержащих несанкционированный исполняемый код, может влиять как на сами элементы ИСПДн, так и на персональные данные. Данная угроза в Банке является актуальной, но реализуемые меры по ее предотвращению являются достаточными.

Комбинированная угроза является сочетанием всех актуальных угроз. При сведении всех актуальных угроз к минимуму возможность реализации комбинированной угрозы минимальна.

По построенной модели угроз всем трем ИСПДн был присвоен 3-й класс.

В ходе анализа соответствия требования руководящему документу ФСТЭК России от 15 февраля 2008 г. «Основные мероприятия по орга-

низации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» было установлено несоответствие по следующим моментам:

– используемые средства защиты персональных данных не имеют сертификатов на отсутствие недекларированных возможностей;

– используемые межсетевой экран, антивирусное программное обеспечение, средство анализа защищенности не имеют необходимых сертификатов;

– используемый межсетевой экран не обеспечивает контроль своей программной и информационной части в процессе загрузки и динамически;

– не выполняется периодическая проверка на предмет наличия вредоносного программного обеспечения в средствах защиты;

– не выполняется контроль целостности программных средств защиты, неизменности программной среды;

– отсутствует лицензия по технической защите конфиденциальной информации.

ЛИТЕРАТУРА

1. Федеральный закон № 152 от 27 июля 2006 г. «О персональных данных» [Электронный ресурс]. Режим доступа: http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html, свободный.

2. Приказ ФСТЭК/ФСБ/Мининформсвязи России от 13 февраля 2008 года №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» [Электронный ресурс]. Режим доступа: http://www.rg.ru/2008/04/12/informaciya-doc.html, свободный.

3. Руководящий документ ФСТЭК России от 15 февраля 2008 г. «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных».

БЕЗОПАСНОСТЬ БАЗЫ ДАННЫХ ПО ГРУППОВОМУ ПРОЕКТНОМУ ОБУЧЕНИЮ*

В.М. Козлов, Р.Ю. Ибрагимов, К.А. Нечаев, студенты 3-го курса;
Н.А. Новгородова, науч. рук., ст. преп.
г. Томск, ТУСУР, каф. КИБЭВС, akadelpher@gmail.com

Групповое проектное обучение (ГПО) является инновационной особенностью процесса обучения в Томском государственном университете систем управления и радиоэлектроники. В ходе работы проект-

* Выполнено в рамках проекта ГПО КИБЭВС-0902 – Инженерия баз данных.

ных групп возникают проблемы обмена информацией между участниками группы и руководителями, а также зачастую между сотрудничающими группами.

В рамках задачи разработки автоматизированной системы учета и управления ГПО было принято решение снабдить систему возможностями документооборота с гибким разграничением прав доступа к документам и возможностью пользоваться ей всем участникам ГПО. Для решения данной задачи используется система управления реляционными базами данных (РСУБД) как наиболее зарекомендовавший себя вариант.

Основными участниками системы являются студенты и руководители. Студенты могут менять группы (переводится из одной в другую), поэтому удобнее всего использовать модель для хранения информации о пользователе, представленную на рис. 1.

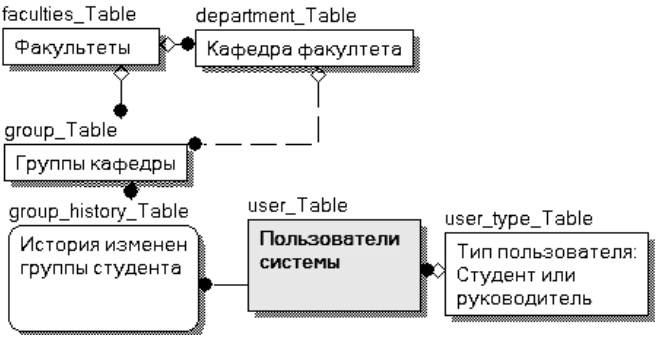


Рис. 1. Пользователи системы

Следующим важным аспектом системы является контроль за нахождением пользователей на проектах и подпроектах ГПО. Необходимо иметь возможность назначить или исключить студента или руководителя на проект ГПО.

Наибольшее внимание при защите проектируемой базы данных было отведено созданию и доработке матрицы доступа. Несмотря на то, что проектируемая база имеет особый способ распределения полномочий, матрица доступа также необходима для более надёжной защиты. Имеется 6 различных ролей (гость, студент, ответственный студент, научный руководитель, главный руководитель, работник деканата). Список прав стандартен для большинства баз данных, а их комбинация с различными уровнями доступа (только для своей учётной записи, в пределах проекта, в пределах ГПО, не ограничено) даёт более надёжную защиту (рис. 2).

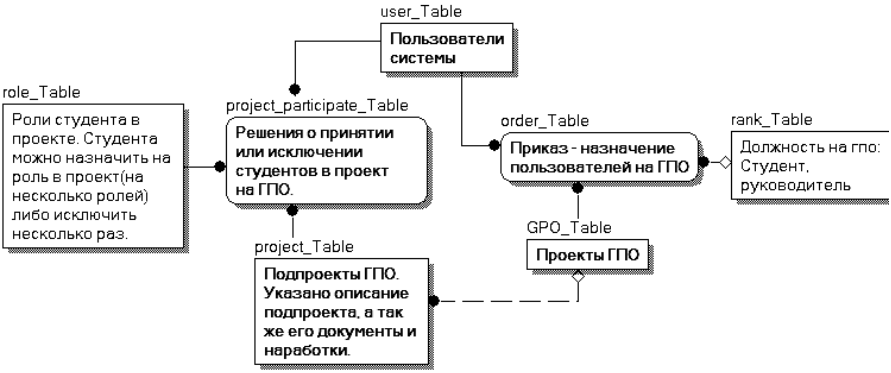


Рис. 2. Членство в группах

В ходе работы над безопасностью был также проведён анализ возможных рисков, которые могут возникнуть на различных этапах работы с базой данных. В результате наибольшее влияние имеют ошибки при постановке цели проекта, ошибки ответственных лиц и потеря данных.

Главной особенностью описанного подхода к решению задачи являются её гибкость и возможность совершенствования. Так, вокруг документа могут создаваться системы атрибутов, контроля версий документа, списков вложений в документ, не меняя уже созданной структуры.

ЛИТЕРАТУРА

1. Аутентификация, шифрование, защита программ, контентная фильтрация [Электронный ресурс]. Режим доступа: http://www.aladdin.ru

2. Защита баз данных [Электронный ресурс]. Режим доступа: http://azone-it.ru/index.php?option=com_content

3. IBDI Really Useful: Some Solutions to Old Problems [Электронный ресурс]. Режим доступа: http://www.ibase.ru/devinfo

4. Программирование баз данных SQL Server 2005 для профессионалов. [Текст]/ Роберт Виейра: Пер. с англ. М.: ООО «И.Д. Вильямс»; Диалектика, 2008. 1072 с.

ГЕНЕРАТОР СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Д.В. Кручинин, Е.А. Сопов, студенты 4-го курса;
Ю.М. Филимонов, науч. рук., к.ф.-м.н., доцент
г. Томск,ТУСУР, каф. КИБЭВС, kru_div@mail.ru

В последнее время, в век информатизации и глобализации, открыто встает вопрос о информационной безопасности, так как потеря ин-

формации может нанести непоправимый ущерб для ее владельца. Для того чтобы уменьшить вероятность угроз безопасности и негативных последствий данного события, необходимо грамотно и рационально подойти к вопросу проектирования системы безопасности и ее исследованию на уязвимость.

Наша работа, в рамках проекта ГПО №1001 «Исследование моделей систем безопасности методом имитационного моделирования», заключается в исследовании различных моделей систем безопасности на нарушения: правил разграничения доступа и реализации нелегальных потоков. За основу берется метод Монте-Карло. Как и для иммитации в реальных физических системах, необходимо использовать генератор случайных последовательностей для построения и «жизни» модели системы безопасности, фиксируя различные нарушения разграничения прав и целостности системы.

Нами разработан генератор случайных последовательностей, реализованный на основе датчика, за датчик был взят микрофон. Сигнал снимается программно с микрофона, под операционной системой Windows.

Звук в семействе ОС Windows. В Windows нет разделения каналов записи по источникам. Все поступающие в систему звуки смешиваются, и лишь после этого их получает программа (рис. 1).

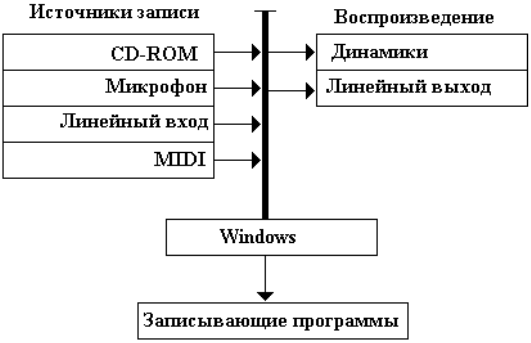


Рис. 1. Структурная схема устройства аудиосистемы в Windows

Для получения звукового сигнала нужно воспользоваться WinAPI. WaveInOpen открывает доступ к микрофону. Одновременно только одна программа может работать с микрофоном. Неодходимо указать частоту дискретизации, размер буфера. От последнего зависит, как часто и в каком объеме информация будет поступать в программу.

Нужно выделить память для буфера и вызвать функцию WaveInAddBuffer, которая передаст Windows пустой буфер. После вызова WaveInStart Windows начнет заполнять буфер и, после его заполнения, пошлет сообщение MM_WIM_DATA. В нем нужно обработать

полученную информацию и вновь вызвать WaveInAddBuffer, тем самым указав, что буфер пуст. Функции WaveInReset и WaveInClose прекратят поступление информации в программу и закроют доступ к микрофону.

На основе вышеописанного метода работы со звуком был реализован класс. При создании экземпляра класса начинаются считывание, обработка и запись в указанный файл. При деконструкции экземпляра класса запись прерывается.

Наша программа позволяет выбрать количество данных, имя файла. Интерфейс программы изображен на рис. 2.

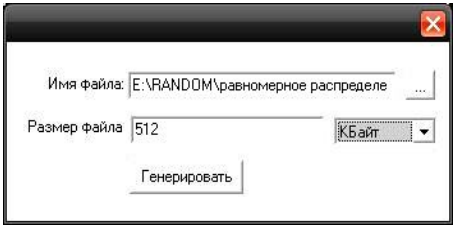


Рис. 2. Генератор случайных последовательностей

С помощью вышеописанного генератора случайных последовательностей была сгенерированна последовательность, состоящая из 8-битных чисел, и ее функция вероятности изображена на рис. 3.

Рис. 3. Функция вероятности сгенерированной случайной последовательности

Начат более детальный анализ получаемых последовательностей, основанный на статистическом тестировании.

ЛИТЕРАТУРА

1. Соболь И.М. Численные методы Монте-Карло. М.: Наука, 1973. – 312 с.

2. Federal Information Processing Standards Publication 140-1. Announcing the Standard for SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES. M., 1994. 105 с.

3. интернет ресурс: http://msdn.microsoft.com/

ГЕНЕРАЦИЯ ДИСТРИБУТИВОВ ОПЕРАЦИОННЫХ СИСТЕМ

А.А. Кучкильдин, студент 5-го курса
г. Томск, ТУСУР, каф. КИБЭВС, kandrey88@gmail.com

Установка операционной системы Windows XP не вызывает особых трудностей даже у начинающих пользователей персонального компьютера, не говоря об опытных пользователях. Однако что делать, если Windows необходимо устанавливать не на один компьютер, и не раз в год, а ежедневно? Системные администраторы часто сталкиваются с надобностью устанавливать операционную систему на большое количество ПК, что требует много времени и усилий. К тому же постоянные вопросы мастера установки об имени пользователя, регионе и серийном номере порядком надоедают. В этой статье речь пойдет о создании дистрибутива Windows XP, который бы устанавливался автоматически**,** т.е. без надобности вводить серийные номера и прочую стандартную информацию.

Процесс установки операционной системы, имея дистрибутив, довольно прост. Однако установка ОС – это еще далеко не все, ведь после этого следуют рутинные процессы настройки ОС, установки Service Pack, обновлений к ОС, всех необходимых драйверов, прикладных программ и утилит. И именно этап отладки ОС занимает куда больше времени, чем установка самой операционной системы. При этом не стоит забывать, что под рукой нужно иметь не только диск с дистрибутивом ОС, но и диск со всеми драйверами, любимыми программами и утилитами. Видимо, все, кому доводилось выполнять эту задачу, задумывались над возможностью полной автоматизации процесса установки, автоматизации, при которой не нужно вводить серийный номер ОС, отлаживать ее, устанавливать массу драйверов и т.д. Идеальным в этом смысле представляется такой процесс установки, когда с одного загрузочного компакт-диска без участия пользователя можно установить операционную систему с Service Pack (SP) со всеми драйверами и утилитами и получить на выходе полностью настроенную ОС. Подведя итог, можно сказать, что актуальность задачи автоматизации процесса установки операционной системы не подлежит сомнению.

Существует много способов создания дистрибутивов. Можно создать его вручную, а можно и с помощью программ. Помочь автоматизировать установку могут nLite, Windows Unattended CD Creator и многие другие. Для работы понадобится только лицензионный ключ XP. В данной статье будет рассмотрен способ создания дистрибутива с помощью утилиты nLite. nLite – это программа для работы с дистрибутивами Windows XP, Windows 2000 или Windows 2003. При помощи nLite можно интегрировать предварительно загруженные пакеты обновлений исправлений. nLite предоставляет широкие возможности для «выреза-

ния» из дистрибутива различных компонентов, которые обычно устанавливаются по умолчанию. Это позволяет уменьшить общий объем инсталляционных файлов и сэкономить место на диске после установки системы. nLite позволяет заранее сконфигурировать разнообразные настройки системы при помощи многочисленных твиков, заложенных в программу. Таким образом, после инсталляции вам уже не понадобится тратить время на настройку системы. nLite предоставляет графический интерфейс для создания файла ответов для автоматической установки Windows. И, наконец, при помощи nLite можно создать образ загрузочного диска (ISO), который потом легко записать на CD/DVD. Все вышеперечисленные задачи выполняются через удобный графический интерфейс программы.

Программа действительно очень удобна для выполнения различных задач. В то же время она является очень мощным средством модификации дистрибутива. Выполняя изменение системных файлов, удаление компонентов или включение твиков, необходимо совершенно отчетливо представлять, к каким последствиям это может привести. Необдуманное удаление компонентов или отключение служб может повлечь за собой неработоспособность системы. Более того, массовое отключение компонентов или включение твиков реестра делает отслеживание причин некорректной работы системы очень сложной задачей, а вернуть компоненты на место после установки системы может быть просто невозможно.

Научный руководитель – А.А. Конев, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Автоматическая установка Windows // www.oszone.net : компьютерный информационный портал. URL: http://www.oszone.net/2747/

МОТИВАЦИЯ СТУДЕНТОВ*

Н.В. Кумушбаева, Е.В. Шмитько – студенты 3-го курса;
Е.М. Давыдова, науч. рук., к.т.н., доцент
г. Томск, ТУСУР, каф. КИБЭВС, madmasele@sibmail.com

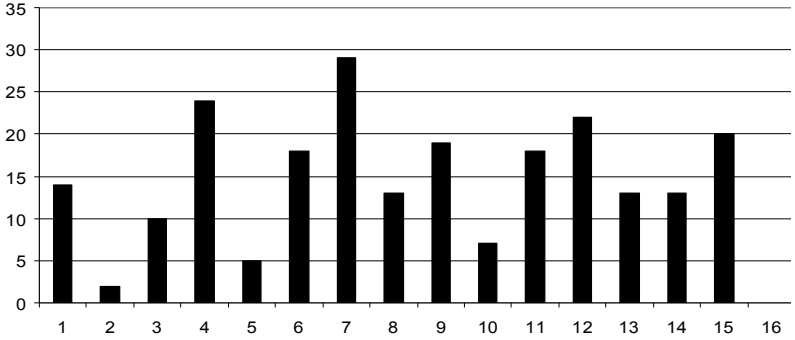
Что побуждает студентов к учебе? Почему одни учатся с удовольствием и сдают сессии в срок, получая только положительные оценки, а другие редко посещают пары и кое-как сдают на тройки? Дело не толь-

* Выполнено в рамках проекта ГПО КИБЭВС-0906 – Исследование процессов накопления знаний.

ко в индивидуальных склонностях и способностях каждого учащегося, но и в факторах, влияющих на мотивацию студентов к обучению, таких как материальное положение, состояние здоровья, возраст; семейное положение, уровень довузовской подготовки; владение навыками самоорганизации, планирования и контроля своей деятельности и др.

Анализу этих особенностей и выявлению факторов, влияющих на мотивацию студентов к обучению, с целью повышения эффективности учебно-воспитательного процесса и посвящена настоящая работа, выполненная в рамках группового проектного обучения.

Среди студентов пятых курсов кафедры КИБЭВС провели опрос. Из списка предложенных мотиваций нужно было выбрать наиболее подходящие либо расставить мотивации в порядке значимости. Всего в анкетировании приняло участие 40 человек. Из каждой анкеты были выделены несколько (4–7) пунктов с наивысшим приоритетом, после чего по каждому пункту был вычислен суммарный бал и высчитан процент от общего числа опрошенных.



Результаты опроса

Цифрами на рисунке обозначены следующие мотивы:

1) долг, ответственность;
2) желание занять определенное место в группе;
3) желание стать полноценным членом общества;
4) лучше подготовиться к профессиональной деятельности;
5) одобрение преподавателей;
6) ориентация на новые знания;
7) получить высокооплачиваемую работу;
8) потребность в постоянном духовном и интеллектуальном росте;
9) престижность высшего образования;
10) процесс решения познавательных задач;
11) самообразование;

12) сознание нужности высшего образования;
13) стремление к творческой и исследовательской деятельности;
14) стремление повысить свой культурный уровень;
15) стремление расширить кругозор и эрудицию [1].

Результаты сравнительного исследования познавательных мотивов и мотивов развития личности представлены в табл. 1. Итоги изучения социальных мотивов, мотивов достижения систематизированы в табл. 2.

Таблица 1

Познавательные мотивы и мотивы развития личности (в % к числу опрошенных)

Мотивы	%
Стремление к творческой и исследовательской деятельности	31
Процесс решения познавательных задач	15
Самообразование	46
Ориентация на новые знания	44
Потребность в постоянном духовном и интеллектуальном росте	33
Стремление расширить свой кругозор и эрудицию	49
Стремление повысить свой культурный уровень	33

Таблица 2

Мотивация учебной деятельности студентов (в % к числу опрошенных)

Стимулы к учебе	%
Сознание нужности высшего образования	56
Престижность высшего образования	49
Желание стать полноценным членом общества	26
Долг, ответственность	36
Желание занять определенное место в группе	5
Ооодобрение преподавателей	13
Лучше подготовиться к профессиональной деятельности	62
Получить высокооплачиваемую работу	74

Из полученных результатов в блоке познавательных мотивов наиболее наибольший вес имеет «стремление расширить свой кругозор и эрудицию» и мотивы «самообразования» и «ориентация на новые знания».

В блоке мотивации к учебной деятельности наибольший вес имеет группа мотивов достижения, такие как «получить высокооплачиваемую работу», «лучше подготовиться к профессиональной деятельности». То есть студенты пятого курса уже отчетливо понимают, что успешная учеба в вузе будет являться основой их становления как настоящих специалистов и что их знания пригодятся для достижения материального благополучия.

Результаты исследования показывают, что мотивы социальной идентичности (желание занять определенное место в группе, одобрение преподавателей) не имеют значения для мотивации учебной деятельности студентов.

ЛИТЕРАТУРА

1. Малинаускаус Р.К. Мотивация студентов разных периодов обучения. Каунас, 2004.

ИССЛЕДОВАНИЕ РЕАЛИЗАЦИЙ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Г.И. Кузнецов, студент 5-го курса;
Ю.М. Филимонов, науч. рук., к.ф.-м.н.
г. Томск, ТУСУР, каф. КИБЭВС, aligator_4@sibmail.com

Криптографическая подсистема является составной частью системы защиты информации от несанкционированного доступа [1] и реализована в операционных системах семейства Windows как служба поставщика криптографии – криптопровайдер. Эта служба позволяет осуществлять криптографические операции, к которым относятся генерация ключей, шифрование и расшифрование данных, выработка и проверка электронной цифровой подписи (ЭЦП). Алгоритмы шифрования и выработки ЭЦП являются стандартами, прошедшими многочисленные тесты, и гарантируют пользователям высокий уровень криптостойкости. В цепи криптографических операций слабым звеном оказывается генерация ключевой информации. Для генерации ключей шифрования предпочтительно использовать аппаратные датчики случайных чисел, прошедшие соответствующие тесты [2]. Аппаратные датчики случайных чисел являются внешними устройствами по отношению к компьютеру. Поэтому все поставщики услуг криптографии имеют в своем арсенале программные средства для создания ключей, генераторы псевдослучайных чисел с внешним источником энтропии. Как показали исследования, генератор случайных чисел в операционной системе Windows 2000 дает неслучайную последовательность [3].

В связи с этим возникает вопрос, как реализован датчик случайных чисел у других поставщиков служб криптографии. В данной работе проведено исследование генераторов ключей поставщика служб криптографии компании «Крипто-Про» (КриптоПро CSP) и аппаратного датчика случайных чисел, реализованного в USB-ключах eToken фирмы «Аладдин». КриптоПро CSP вызывается через интерфейс

CryptoAPI 2.0. Использование интерфейса CryptoAPI 2.0 дает нам доступ к криптографическим функциям для генерации ключей.

Были выбраны три функции:

− Функция CPCGenKey() генерирует случайные криптографические ключи или ключевую пару (закрытый/открытый ключи).

− Функция CPCDeriveKey() производит криптографические ключи сессии на основе значения хеш-функции, вычисленной по другим ключам, паролям или любым другим данным пользователя.

− Функция CPCGenRandom() заполняет буфер случайными байтами.

Проведены серии экспериментов, в которых получены случайные последовательности и проверенные по тестам FIPS [2]. Для USB-ключа eToken PRO протестирована аппаратная реализация генерация ключевых пар RSA 1024/2048.

ЛИТЕРАТУРА

1. Руководящий документ Гостехкомиссии РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

2. FIPS PUB 140-1. Security Requirements for Cryptographic Modules.

3. Zvi Gutterman, Benny Pinkas. Cryptanalysis of the Random Number Generator of the Windows Operating System. 2007. 24 с.

МЕТОДИКИ ТЕСТИРОВАНИЯ БЫСТРОДЕЙСТВИЯ АППАРАТНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРА

В.А. Лавриненко, студент 5-го курса

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

Эффективность использования ПК в большой степени определяется количеством и типами устройств, которые могут применяться в его составе. Широкая номенклатура устройств, разнообразие их технико-эксплуатационных характеристик и знание этих характеристик дают возможность пользователю выбрать такие конфигурации ПК, которые в наибольшей степени соответствуют его потребностям и обеспечивают рациональное решение его задачи.

Объектом исследования в данной работе являются методики тестирования быстродействия аппаратного обеспечения компьютера, с целью максимально эффективного конфигурирования компьютера для выполнения поставленных задач.

Методика тестирования быстродействия компьютерных систем разбита на несколько более узких направлений. Служит это для того, чтобы не сравнивать между собой быстродействие конкретных систем

в тех задачах, в которых их использование не предусмотрено самим производителем, в результате чего подобное сравнение, даже если его провести, становится абсолютно бессмысленным (например, методика тестирования домашнего компьютера будет отличаться от тестирования рабочей станции).

Результатом тестирования быстродействия компьютерной системы в рамках одной из методик является средний балл быстродействия, полученный путём усреднения результатов конкретных тестов, входящих в методику.

Обзор классов программ, используемых для разработки методики

– *Пакеты трехмерного моделирования.*

Этот класс программ традиционно относится к ресурсоёмкому программному обеспечению, используемому, как правило, профессионалами. Пакеты трёхмерного моделирования в режиме рендеринга дают высокую нагрузку на процессор, в режиме интерактивной работы – на подсистему процессор–память и 3D-акселератор. Практически все пакеты трёхмерного моделирования требуют достаточного объёма ОЗУ.

– *Программы класса CAD/CAM/CAE.*

Пакеты, используемые практически исключительно профессионалами, требуют очень много времени на освоение и очень дорогостоящие. Предназначены для использования в производстве, для моделирования различных процессов или для использования инженерами при разработке и проектировании различных узлов. Критичны к производительности всех без исключения составляющих компьютерной системы, очень требовательны к объёму ОЗУ.

– *Компиляторы.*

Нагрузка при тесте распределяется примерно в равной степени между процессором, подсистемой памяти и дисковой подсистемой. С целью уменьшения влияния последней перед проведением тестов запускается процесс дефрагментации.

– *Синтетические и полусинтетические тесты.*

Программы, основной задачей которых является определение предельно возможной производительности компьютера на относительно несложных, но очень часто используемых операциях. Результаты этих тестов не имеют прямого отношения к быстродействию тестируемой системы в реальном ПО, но могут быть использованы для «экспресс-сравнения» компьютерных систем между собой.

– *Программы архивирования.*

Программы, используемые практически всеми, независимо от профессионального или любительского статуса. Критичны к скорости процессора и подсистемы памяти, частично зависят от скорости дисковой подсистемы.

– *Программы компрессии аудио- и видеоданных.*

Распространённая задача для домашнего компьютера, впрочем, порой некоторые из представленных здесь программных пакетов используются и в профессиональной деятельности.

Данный класс программ, как правило, критичен к быстродействию и архитектуре процессора чуть в меньшей степени – подсистемы памяти.

– *Программы для работы с растровой и векторной графикой.*

Тест критичен к быстродействию процессора и подсистемы памяти, может задействовать более одного процессора, также очень важную роль играет объём ОЗУ.

Основной целью работы является составление наиболее подходящей методики тестирования компьютера для повышения эффективности выполнения задач.

Обобщенные виды методик:

– Методика для компьютеров, предназначенных для профессионального применения.

Позволяет оценить быстродействие рабочей станции с точки зрения пригодности к профессиональной работе. Длительность тестирования – до полутора рабочих дней.

– Методика для домашних и офисных компьютеров.

Позволяет вполне адекватно оценить производительность компьютера с точки зрения домашнего и/или офисного применения. Длительность тестов в зависимости от быстродействия компьютера – от 6 до 8 часов.

Каждая методика включает в себя классы программ, которые используются для решения поставленных задач.

Научный руководитель – А.А. Конев, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Тестирование: компьютеров, серверов, ноутбуков, мониторов, материнских плат, процессоров, жестких дисков, видеокарт, принтеров и др. http://www.compress.ru/. Журнал КомпьютерПресс. URL: http://www.compress.ru/tests.aspx

РАЗРАБОТКА ЭФФЕКТИВНОЙ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ*

Е.А. Левитская, аспирантка;
Б.Н. Епифанцев, науч. рук., д.т.н., зав. каф. ИБ
г. Омск, СиБАДИ, каф. ИБ, laska_kb@mail.ru

Надежность СКУД во многом зависит от типа предоставляемого считывателю кодоносителя. На данный момент большое распространение получили магнитные карты, радио-брелоки и бесконтактные проксимити-карты. Основной недостаток данных кодоносителей – происходит идентификация материального носителя, а не человека. В случае утери идентификатора или его фальсификации незарегистрированный пользователь может получить доступ.

При выборе типа кодоносителя необходимо учитывать специфику объекта защиты. Так, организация СКУД на крупном промышленном предприятии накладывает следующие требования на тип идентификатора:

1) высокая надежность идентификации;
2) быстрота идентификации;
3) возможность бесконтактного получения данных;
4) удобство использования;
5) обеспечение непрерывности работы системы;
6) устойчивость системы к воздействиям внешних факторов;
7) приемлемая сложность системы.

Наиболее перспективными и отвечающими всем предъявляемым требованиям являются биометрические считыватели. Это связано с тем, что биометрические данные в силу своей уникальности очень трудно фальсифицировать и их нельзя забыть дома или потерять.

Кроме несомненных преимуществ, все существующие методы биометрической идентификации имеют свои недостатки. Разные технологии обеспечивают отличные ошибки первого (вероятность ложного отказа) и второго рода (вероятность ложного допуска), предъявляют различные требования к условиям окружающей среды для проведения идентификации, сильно зависят от объема базы субъектов идентификации и т.д.

Решением данных проблем может стать разработка мультибиометрической СКУД, т.е. системы, основанной на параллельном применении нескольких биометрических идентификаторов. Использование нескольких идентификаторов позволит скомпенсировать недостатки одной технологии преимуществами другой.

* Работа выполнена в рамках государственного контракта № П215 от 22.07.2009 г.

Ниже представлены оценки основных биометрических технологий и основанных на них систем с точки зрения ранее изложенных требований.

Оценки основных биометрических технологий

Характеристика систем	Технология				
	Отпечатки пальцев	Геометрия руки	Изображение лица	Термообраз лица	Радужная оболочка глаза
Надежность идентификации	Средняя	Средняя	Средняя	Высокая	Высокая
Быстрота идентификации	Высокая	Высокая	Средняя	Средняя	Низкая
Бесконтактное получение данных	Нет	Нет	Да	Да	Да
Возможность обмана	Средняя	Высокая	Средняя	Низкая	Низкая
Устойчивость к внешним факторам	Средняя	Высокая	Средняя	Высокая	Высокая
Удобство использования	Средняя	Средняя	Высокая	Высокая	Высокая
Сложность системы	Средняя	Низкая	Средняя	Средняя	Высокая

Из таблицы видно, что в качестве биометрических идентификаторов наиболее перспективно использование образа ладони и изображения термограммы лица.

Использование технологии распознавания лица в ИК-диапазоне позволит решить некоторые проблемы стандартной идентификации по лицу – исключить влияние изменений освещения, влияние естественных возрастных изменений и использование маскировок.

При очевидных достоинствах подобной мультибиометрической СКУД возникает ряд проблем, связанных с синтезом информации от двух источников.

Для определения этапа слияния данных в мультибиометрической системе необходимо рассмотреть одномодальную систему и составляющие ее блоки.

Одномодальная биометрическая СКУД

Объединение информации может производиться на этапах принятия решения (*1*) и на уровне значений соответствия (*2*), на этапах выде-

ления признаков (*3*) и биометрических образцов (*4*). Слияние на уровнях (*1*) и (*2*) происходит после сравнения с эталоном, в то время как слияние на уровнях (*3*) и (*4*) происходит до получения результатов сравнения. Хотя интеграция данных возможна на всех перечисленных этапах, слияние на уровне множества признаков наиболее удобно.

При слиянии на уровне признаков объединение биометрической информации происходит после выделения признаков из образцов (образа ладони и изображения лица), но перед проведением сравнения. В мультибиометрической системе признаки не являются независимыми, поэтому хороший алгоритм слияния на уровне признаков позволит использовать зависимости в более полной мере, что позволит достичь лучшей производительности системы.

Проведенные эксперименты подтверждают увеличение надежности СКУД в случае слияния биометрических данных на уровне выделения признаков.

ЛИТЕРАТУРА

1. Лукашев И. Биометрия в СКД: вызовы времени и новые возможности // Системы безопасности. 2007. №6.

2. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. СПб.: Политехника, 2001. 240 с.

3. ISO/IEC JTC 1/SC 37 N 1506 «Multimodal and Other Multibiometric Fusion» 2006-05-28.

ЗАДАЧА О ПОКРЫТИИ ТЕЛА ПЛОСКИМИ УГЛАМИ

А.В. Лисин, студент магистратуры;
Р.Т. Файзуллин, науч. рук., д.т.н., профессор
ОмГТУ, г. Омск, каф. ССИБ, andrey.lisin@gmail.com

Задача о покрытии является одной из важных практических задач при создании систем безопасности. Наиболее часто она возникает при проектировании систем видеонаблюдения, при определении мест расположения датчиков движения различных типов и т.д. [1]. Задача может быть описана следующим образом: а) требуется покрыть замкнутую область минимальным числом заданных элементов покрытия; б) заданным количеством элементов покрыть наибольшее количество замкнутых областей. Применительно к построению систем безопасности логичнее рассматривать в качестве элементов покрытия треугольники ввиду того, что зона обзора видеокамер, датчиков движения и других технических средств на плоскости представляет собой треугольник.

Задача о покрытии является NP сложной. Для её решения используются различные эвристические и приближённые методы [2]. В статье описывается алгоритм рассечения выпуклой области углами с заданными растворами.

Можно дать следующую математическую формулировку поставленной задаче: пусть дана замкнутая область F и n треугольных элементов покрытия. Необходимо покрыть область F таким образом, чтобы площадь покрытой поверхности $S \to \max$.

Следует сделать несколько начальных предположений с целью построения эффективного алгоритма покрытия: а) пусть тело F является выпуклым; б) функция L, задающая кривую, ограничивающую тело F, – гладкая на всей области определения; в) если AB – хорда F, а h_i – высота треугольника, представляющего проекцию зоны обзора видеокамеры на плоскость, то $h_i \geq AB, \forall A, B \in L$ и треугольник можно заменить плоским углом. Тогда покрытие может быть произведено с помощью заданных растворов углов, вершины которых располагаются на кривой L [3].

Итак, пусть дано выпуклое тело, ограниченное кривой L, заданной гладкой функцией, и множество $\{\theta_n\}$ углов с различными растворами, при этом $0 < \theta < \pi/2$. Диаметром тела F назовём отрезок, соединяющий точки $A \in L$, $B \in L$ такие, что $AB = \max$. Выберем из данных углов угол с максимальным раствором и разобьём им тело таким образом, что диаметр AB будет его биссектрисой, а вершина будет находиться в точке A или B (рис. 1).

Для нахождения площади, «вырезаемой» углом при таком разбиении, расположим тело F так, что его диаметр будет лежать на оси абсцисс, а вершину угла совместим с началом координат (рис. 2).

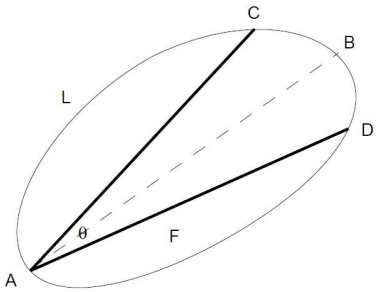


Рис. 1. Разбиение тела по диаметру

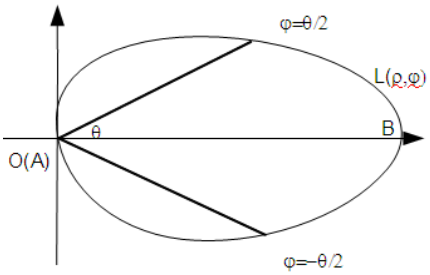


Рис. 2. Нахождение площади сегмента

Перейдём к полярным координатам. Тогда площадь вырезанного сегмента будет равна:

$$S = \iint\limits_F L(\rho,\varphi)\rho d\rho d\varphi = \int\limits_{-\theta/2}^{\theta/2} d\varphi \int\limits_0^{L(\rho,\varphi)} \rho d\rho .$$

Учитывая непрерывность функции L и тот факт, что $\theta = \theta/2 - (-\theta/2) < 2\pi$, можно записать следующее выражение для площади:

$$S = \frac{1}{2} \int\limits_{-\theta/2}^{\theta/2} L^2(\rho,\varphi) d\varphi .$$

Отсюда можно показать, что разбиение «по диаметру» будет наилучшим для произвольной гладкой функции $L(\rho,\varphi)$ [4].

После первого разбиения, очевидно, останутся непокрытыми два выпуклых тела, ограниченные однако кривыми, заданными *не*гладкими функциями (см. рис. 1). Диаметрами этих двух тел будут являться отрезки AC и AD. На втором шаге алгоритма требуется найти максимальное покрытие оставшихся тел. Для этого можно задействовать следующую рекурсивную процедуру:

1) ищутся углы, образованные отрезками и касательными, проходящими через точки A (слева и справа), C и D;

2) выбирается максимальный угол между диметрами и касательными – ψ_1;

3) из оставшихся элементов покрытия выбираем угол такой, что $\theta_1 - \psi_1 = r, r \to \min$;

4) производится сечение тела углом так, что одна из сторон угла совпадает с диаметром.

Отдельно следует рассмотреть случай, когда тело может быть полностью покрыто за два разбиения. Для проверки наличия такой возможности после построения диаметра AB найдём углы, образованные полукасательными в точках A и B. Например, если $L(A) = x_A$, то $\angle\mu = (y_-, y_+)$, где $y = L(x_A) - L'(x_A)(x - x_A)$ при устремлении x к A соответственно слева и справа. В случае, если имеются θ_i и θ_j, большие $\mu/2$, то полное покрытие за два шага, очевидно, возможно.

Предложенный в статье алгоритм легко реализуем программно и может быть использован при проектировании систем безопасности, использующих видеонаблюдение и различного рода датчики.

Допущения, сделанные при реализации алгоритма, при практическом его применении не снижают эффективности работы, так как форма охраняемых территорий, как правило, представляется выпуклыми телами.

ЛИТЕРАТУРА

1. Гедзберг Ю. М. Охранное телевидение. М.: Горячая линия – Телеком, 2005. 312 с.

2. Кузнецов В.Ю. Задача покрытия ортогональных многоугольников с запретными участками // Вестник УГАТУ. 2008. № 2. С. 177–182.

3. Половкин Е.С., Балашов М.В. Элементы выпуклого и сильно выпуклого анализа. М.: ФИЗМАТЛИТ, 2004. 416 с.

4. Ильин В. А., Садовничий В. А., Сендов Бл.Х. Математический анализ. М.: Изд-во Мос. Ун-та, 1985. 662 с.

5. Кормен Т., Лейзерсон Ч. Алгоритмы: построение и анализ. М.: Вильямс, 2005. 1296 с.

ВИРТУАЛЬНЫЕ СРЕДЫ OPENVZ

С.Д. Литвинов, студент 5-го курса;
Р.В. Мещеряков, науч. рук., к.т.н., доцент
г. Томск, ТУСУР, каф. КИБЭВС, litvinovsd@gmail.com

В данной статье кратко раскрывается вопрос виртуализации операционных систем на базе linux на примере системы виртуализации OpenVZ.

Сегодня виртуализация становится всё более популярной.

Во-первых, она допускает возможность иметь несколько разнотипных операционных систем на одной машине, что позволяет существенно экономить на издержках, связанных с покупкой аппаратного обеспечения, а также наиболее экономично расходовать вычислительные ресурсы, так как для большинства программ компьютеры обладают избыточной мощностью.

Во-вторых, изолирование потенциально опасных сервисов, работающих с правами суперпользователя, таких как Apache и Samba повышает безопасность сервера. Также виртуализация позволяет разным пользователям полноценно управлять своими службами с правами суперпользователя, в то же время находясь полностью изолированными.

Виртуализация позволяет управлять вычислительными ресурсами хостовой машины, что обеспечивает дополнительную надежность, так как проблемы в одной изолированной среде никак не повлияют на работу остальных сред.

В-третьих, упрощается обслуживание. Ведь гостевые окружения не привязаны к аппаратной части сервера, что упрощает их миграцию с одного компьютера на другой. Создать новое виртуальное окружение намного быстрее, чем устанавливать новую операционную систему. Сама собой устраняется проблема пересечения настроек сервисов. А

все настройки дисков и межсетевого экрана делаются на хостовой машине.

Сравнение популярных систем

Чтобы оценить системы виртуализаций, необходимо выделить следующие критерии оценки:

− необходима ли системе аппаратная поддержка;

− возможность работы с отличными от установленной операционными системами;

− какой метод установки необходим системе, нужна ли операционная система для её работы или нет;

− может ли система использовать аппаратную поддержку;

− необходима ли графическя консоль для работы;

− необходимы ли драйверы паравиртуализации для гостевых операционных систем.

OpenVZ запускается только из-под Linux, в виртуальных окружениях запускает только Linux и для работы на десктопе не предназначен. Но аппаратная поддержка виртуализации ему не требуется, потребление ресурсов и разница в быстродействии между базовой и виртуальной средой минимальны, установка и управление очень просты.

Поэтому OpenVZ являются идеальной системой для применения в следующих сферах:

− хостинги Linux-VPS;

− серверы, на которых запущено несколько сервисов с правами суперпользователя (разнесение по изолированным окружениям повысит безопасность) или со сложными настройками (разнесение упростит сопровождение).

В этих сферах OpenVZ превосходит linux-vserver, а также FreeBSD Jails и по возможностям становится сравнимой с Solaris Zones.

Архитектура

OpenVZ является патчем к исходным текстам ядра Linux. После установки в ядре добавляется массив дополнительных сущностей – виртуальных окружений, а для всех имеющихся объектов (процессы, сокеты и т.д.) введены дополнительные поля – номер виртуального окружения, к которому этот объект относится, и номер объекта внутри виртуального окружения.

Эти виртуальные окружения имеют свой каталог, в который и будет монтироваться корень файловой системы, а также они имеют свой набор квот на потребление системных ресурсов.

Более детальное описание файловой системы контейнера можно найти в книге А. Робаческого «Операционная система UNIX».

Модули, идущие к ядру (vzdev, vzmon и пр.), позволяют ввести работу ограничений, которые ориентируются на набор квот, эмуляцию

сети и мониторинг в виртуальном окружении, а также сохранение и восстановление текущего состояния запущенных контейнеров.

Также OpenVZ выгодно выделяется на фоне других систем универсальной виртуализации, таких как KVM и Xen, тем, что позволяет осуществлять прозрачный доступ из хостовой системы к ресурсам гостевых систем. Это может быть очень полезным, если вдруг обнаружится уязвимость в сервисе, запущенном в гостевых системах, тогда для того, чтобы его остановить, потребуется всего лишь выполнить команду «killall исполняемый файл».

В этой статье рассмотрена архитектура системы виртуализации OpenVZ и произведен небольшой сравнительный анализ с другими системами виртуализаций.

ЛИТЕРАТУРА

1. Робачевский А. Операционная система UNIX. СПб.: БХВ-Петербург, 2007.

ИНФОРМАЦИОННОЕ ОРУЖИЕ КАК СРЕДСТВО ВЕДЕНИЯ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

К.Т. Магомедова; Г.Н. Лихачева, науч. рук., к.э.н., ст. науч. сотр., проф.

г. Москва, МЭСИ, kallipsso@list.ru

Стремительные темпы развития компьютеризации и информатизации общества неизбежно ведут к созданию единого мирового информационного пространства. В России современная информационная инфраструктура в настоящее время только формируется, и входящие в нее информационные системы зачастую не имеют выхода в открытые сети связи.

Информационное оружие

Информационное пространство фактически стало театром военных действий, где каждая противоборствующая сторона стремится получить преимущество, а в случае необходимости разгромить противника. Размах противоборства в информационной сфере достиг таких масштабов, что потребовалось создание специальной концепции, получившей название «информационная война», или «информационное противоборство».

Информационная война – это комплекс мероприятий по достижению информационного превосходства путем воздействия на информацию, информационные процессы, информационные системы и компьютерные сети противника при одновременной защите своей информа-

ции, информационных процессов, информационных систем и компьютерных сетей. В рамках информационной войны проводятся мероприятия наступательного и оборонительного характера.

Информационная инфраструктура России ввиду ряда причин является уязвимой от воздействия наступательных средств ведения информационного противоборства, получивших название «информационное оружие». Информационное оружие согласно одному из существующих определений – это комплекс программных и технических средств, предназначенных для контроля информационных ресурсов объекта воздействия и вмешательства в работу его информационных систем. Информационное оружие возможно классифицировать по методам воздействия на информацию, информационные процессы и информационные системы противника. Это воздействие может быть физическим, информационным, программно-техническим или радиоэлектронным.

Физическое воздействие может быть осуществлено путем применения любых средств огневого поражения. Однако более корректным было бы отнести к информационному оружию физического воздействия средства, предназначенные исключительно для воздействия на элементы информационной системы: противорадиолокационные ракеты, специализированные аккумуляторные батареи генерации импульса высокого напряжения, средства генерации электромагнитного импульса, графитовые бомбы, биологические и химические средства воздействия на элементарную базу.

Информационные методы воздействия реализуются посредством всей совокупности средств массовой информации и глобальных информационных сетей типа Интернет, станциями голосовой дезинформации.

Так как основным элементом информационной инфраструктуры являются люди, мотивация деятельности которых базируется на их физиологических, социальных и информационных потребностях, то правильно рассчитанное применение так называемых информационно-психологических методов воздействия оказывает прямое влияние на уровень безопасности государства. Особенно это касается России, где пока отсутствует организованная система формирования и поддержания в обществе необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны. Научно-технический прогресс в области информационных технологий, развитие СМИ стерли национальные границы в информационном пространстве и создали беспрецедентные возможности для подавления противника с помощью нетрадиционных средств поражения, не вызывающих физических разрушений. Проходя через сознание каждого члена общества, длительное массированное информационно-психологическое воздействие разру-

шающего характера создает реальную угрозу существованию нации в результате трансформации ее исторически сложившейся культуры, основных мировоззренческих и идеологических установок.

Средствами реализации программно-технических методов являются компьютерные вирусы, логические бомбы и аппаратные закладки, а также специальные средства проникновения в информационные сети. Данные средства используются для сбора, изменения и разрушения информации, хранящейся в базах данных, а также для нарушения или замедления выполнения различных функций информационно-вычислительных систем.

Программно-технические средства можно классифицировать согласно выполняемым с их помощью задачам на средства сбора информации, средства искажения и уничтожения информации и средства воздействия на функционирование информационных систем.

Средства сбора информации позволяют производить несанкционированный доступ к компьютерным системам, определять коды доступа, ключи к шифрам или другую информацию о зашифрованных данных и по каналам обмена передавать полученные сведения заинтересованным организациям.

В настоящее время разработаны специальные программные продукты, так называемые «ноуботы» (Knowbot – Knowledge Robot), которые способны перемещаться в информационной сети от компьютера к компьютеру и при этом размножаться, создавая копии.

Задачи сбора информации решаются и с помощью программных продуктов «Демон» («Demon»), «Вынюхиватели» («Sniffers»), «Дверь-ловушка» («Trap Door»). Перспективным является также создание миниатюрных специализированных комплексов сбора, обработки и передачи информации, которые могут внедряться под видом обычных микросхем в состав самых различных радиоэлектронных устройств. Средства искажения и уничтожения информации включают программные продукты «Троянский конь» («Trojan Horse»), «Червь» («Worm»), а также многочисленные компьютерные вирусы, количество которых превышает 60 тысяч.

К средствам воздействия на функционирование информационных систем относятся «Логические бомбы», «Бомбы электронной почты» и т.д.

Радиоэлектронные методы воздействия предполагают использования средств радиоэлектронного подавления, радиоэлектронной разведки и некоторые другие. Основным предназначением такого оружия является контроль информационных ресурсов потенциального противника и скрытое или явное вмешательство в работу его систем управления и связи в целях дезорганизации, нарушения нормального функционирования или вывода их из строя как в мирное, так и в военное время

при действиях самостоятельно либо в сочетании с другими средствами воздействия на противника.

Однако остается вопрос причисления к оружию средств массовой информации, включая глобальную информационную сеть Интернет, а также программно-технические и радиоэлектронные средства сбора информации.

Что касается средств массовой информации, то использование их с целью оказания активного информационно-психологического воздействия может снизить или даже лишить личный состав противника на определенный период боеспособности, заставив его уклоняться различными путями от участия в боевых действиях. В этом случае СМИ выступают в качестве средства подавления, т.е. относятся к оружию.

Программно-технические и радиоэлектронные средства сбора информации не попадают под классическое определение оружия, так как они не участвуют в непосредственном поражении противника, а лишь обеспечивают условия для эффективного ведения вооруженного и, в частности, информационного противоборства. Но если принять за основу сформулированное выше определение информационного оружия, то средства сбора информации несомненно обеспечивают контроль над информационными ресурсами противника и могут быть причислены к этому виду оружия.

Таким образом, создание единого глобального информационного пространства, являющееся естественным результатом развития мировой научно-технической мысли и совершенствования компьютерных и информационных технологий, создает предпосылки к разработке и применению информационного оружия.

ЛИТЕРАТУРА

1. Концепция национальной безопасности Российской Федерациию М., 2000.

2. Доктрина информационной безопасности Российской Федерации. М., 2000.

3. Советская военная энциклопедия. М., 1978. Т. 6.

4. ИНФО-ТАСС. 1999. 31 марта.

5. Независимое военное обозрение. 1998. 17 июля.

6. Независимое военное обозрение. 1995. 18 ноября.

7. http://www.vrazvedka.ru/main/analytical/lekt-03.shtml (статья из электронного журнала «Разведчик»).

БЕЗОПАСНОСТЬ САЙТА, СОЗДАННОГО НА CMS DRUPAL

А.Е. Малахов, студент 4-го курса;
Р.В. Мещеряков, науч. рук., к.т.н., доцент
г. Томск, ТУСУР, каф. КИБЭВС, malahov.alexander@gmail.com

Drupal в настоящий момент – одна из самых популярных CMS (content management system, система управления содержанием). Drupal является универсальной CMS, т.е. на её основе можно создать от простого статичного сайта до портала с обширным набором функционала [1, 2]. Drupal написана на языке PHP, считающимся одним из самых простых для изучения. Ядро Drupal является структурно-ориентированным и позволяет легко подключать пользовательские модули, не уступая в этом объектно-ориентированным Joomla!/Mambo и RunCMS/XOOPS.

В нем так же, как и во всех популярных продуктах, существуют уязвимости. Большая часть уязвимостей в Drupal обнаруживается в подключенных модулях. Модули регулярно обновляются на официальном сайте группой разработчиков, но при этом для безопасности необходимо проверять код модуля перед установкой на работающий сайт. Не все модули могут корректно работать совместно. Соответственно перед установкой необходимо ознакомиться с устанавливаемым модулем, информацию можно получить из файла UPGRADE.txt, распространяемой с каждым модулем, и на официальном сайте или на сайте данного модуля.

Для большинства программных продуктов своевременное обновление программ может улучшить безопасность. Обновление сайта на Drupal может осуществляться следующими вариантами:

1. Получение почтой последних новостей [3].
2. Получение информации через ленту новостей RSS [4].
3. С помощью постоянной работы модуля cron, который обеспечивает проверку обновления ядра и установленных модулей. Данный модуль устанавливается вместе с ядром.

Ядро Drupal постоянно рассматривается диапазоном экспертов и является одним из главных центров группы безопасности Drupal. Это не безупречно, но по крайней мере Вы можете быть уверены, что любые слабости в ядре будут устранены быстро.

В Drupal применены свои средства работы с базами данных, что в свою очередь позволяет не зависеть от конкретного типа СУБД и защищает от SQL-инъекций. Описание необходимых функций для работы с базой данных на Drupal на официальном сайте [2] и на сайте [5].

Многие, кто создавал сайты, наверняка сталкивались с XSS-атакой, самой популярной, как и SQL-инъекции. Их принцип прост, а послед-

ствия могут быть разные – от некорректного вывода страницы до получения полного контроля над сайтом.

В Drupal может быть применен один из способов защиты от XSS-атак – фильтрация вывода на страницу.

Золотое правило работы с данными – хранить пользовательский ввод в базе именно в том виде, в котором он был отправлен. Поэтому всю фильтрацию следует производить на этапе вывода пользовательских данных на страницу. Более подробно об XSS-атаке и защите от нее описано на сайте, посвященном Drupal [6].

Еще одна из серьезных уязвимостей и защита от нее, подделка межсайтовых запросов (англ. Cross Site Request Forgery, CSRF). CSRF – это вид атаки на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от ее лица тайно отправляется запрос на другой сервер, осуществляющий некую вредоносную операцию (например, перевод денег на счет злоумышленника). Для осуществления данной атаки жертва должна быть зарегистрирована на том сервере, на который отправляется запрос, и этот запрос не должен требовать подтверждения со стороны пользователя.

В Drupal используется метод токенизации ссылок. Это означает, что к каждой ссылке активного действия прибавляется уникальный параметр, который проверяется при осуществлении самого действия. Токен генерирует на основе подаваемого значения сессии пользователя, а также приватного ключа сайта, что позволяет получить уникальные ссылки для действия по изменению данных. Подробнее об CSRF можно узнать на сайте, посвященном Drupal [7].

Также Drupal позволяет разграничить права доступа на сайт, к блокам, форумам, модулям и действия над ними.

Все приведенные выше уязвимости и защиты позволяют получить высокую степень защиты сайта, созданного на CMS Drupal.

ЛИТЕРАТУРА

1. Drupal Россия [Электронный ресурс]. Официальное русское сообщество CMS Drupal // URL:http://drupal.ru (дата обращения: 28.02.2010)

2. Drupal [Электронный ресурс]. Официальный сайт CMS Drupal // URL:http://drupal.org (дата обращения: 28.02.2010)

3. Drupal [Электронный ресурс]. Раздел безопасности Drupal // URL: http://drupal.org/security (дата обращения: 28.02.2010)

4. Drupal [Электронный ресурс]. Лента новостей раздела безопасности// URL: http://drupal.org/security/rss.xml (дата обращения: 28.02.2010)

5. DrupalDance [Электронный ресурс]. Безопасный код: Работа с базой данных // URL: http://drupaldance.com/lessons/secure-code-database-layer (дата обращения: 28.02.2010)

6. DrupalDance [Электронный ресурс]. Безопасный код: Работа с пользовательским вводом // URL: http://drupaldance.com/lessons/secure-code-user-input (дата обращения: 28.02.2010)

7. DrupalDance [Электронный ресурс]. Безопасный код: Подделка межсайтовых запросов (CSRF) // URL: http://drupaldance.com/lessons/secure-code-user-input (дата обращения: 28.02.2010)

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС НАБЛЮДЕНИЯ МОБИЛЬНЫХ ОБЪЕКТОВ ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

И.В. Маренков, студент 5-го курса;
А.Ю. Баранов, науч. рук., генеральный директор ЗАО «СИКЬЮБ»
г. Томск, ТУСУР, каф. КИБЭВС, Igor.Marenkov@siqube.u

В настоящее время рынок систем видеонаблюдения представлен большим количеством разнообразных систем, предназначенных для наблюдения зданий, неподвижных объектов, территорий и иных целей. Однако предложение систем видеонаблюдения, способных осуществлять наблюдение за мобильными объектами, ограничено.

Большинство представленных на рынке систем наблюдения за мобильными объектами строятся с применением цифровой беспроводной связи стандартов GPRS/EDGE/3G (цифровая связь, предоставляемая сетями сотовой связи) [1, 2]. Однако зона действия данного вида связи, как правило, ограничена окрестностями крупных населённых пунктов, что вносит ограничение в применение систем наблюдения за мобильными объектами, перемещающимися на большие расстояния.

Одной из перспективных разработок в сфере наблюдения за мобильными объектами является разрабатываемый в настоящее время ЗАО «Сикьюб» программно-аппаратный комплекс наблюдения мобильных объектов. Ключевой особенностью комплекса является возможность его применения для наблюдения за объектами, перемещающимися по всей территории России, а также возможность создавать и накапливать видеозаписи на протяжении всего пути его следования.

Потенциальными клиентами, в первую очередь, являются транспортные компании, осуществляющие транспортировку ценных грузов на большие расстояния различными видами транспорта (железнодорожный, автомобильный, речной, воздушный), и владельцы ценных грузов.

Комплекс проектируется как автоматизированная централизированная система, состоящая из территориально разделённых модулей. В

задачи, решаемые при помощи комплекса, входит ведение наблюдения за множеством мобильных объектов и круглосуточная видеозапись изображения наблюдаемых объектов.

Рассмотрим архитектуру комплекса на примере процесса наблюдения за грузами, транспортируемыми железнодорожным транспортом (рис.). В состав комплекса входят следующие модули:

Ip-камера – оборудование, предназначенное для видеосъёмки объекта наблюдения;

− TMET-контроллер – оборудование, устанавливаемое вместе с IP-камерами (предназначено для управления IP-камерами, создания и накопления видеозаписей, связи с другими модулями комплекса);

− промежуточный сервер – оборудование, являющееся звеном между центральным сервером и TMET-контроллером;

− главный сервер – оборудование, осуществляющие управление системой, накопление видеозаписей и предоставляющее интерфейс для управления / настройки комплекса.

Рис. 1. Модули системы и их взаимосвязь

TMET-контроллер и IP-видеокамеры располагаются непосредственно в железнодорожном вагоне. Связь TMET-контроллера и промежуточного сервера осуществляется по технологии беспроводной связи Wi-Fi в моменты нахождения состава с грузом на соответствующих железнодорожных станциях. Связь TMET-контроллера и главного сервера может быть осуществлена как непосредственно (посредством сетей сотовой связи), так и при посредничестве промежуточного сервера.

Для TMET-контроллера, промежуточного сервера и главного сервера разрабатывается общее программное обеспечение, называемое «сервер управления и распределения ресурсов» (СУРР). Для взаимо-

действия СУРР друг с другом предполагается использование специализированного закрытого протокола, находящегося в данный момент в разработке.

Потенциальный злоумышленник может быть заинтересован в нарушении работоспособности комплекса, в получении доступа к видеозаписям накапливаемым комплексом или в подделке видеозаписей, то есть заинтересован в осуществлении угроз доступности, конфиденциальности и целостности соответственно.

Для реализации указанных угроз злоумышленник может попытаться произвести атаку на программное обеспечение комплекса (для чего ему достаточно получить доступ к каналам связи, задействованным в информационном обмене между модулями комплекса). Атаки могут быть следующих типов:

− распределенная атака в отказе доступа (DOS);

− атака прослушивания (угроза доступности, конфиденциальности и целостности);

− атака при помощи подделки сообщений (угроза целостности и конфиденциальности);

− атака типа «повтор сообщения» (угроза конфиденциальности);

− атака на основе неправильно сформированных сообщений (угроза доступности);

− атака при помощи захвата сессии (угроза доступности, конфиденциальности и целостности), атака при помощи фальшивого сервера (угроза доступности, конфиденциальности и целостности).

Для минимизации потенциального вреда от описанных атак ЗАО «Сикьюб» необходимо предусмотреть защиту на уровне протокола обмена данными СУРР, а именно: шифрование канала данных, электронно-цифровая подпись сообщений, процедуры проверки сообщений на корректность, максимально сократить количество сообщений которые может принять СУРР от неаунтентифицированного клиента.

ЛИТЕРАТУРА

1. Кадейшвили А.А. Цифровое видеонаблюдение для мобильных объектов // Системы безопасности. 2009. № 9.

2. Мультимедийные услуги и приложения/Мобильное видеонаблюдение // сайт SkyLink. Режим доступа: http://www.skylink.ru/pages/article.aspx?id=4759&r=77

ОРГАНИЗАЦИЯ РАЗГРАНИЧЕНИЯ ДОСТУПА В БЕСПРОВОДНОЙ СЕТИ

А.А. Майнагашев, Е.А. Катаев, В.И. Хасанов, студенты 4-го курса;
А.С. Карауш, науч. рук., директор МИБС, к.т.н.
г. Томск, ТУСУР, каф. РЗИ, kataev.ea@gmail.com.

Распространение беспроводных сетей WiFi привело к увеличению числа устройств, поддерживающих данные сети, сделало эти устройства более доступными для потребителей. С другой стороны, такие сети являются удобным каналом для получения доступа к ресурсам библиотечной системы, а также к сети Интернет. Организация беспроводных сетей в крупных библиотеках обеспечит удобный доступ к информационным ресурсам как для сотрудников организации, так и для пользователей библиотечной системы.

Для достижения данной цели необходимо решить следующие задачи:

1) модель построения сети;
2) организация разграничения доступа;
3) изучение существующих систем разграничения доступа;
4) определение существующих возможностей решения;
5) выбор серверной ОС;
6) установка на сервера выбранных систем;
7) конфигурирование;
8) выработка собственного решения (если не будет найдено из существующих);
9) определение местоположения точек доступа;
10) установка операционной системы серверов;
11) конфигурирование точек доступа;
12) конфигурирование Radius-сервера;
13) установка на сервера биллинговой системы;
14) внедрение;
15) внедрение системы в существующую инфраструктуру;
16) организационное обеспечение функционирования;
17) тиражирование по филиалам.

Модель построения сети

Требования к создаваемой модели:

1) обеспечение доступа к сети Интернет на территории помещения библиотек, в том числе в читальном зале для свободного использования;
2) разграничение доступа читателей сотрудников;
3) ограничение на количество одновременных подключений: 255 (обусловлено количеством пользователей в подсети);

4) удобство подключения: подключение осуществляется в открытом режиме, но после требует идентификации;

5) шифрация передаваемого трафика;

6) регистрация производится по номеру читательского билета пользователя. Включена защита от «спам-ботов» в виде растрового изображения некоего числа;

7) возможность наложения ограничений на подключение определенного пользователя (после завершения его сеанса подключения). Осуществляется через базу данных выставлением определенного значения некой записи;

8) ведение логов и их хранение в течение 3 месяцев. Осуществляется резервирование и шифрование журналов регистрации событий;

9) политика безопасности и управления работоспособностью реализуется отделом НИТ.

Сравнение различных платформ для реализации брандмауэра выявило наиболее эффективным средством систему PfSense.

Анализ безопасности

Первым этапом процедуры тестирования системы на возможность вторжения и аудита безопасности был осмотр места развертывания беспроводной сети: выявление мест, в которых может быть получен сигнал, оценка четкости сигнала (отношение сигнал/шум) и измерение быстродействия канала в разных точках зоны покрытия. Необходимо также найти соседние беспроводные сети и другие возможные источники помех. Перед процедурой осмотра места развертывания ставится четыре задачи:

1) найти точки, в которые может физически внедриться взломщик;

2) выявить нелегальные точки доступа и соседние сети (создающие возможности для атаки по случаю или непреднамеренной атаки);

3) оценить проект сети и ее конфигурацию с точки зрения безопасности.

Так как беспроводная сеть подключена к локальной корпоративной вычислительной сети, следовательно, первый пункт анализа нужно учитывать.

Далее было произведено сканирование на наличие сторонних беспроводных сетей по всей площади, на которой располагается предприятие. Сканирование проводилось программой NetStumbler, установленной на мобильном ПК с беспроводным адаптером. В ходе сканирования не было обнаружено посторонних сетей, что значительно снизило уровень потенциальной угрозы.

Далее были проведены измерения уровня мощности сигнала в разных частях здания, которые показали, в каких местах возможно свободное подключение к беспроводной сети, а в каких оно невозможно. Измерения проводились на Wireless-адаптере с антенной чувствитель-

ностью 76 dBm, и исходящей максимальной мощностью сигнала от точки доступа 68 dBm.

В результате выполнения проекта получена рабочая модель построения беспроводной сети в библиотечной системе. Учтены требования, предъявленные к модели на первом этапе, в том числе разделение пользователей, шифрация трафика и т.д. Система прошла проверку в муниципальной библиотеке «Центральная», где показала свою работоспособность, надежность, удобство обслуживания и управления.

Система является адаптируемой и масштабируемой, что позволяет осуществить тиражирование в остальные библиотеки, имеющие широкополосный доступ к сети Интернет.

Полученное решение может быть использовать в организации беспроводных сетей различной конфигурации без существенных изменений.

ЛИТЕРАТУРА

1. Виртуальная энциклопедия «Linux по-русски» [Электронный ресурс] / Файрволл pfSense на страже вашей сети ; автор Александр Тарасов. Режим доступа: http://rus-linux.net/lib.php?name=MyLDP/sec/pfsense.html, свободный. Загл. с экрана. Яз. рус.

2. Журнал «Хакер» [Электронный ресурс] / На страже безопасности: pfSense – дистрибутив для создания роутера; автор Ульяна Смелая. Режим доступа: http://www.xakep.ru/post/46309/?print=true, свободный. Загл. с экрана. Яз. рус.

3. Для системного администратора [Электронный ресурс] / pfSense; автор неизвестен. Режим доступа: http://system-administrators.info/?p=2723, свободный. Загл. с экрана. Яз. рус.

4. BruteForcer [Электронный ресурс] / Установка pfSense и BackTrack 4 в Vmware Server 1.0.10.; автор Э_L_A_Y. Режим доступа: http://bruteforcer.ru/index.php/2009/11/15/ustanovka-pfsense-i-backtrack4-v-vmware-server-1-0-10/, свободный. – Загл. с экрана.– Яз. рус.

5. Tamo Oft [Электронный ресурс] / CommView for WiFi – мониторинг и анализ беспроводных сетей; автор неизвестен. Режим доступа: http://www.tamos.ru/htmlhelp/commwifi/nodes.htm, свободный. Загл. с экрана. Яз. рус.

ВНЕДРЕНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ И КОНТРОЛЯ ДОСТУПА В ДЕЯТЕЛЬНОСТЬ ПРЕДПРИЯТИЯ

А.В. Меркульев, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, cooer@ms.tusur.ru

Обеспечение безопасности является необходимым условием функционирования любой компании, поэтому важной задачей является выбор технических средств, способствующих повышению уровня безопасности.

Компания «Комплексные услуги безопасности» (ООО «КУБ») поставила задачу внедрения системы видеонаблюдения и контроля доступа в деятельность предприятия.

В качестве средств автоматизации, направленных на защиту информации, используются система видеонаблюдения и система разграничения доступа в помещения по биометрическим данным. Преимущество данного типа разграничения доступа заключается в том, что биометрические идентификаторы нельзя потерять, забыть, передать, похитить, что особенно важно для решения задач контроля доступа.

Система контроля доступа обеспечивает:

– безопасность сотрудников и посетителей;

– защиту материальных ценностей, оборудования, имущества и других активов;

– при интеграции с системами учета рабочего времени – рациональное управление персоналом.

Система учета рабочего времени обеспечивает:

– возможность отмечать приход на работу или уход с нее посредством касания пальцем сканера отпечатков;

– возможность вести контроль состояния трудовой дисциплины и своевременность явки сотрудников на рабочие места;

– возможность службе безопасности получать оперативную информацию о присутствии и отсутствии сотрудников.

Система видеонаблюдения обеспечивает:

– ведение круглосуточного наблюдения за офисными помещениями;

– ведение круглосуточного наблюдения за территорией перед входом в подъезд здания;

– возможность видеть крупным планом лица людей, входящих в подъезд здания.

Для того чтобы выбрать оптимальный вариант системы видеонаблюдения, был проведен анализ существующих систем на рынке, определены основные характеристики систем видеонаблюдения и требования к помещениям.

Под системой видеонаблюдения понимается совокупность камеры и устройства видеорегистрации, соединенных между собой.

К основным характеристикам видеокамер относятся:

– формат матрицы;

– разрешение камеры наблюдения;

– чувствительность камеры наблюдения;

– фокусное расстояние, мм (угол);

– размер, мм;

– функции/особенности;

– цена.

К основным характеристикам устройств видеорегистрации относятся:

– разрешение записи;
– скорость записи;
– варианты записи;
– запись аудио;
– число каналов видео;
– цена.

В рамках поставленных требований к помещениям были выбраны те системы, которые удовлетворяют условиям этих требований, были проработаны конструкции системы защиты информации и внедрены в деятельность предприятия.

Используя существующую политику безопасности и план-схему помещений, были созданы помещения в системе контроля доступа, установлены правила прохода персонала в них, определены права и график доступа.

Текущая структура предприятия была учтена при проектировании системы контроля доступа, тем самым была сформирована база данных сотрудников и их отпечатков пальцев для идентификации.

Таким образом, внедренная в деятельность предприятия система видеонаблюдения и контроля доступа позволяет предотвратить несанкционированный доступ в помещения злоумышленникам и, если же доступ был получен, определить их личность, используя записи видеокамер.

Научный руководитель – А.А. Конев, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации: Учеб. пособие. Томск: Изд-во ТУСУРа, 2006. 388 с.

АВТОРИЗАЦИЯ С ПОМОЩЬЮ КЛИЕНТСКИХ SSL-СЕРТИФИКАТОВ

Н.С. Михайлов, студент 5-го курса;
Р.В. Мещеряков, науч. рук., к.т.н., доцент
г. Томск, ТУСУР, каф. КИБЭВС, dem@ms.tusur.ru

При разработке автоматизированной системы управления IP-телефонией возникла необходимость авторизации пользователей, не находящихся на рабочем месте. Проводить свои линии связи для удалённых пользователей крайне неудобно и требует значительных мате-

риальных затрат. Кроме того, расположение пользователей может меняться. Таким образом, было решено использовать открытые каналы связи. Вследствие этого возникает проблема безопасности информации в этих каналах.

Безопасность данных в открытых информационных сетях, таких как Интернет, всегда будет источником серьезного беспокойства для разработчиков и клиентов. Поэтому для любого используемого продукта крайне важно создать безопасную среду исполнения.

Протокол SSL [1] (Secure Socket Layers – протокол защищенных сокетов), совместно разработанный Netscape Communications и RSA Data Security, позволяет эффективно обеспечить такую безопасность. Протокол SSL обеспечивает безопасность, аутентификацию на базе сертификатов и согласование безопасности по установленному сетевому соединению, поэтому множество компаний и продуктов приняли SSL в качестве коммуникационного протокола.

Протокол SSL обеспечивает целостность и конфиденциальность обмена данными между двумя общающимися приложениями, использующими TCP/IP. Данные, перемещающиеся между клиентом и сервером, шифруются симметричным алгоритмом.

Для цифровых подписей и обмена ключами шифрования используется алгоритм с открытым ключом. В шифровании с открытым ключом задействованы два ключа, каждый из которых может использоваться для шифрования сообщений. Если один ключ используется для шифрования сообщения, для его расшифровки необходимо использовать другой. Это позволяет получать защищенные сообщения, просто публикуя один (открытый) ключ и храня другой (секретный) ключ в тайне.

Это подводит к обсуждению цифровых сертификатов, играющих важную роль в SSL [2]. Цифровые сертификаты в основном служат двум целям:

– установить личность владельца;

– сделать доступным открытый ключ владельца.

Цифровой сертификат выпускается проверенной полномочной организацией – удостоверяющим центром и выдается только на ограниченное время. После истечения срока действия сертификата его необходимо заменить. Протокол SSL использует цифровые сертификаты для обмена ключами, аутентификации серверов и, при необходимости, аутентификации клиентов.

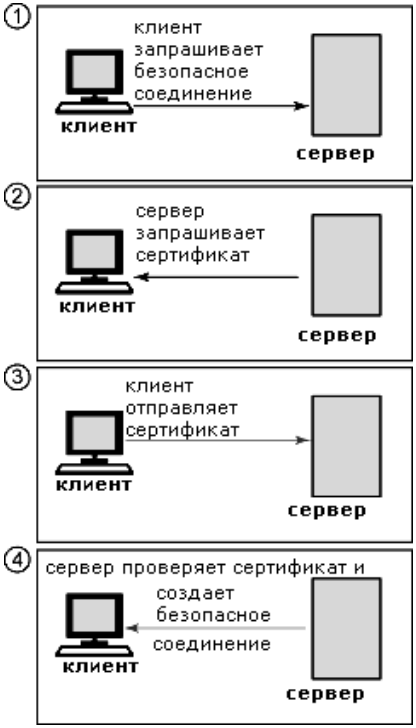
После того как сертификат был получен, необходимо установить его подлинность (аутентифицировать). В протоколе SSL есть два типа аутентификации:

– аутентификация на стороне клиента;

– аутентификация на стороне сервера.

SSL-аутентификация сервера позволяет клиенту проверить подлинность сервера. Клиентское ПО, поддерживающее SSL, может с помощью стандартных приемов криптографии с открытым ключом проверить, что сертификат сервера и открытый ключ действительны и были выданы источником, находящимся в списке доверенных источников сертификатов этого клиента. Это подтверждение может быть важным, если пользователь, например, отправляет номер кредитной карты по сети и хочет проверить подлинность сервера-получателя.

SSL-аутентификация клиента позволяет серверу проверить личность пользователя. Используя те же приемы, что и в случае с аутентификацией сервера, серверное ПО с поддержкой SSL может проверить, что сертификат клиента и открытый ключ действительны и были выданы источником сертификатов, имеющимся в списке доверенных источников сервера. Это подтверждение может быть важным, если, например, сервер – это банк, отправляющий конфиденциальную финансовую информацию заказчику, и он хочет проверить личность получателя. На рисунке приведена диаграмма, иллюстрирующая этот процесс.



Процесс аутентификации между клиентом и сервером

Было решено отказаться от привычной парольной авторизации пользователей и применить описанную выше технологию для защищённого управления IP-телефонии. Пользователи авторизуются на сервере с помощью своей ключевой пары, выданной Удостоверяющим центром Сибири.

ЛИТЕРАТУРА

1. Introduction to SSL [Электронный ресурс]. Режим доступа: https://developer.mozilla.org/en/Introduction_to_SSL

2. Всё об SSL технологиях [Электронный ресурс]. Режим доступа: http://www.inssl.com/

ОТЛИЧИЕ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ ЗАРУБЕЖНЫХ АНАЛОГОВ

В.Г. Миронова, студентка 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, mvg@security.tomsk.ru

В 1981 г. Совет Европы принял конвенцию «О защите личности в связи с автоматической обработкой персональных данных». 25 ноября 2005 г. Государственная дума ратифицировала данную конвенцию (ФЗ от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных (ПДн)»), возложив на Российскую Федерацию обязательства по приведению в соответствие с нормами европейского законодательства деятельность в области защиты прав субъектов ПДн [1]. Первым шагом в реализации взятых обязательств стало принятие Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных». Закон вступил в силу в январе 2007 г.

Целью российского законодательства в области защиты персональных данных «является обеспечение защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну» [2]. Законодательством регулируются отношения, связанные с обработкой ПДн, осуществляемой государственными органами власти, органами местного самоуправления, юридическими и физическими лицами.

Стоит заметить, что к моменту подписания Федерального закона № 152 «О персональных данных» почти вся Европа, многие страны Азии, Америки и даже Африки уже имели аналогичные законы.

Первые нормативные акты по защите ПДн в Финляндии появились в 1987 г., закон же, который носит название «Act on the Amedment of the Personal Data Act», был принят в 2000 г.

В Великобритании в 1998 г. был принят Закон о защите персональных данных – Data Protection Act 1998. Его техническая реализация – проект стандарта «Specification for the management of personal information in compliance with the Data Protection Act 1998» (BS 10012) должен был получить статус официального документа в июне 2009 г.. Параллельно с англичанами свою версию стандарта по безопасности ПДн выпустили в США. Проект документа по защите персональных данных для американских государственных структур – «Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)» (SP 800-122) регламентирует выполнение законов «The Privacy Act of 1974» и «Privacy Protection Act of 1980». Канада выпустила «Privacy Code» – набор документов для реализации законодательства по защите сведений о частных лицах (The Privacy Act и PIPEDA) [3].

США, Великобритания и Канада, как и Россия, разработали технические регламенты, которые транслируют положения законодательства верхнего уровня в конкретные советы и рекомендации по защите персональных данных.

Канадский, английский и американский стандарты, в отличие от документов российских регуляторов, дают более общие рекомендации по обеспечению безопасности ПДн и не предписывают, как конкретно должны защищаться персональные данные. Более того, тот же американский стандарт рекомендует по возможности обезличивать персональные данные, чтобы уйти от различных защитных мер, снижающих удобство пользования информацией.

Российские регуляторы разработали технические регламенты и требования, которые транслируют положения законодательства верхнего уровня в конкретные советы и рекомендации, которые представлены в виде четырех документов: «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Научный руководитель – А.А. Шелупанов, д.т.н., профессор, зав. каф. КИБЭВС, проректор по научной работе ТУСУРа.

ЛИТЕРАТУРА

1. О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных (ПДн): Федеральный закон №160-ФЗ. Утвержден Президентом Российской Федерации от 19.12.2005.

2. О персональных данных: Федеральный закон №152-ФЗ. Утвержден президентом Российской Федерации 27 июля 2006.

3. Слепов О. Защита персональных данных // Инфосистемы Джет. 2009. № 5. С. 34.

СПЕЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В.Г. Миронова, студентка 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, mvg@security.tomsk.ru

27 июля 2006 г. Президент РФ В.В. Путин подписал закон № 152 – ФЗ «О персональных данных». В сферу действия этого нормативного акта попадают все юридические и физические лица, на попечении которых находятся приватные сведения других граждан.

Согласно ФЗ № 152, информационные системы персональных данных (ПДн), созданные до 1 января 2010 г., должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2011 г. (часть третья в ред. Федерального «закона» от 27.12.2009 № 363-ФЗ).

Правительством Российской Федерации и государственными регулирующими органами определен порядок классификации информационных систем персональных данных, сформированы конкретные технические требования к соответствующим классам систем, установлен порядок уведомления уполномоченного органа об обработке персональных данных, уточняется система мер ответственности за неисполнение норм Федерального закона «О персональных данных».

В «Порядке о проведении классификации информационных систем персональных данных» выделен пункт, касающийся отнесению самой информационной системы к типовой либо специальной.

«По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий)» [1].

Классификацию оператор персональных данных должен осуществить самостоятельно, а модель угроз безопасности ПДн создать, не исходя из своего опыта и здравого смысла, а на основании базовой модели, утвержденной ФСТЭК, и по методике того же ведомства.

От того, типовая система или специальная, какие требования предъявляются к ней, зависит, какие конкретно средства защиты придется использовать для обеспечения безопасности.

Таким образом, для типовой информационной системы ПДн необходимо рассматривать угрозы информационной безопасности, которые нарушают только конфиденциальность ПДн, и перечень этих угроз приведен в методических рекомендациях ФСТЭК, а именно «Базовая модель угроз обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных».

Для специальных информационных систем недостаточно рассматривать угрозы безопасности ПДн только по отношению к конфиденциальности ПДн. Ведь, как известно, «безопасность информации – это состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, целостность, доступность, подлинность и аутентичность» [2]. Поэтому рассмотрение более широкого перечня угроз, при построении модели угроз для специальных информационных систем, просто необходимо. Таким образом, основываясь на методике Федеральной службы по техническому и экспортному контролю (ФСТЭК) для типовых информационных систем ПДн, можно расширить перечень угроз, которым будут подвергаться информационные системы ПДн, и построить модель угроз обеспечения безопасности персональных данных для специальных информационных систем ПДн. На рисунке показана возможная схема построения модели угроз информационной безопасности персональных данных.

Но для начала стоит составить полный перечень вопросов, касающихся информационной системы ПДн, технологии обработки ПДн, программного обеспечения, которое используется при обработке, и технических средств, как основных, так и вспомогательных. Стоит также в перечень включить вопросы, касающиеся организационного обеспечения информационной безопасности.

После составления перечня вопросов необходимо предоставить данный опросник пользователям информационной системы с целью получения ответов, которые будут являться актуальными и отражать реальную ситуацию, происходящую в информационной системе.

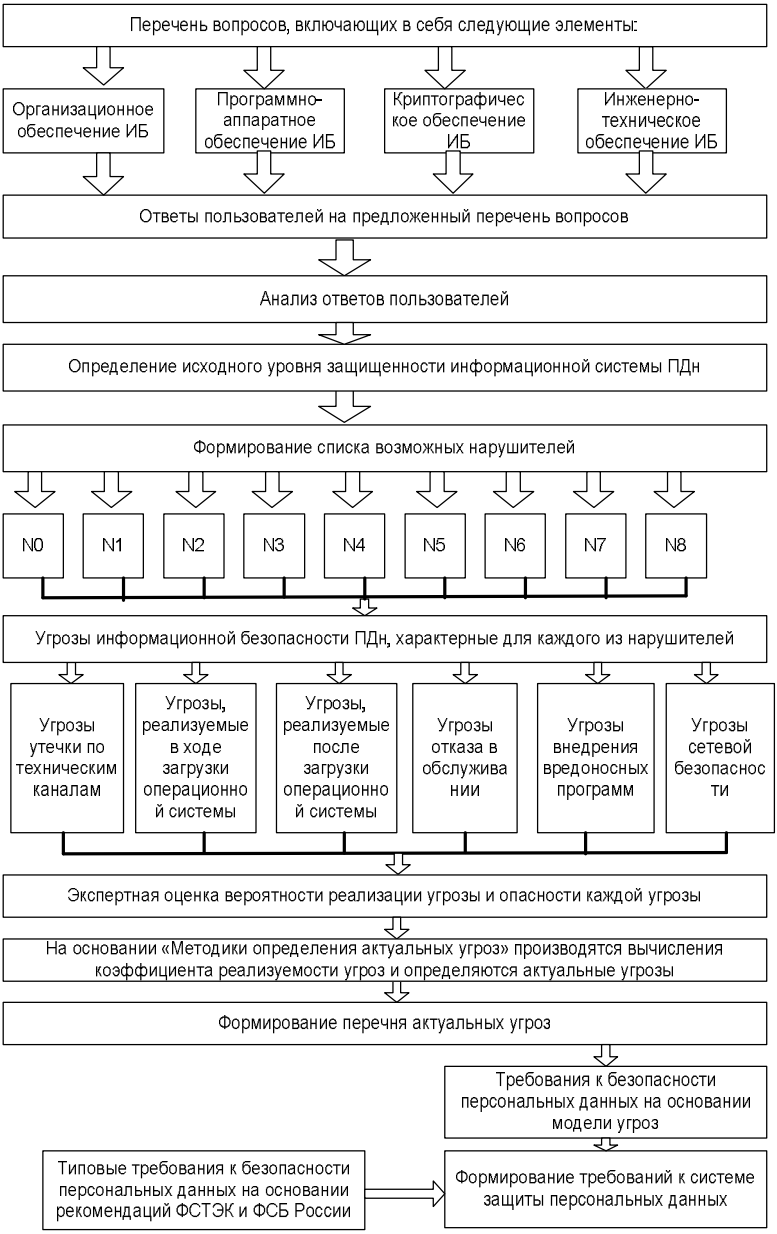


Схема построения модели угроз информационной безопасности персональных данных

Также необходимо составить полный перечень угроз безопасности ПДн и сопоставить их с ранее выделенным перечнем вопросов.

После того как пользователь ответит на предоставленные ему вопросы, будут выделены угрозы, которым может быть подвергнута его информационная система, после этого специалисту по информационной безопасности останется экспертным путем определить вероятность возникновения той или иной угрозы.

На основании методики, предложенной ФСТЭК, «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» производятся вычисления коэффициентов и выясняется возможность реализации угрозы.

Следующим шагом являются определение опасности реализации той или иной угрозы и определение актуальность угроз, в результате чего получаем модель угроз для специальных информационных систем персональных данных.

Научный руководитель – А.А. Шелупанов, д.т.н., профессор, зав. каф. КИБЭВС, проректор по научной работе ТУСУРа.

ЛИТЕРАТУРА

1. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

2. Свободная энциклопедии «Википедия» [Электронный ресурс]. Режим доступа: www.wikipedia.tomsk.ru

3. О персональных данных: Федеральный закон №152-ФЗ. Утвержден Президентом Российской Федерации 27 июля 2006 г.

МЕТОДЫ МАТЕМАТИЧЕСКОГО ПРОГРАММИРОВАНИЯ В ПОИСКЕ ОПТИМАЛЬНЫХ СЗИ

Е.А. Мошников, аспирант; А.П. Зайцев, науч. рук., к.т.н. профессор

г. Томск, ТУСУР, каф. КИБЭВС, mea@security.tomsk.ru

При решении конкретной задачи оптимизации необходимо прежде всего выбрать математический метод, который приводил бы к конечным результатам с наименьшими затратами на вычисления или же давал возможность получить наибольший объем информации об искомом решении. Выбор того или иного метода в значительной степени определяется постановкой задачи оптимизации, а также используемой математической моделью объекта оптимизации [1].

Рассмотрим математическое программирование для решения задач оптимизации, в частности динамическое программирование.

Некоторые методы математического программирования:

– динамическое программирование;

– линейное программирование;

– дробно-линейное программирование;

– нелинейное программирование.

Математическое программирование – математическая дисциплина, изучающая теорию и методы решения задач о нахождении экстремумов функций на множествах конечномерного векторного пространства, определяемых линейными и нелинейными ограничениями (равенствами и неравенствами) [2]. Термин «программирование» в данном случае, понимается как «планирование». Данный термин введен Джорджем Данцигом ещё до того, как компьютеры были использованы для решения задач оптимизации.

Рассмотрим более подробно динамическое программирование. Словосочетание «динамическое программирование» впервые было использовано в 1940-х годах Р. Беллманом для описания процесса нахождения решения задачи, где ответ на одну задачу может быть получен только после решения задачи, «предшествующей» ей. В 1953 г. он уточнил это определение до современного. Первоначально эта область была основана как системный анализ и инжиниринг, которая была признана IEEE. Вклад Беллмана в динамическое программирование был увековечен в названии уравнения Беллмана, центрального результата теории динамического программирования, который переформулирует оптимизационную задачу в рекурсивной форме [2].

Основную идею динамического программирования можно охарактеризовать так. Допустим, задачу можно разбить на подзадачи, которые можно разбить так же. Разбиение происходит до тех пор, пока решение не будет тривиальным либо будет требовать значительно меньше ресурсов на вычисления. К примеру, если нам нужно найти $n!$, то тривиальной задачей будет $1! = 1$ или $0! = 1$. Затем все полученные результаты используются для решения основной задачи.

Динамическое программирование обычно придерживается двух подходов к решению задач:

– нисходящее динамическое программирование;

– восходящее динамическое программирование.

Нисходящее динамическое программирование: задача разбивается на подзадачи меньшего размера, они решаются и затем комбинируются для решения исходной задачи. Используется запоминание для решений часто встречающихся подзадач.

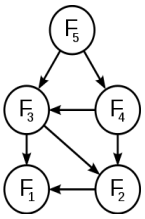
Восходящее динамическое программирование: все подзадачи, которые впоследствии понадобятся для решения исходной задачи, просчитываются заранее и затем используются для построения решения исходной задачи.

Рассмотрим решение конкретной задачи вычисления последовательности Фибоначчи на примере динамического программирования.

Последовательность Фибоначчи:

$$F_1 = 1,\ F_2 = 1,\ \ F_{n+1} = F_n + F_{n-1},\ \ n \in N.$$

$F_3 = F_2 + F_1$ и $F_4 = F_3 + F_2$ – даже в таком тривиальном случае вычисление всего двух чисел Фибоначчи требует подсчета F_2 дважды. Если продолжать дальше и посчитать F_5, то вычисление F_2 потребуется ещё два раза, так как для вычисления F_5 будут нужны опять F_3 и F_4. Граф подзадач (ребро означает, что одна задача зависит от решения другой) для чисел Фибоначчи представлен на рисунке.



Граф подзадач

Получается следующее: простой рекурсивный подход не будет расходовать ресурсы, необходимые на математические операции для решения задач, которые уже решались, но потребуются дополнительные ресурсы для хранения всех полученных результатов. Из этого вытекает основной недостаток динамического программирования – требовательность к ресурсам хранения промежуточных результатов.

Динамическое программирование выбрано для решения задачи поиска оптимальных СЗИ по следующим причинам:

– комплекс СЗИ состоит из множества подсистем;

– многие подсистемы, в свою очередь, являются составными;

– найденные оптимальные решения для одного объекта можно использовать как оптимальные при защите информации и на других объектах;

– учитывая объемы памяти для хранения информации в современных ЭВМ, основным недостатком динамического программирования можно пренебречь.

ЛИТЕРАТУРА

1. Трифонов А.Г. Постановка задачи оптимизации и численные методы ее решения. http://matlab.exponenta.ru/optimiz/book_2/1.php –

2. Методы математического программирования в задачах оптимизации. http://ru.wikipedia.org/wiki/оптимизация_(математика).

МЕТОДИКА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Д.В. Нечаев, студент 5-го курса
г. Томск, ТУСУР, каф. КИБЭВС, ndv87@sibmail.com

В связи с выходом ФЗ № 152 «О персональных данных» встает вопрос о том, как обеспечить безопасность персональных данных в организациях, их обрабатывающих. ФСТЭК разработала и опубликовала ряд методических документов рекомендательного характера:

1) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 г.;

2) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 г.;

3) Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 15 февраля 2008 г. (пометка «для служебного пользования» снята Решением ФСТЭК России от 11 ноября 2009 г.);

4) Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 г.

Рассмотрим порядок действий по защите персональных данных, согласно данным документам:

1. Обследование информационной системы, обрабатывающей персональные данные, и оценка ее соответствия требованиям нормативных документов по защите персональных данных.

1.1. Анализ внутренних нормативных документов, регламентирующих порядок обработки и защиты персональных данных.

1.2. Определение используемых средств защиты персональных данных и оценка их соответствия требованиям нормативных документов РФ.

1.3. Определение перечня персональных данных, подлежащих защите.

1.4. Определение перечня элементов информационной системы персональных данных, обрабатывающих персональные данные.

1.5. Определение степени участия персонала в обработке персональных данных и режима доступа к ним.

По результатам этапа формируется отчет, в котором содержатся описание текущего состояния защиты персональных данных, а также рекомендации по устранению выявленных недостатков и нарушений.

2. Классификация информационной системы, обрабатывающей персональные данные.

Осуществляется в соответствии с порядком проведения классификации, описанным в приказе ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20.

3. Разработка модели угроз безопасности персональных данных и модели нарушителя.

Происходит на основе перечня угроз безопасности персональных данных при их обработке в ИСПДн, который содержится в Базовой модели угроз безопасности ПДн при их обработке в ИСПДн. При необходимости применения средств криптографических защиты разрабатывается модель нарушителя в соответствии с нормативными документами ФСБ России.

4. Разработка технического задания на создание системы защиты персональных данных.

4.1. Обоснование разработки СЗПДн.

4.2. Исходные данные создаваемой ИСПДн в техническом, программном, информационном и организационном аспектах.

4.3. Класс ИСПДн.

4.4. Ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн.

4.5. Мероприятия и требования к СЗПДн, которые определяются в соответствии с классом и типом ИСПДн на основе методических документов ФСТЭК России.

4.6. Перечень предполагаемых к использованию сертифицированных средств защиты информации.

4.7. Состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

5. Макетирование и стендовые испытания средств защиты информации.

6. Разработка технического проекта на создание системы защиты персональных данных.

Содержит детальное описание конкретных программно-технических решений для создания СЗПДн, осуществляется на основе технического задания и результатов стендовых испытаний средств защиты информации.

7. Поставка и внедрение технических средств защиты информации.

Осуществляется согласно результатам предыдущих этапов работ, в частности требований и решений, определенных Техническим проектом на СЗПДн. После завершения поставки производится установка и настройка СЗИ.

8. Разработка проектов организационно-распорядительной документации.

8.1. Требования к комплексу мер и средств обеспечения безопасности ПДн.

8.2. Требования к персоналу ИСПДн, степень ответственности, статус и должностные обязанности сотрудников.

Осуществляется в целях регламентирования порядка обеспечения безопасности ПДн.

9. Аттестация информационной системы, обрабатывающей персональные данные.

В этом случае на данном этапе проводится разработка проектов документов, необходимых для выполнения аттестационных испытаний, включающих технический паспорт, матрицу доступа к ресурсам и другие документы.

ЛИТЕРАТУРА

1. Официальный сайт Федеральной службы по техническому и экспортному контролю [Электронный ресурс]. Режим доступа: http://www.fstec.ru/_razd/_ispo.htm

ХЕШИРОВАНИЕ НА КЛЕТОЧНЫХ АВТОМАТАХ*

С.В. Моисеенко, Е.О. Оплачко, студенты 3-го курса;
С.К. Росошек, науч. рук., к.ф.-м.н, доцент
г. Томск, ТУСУР, каф. КИБЭВС, mosergius@sibmail.com, ekatopla@sibmail.com

Клеточный автомат является динамической системой с дискретными состояниями. Поведение системы полностью определяется локальными зависимостями. Назовём дискретным пространством пространство над дискретным множеством элементов. Экземпляр пространства этого класса будем называть решёткой клеточного автомата, а каждый его элемент – клеткой. Каждая клетка характеризуется определённым значением из некого множества. О клетке говорят, что она содержит или имеет соответствующее значение либо находится или пребывает в состоянии, кодируемом данным значением a_{in}. Оно может быть любым объектом, в зависимости от поставленной задачи. Совокупность состояний всех клеток решётки называется состоянием решётки. Состояние решётки меняется в соответствии с некоторым законом, который называется правилами клеточного автомата. Каждое изменение состояния решётки называется итерацией. Время дискретно, и

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

каждая итерация соответствует некому моменту времени. Правила определяют, какое значение должно содержаться в клетке в следующий момент времени, в зависимости от значений в некоторых других клетках в текущий момент, а также, возможно, от значения, содержащегося в ней самой в текущий момент. Множество клеток, влияющих на значение данной, за исключением её самой, называется окрестностью клетки.

Выделим основные свойства классической модели клеточных автоматов:

– Локальность правил. На новое состояние клетки могут влиять только элементы её окрестности и, возможно, она сама.

– Однородность системы. Ни одна область решётки не может быть отлична от другой по каким-либо особенностям, правилам и т.п.

– Множество возможных состояний клетки конечно.

– Значения во всех клетках меняются единовременно в конце итерации, а не по мере вычисления [1].

Область применения клеточных автоматов почти безгранична: от простейших «крестиков-ноликов» до искусственного интеллекта. Клеточные автоматы применимы в математике, физике, биологии, социологии, экономике и т.д.

Главная особенность клеточного автомата в том, что в автомате и объекты, которые могут быть интерпретированы как пассивные данные, и объекты, которые могут быть интерпретированы как вычислительные устройства, собираются на одном типе структурных элементов и подчиняются одним и тем же законам. Незначительные изменения правила клеточного автомата или его начального состояния приводят к различным конечным состояниям. Даже зная правило и конечное состояние клеточного автомата, представляется предельно сложным вычислить его начальное состояние.

Особенности клеточных автоматов дают возможность для использования клеточного автомата в криптографических преобразованиях, а точнее для преобразования входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования называются хеш-функциями, или хешированием. Хеширование применяется для сравнения данных: если у двух массивов хеш-функции разные, массивы гарантированно различаются; если одинаковые – массивы, скорее всего, одинаковы.

Криптографической хеш-функцией называется всякая хеш-функция, являющаяся криптостойкой, то есть удовлетворяющая ряду требований, специфичных для криптографических приложений:

– Значение хэш-функции должно вычисляться достаточно быстро.

– Необратимость: для заданного значения хеш-функции m должно быть практически невозможно найти блок данных X, для которого $H(X) = m$.

– Стойкость к коллизиям первого рода: для заданного сообщения M должно быть практически невозможно подобрать другое сообщение N, для которого $H(N) = H(M)$.

– Стойкость к коллизиям второго рода: должно быть практически невозможно подобрать пару сообщений (M, M'), имеющих одинаковый хеш.

Коллизией хеш-функции H называется два различных входных блока данных x и y таких, что H(x) = H(y) [2].

Для криптографических хеш-функций также важно, чтобы при малейшем изменении аргумента значение функции сильно изменялось, то есть наблюдался лавинный эффект. В частности, значение хеша не должно давать утечки информации даже об отдельных битах аргумента. Лавинный эффект проявляется в зависимости всех выходных битов от каждого входного бита. Если криптографический алгоритм не обладает лавинным эффектом в достаточной степени, криптоаналитик может сделать предположение о входной информации, основываясь на выходной информации. Таким образом, достижение лавинного эффекта является важной целью при разработке криптографического алгоритма.

Для того чтобы проверить наличие хорошего лавинного эффекта в конкретном алгоритме, используется несколько критериев:

– Криптографический алгоритм удовлетворяет лавинному критерию, если при изменении одного бита входной последовательности изменяется в среднем половина выходных битов.

– Криптографический алгоритм удовлетворяет строгому лавинному критерию, если при изменении одного бита входной последовательности каждый бит выходной последовательности изменяется с вероятностью одна вторая.

– Криптографический алгоритм удовлетворяет критерию независимости битов, если при изменении любого входного бита любые два выходных бита изменяются независимо [3].

На основе полученных в ходе исследования применимости клеточных автоматов в области обеспечения целостности данных была реализована хеш-функция на основе одномерного клеточного автомата. Клеточный автомат изменяет свое состояние по правилу, которое можно описать, как клетка живет, когда оба ее соседа или живы, или мертвы. Это правило во многом схоже с традиционным правилом XOR. Полученная хеш-функция предназначена для получения хеш-кода файлов любого формата.

ЛИТЕРАТУРА

1. Тоффоли Т., Марголус Н. Машины клеточных автоматов. М.: Мир, 1991.

2. Практическая криптография: Пер. с англ. / Н. Фергюсон, Б. Шнайер. М.: Вильямс; Диалектика, 2005. 421 с.

3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2005. 229 с.

КОНТРОЛЬ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ОТ РПЭМИН

Е.М. Пенчиков, студент 5-го курса;
А.П. Зайцев, науч. рук., к.т.н. профессор
г. Томск, ТУСУР, каф. КИБЭВС, penchik_off@mail.ru

Одним из возможных каналов утечки информации является излучение элементов компьютера. Принимая и декодируя эти излучения, можно получить сведения обо всей информации, обрабатываемой в компьютере. Этот канал утечки информации называется ПЭМИН (побочные электромагнитные излучения и наводки).

Контроль защищенности осуществляется с целью предупреждения возможности измерения аппаратурой разведки побочных электромагнитных излучений и наводок (РПЭМИН) информации, циркулирующей на защищаемом от РПЭМИН объекте, и оценки эффективности мероприятий по противодействию РПЭМИН.

Различается два вида контроля защищенности объектов от РПЭМИН:

– аттестационный контроль,

– эксплуатационный контроль.

Аттестационный контроль проводится при вводе объекта в эксплуатацию и после его реконструкции или модернизации и состоит из организационной и инструментальной частей. В организационной части аттестационного контроля необходимы:

– план-схема местности, границы контролируемой зоны объекта и места возможного ведения разведки ПЭМИН;

– категория объекта информатизации;

– фактический состав основных и вспомогательных технических средств и систем защиты на объекте;

– план реального размещения технических средств на объекте;

– выполнение требований эксплуатационной документации по размещению и установке на объекте каждого технического средства и

средства защиты с учетом расстояний до мест возможного ведения РПЭМИН;

– обоснование применения средств активной защиты (САЗ).

В инструментальной части аттестационного контроля необходимо провести следующие работы:

– измерить или рассчитать для технических средств значения схемно-конструктивных параметров, характеризующих их защищенность от РПЭМИН;

– определить реальные размеры зоны R2 технических средств, установленных на объекте, по соответствующим методикам;

– проверить работоспособность всех средств защиты, включая САЗ;

– определить эффективность применения САЗ для защиты автоматизированных систем управления (АСУ) и электронно-вычислительной техники (ЭВТ).

По результатам аттестационного контроля оформляется Аттестат соответствия.

Эксплуатационный контроль защищенности от РПЭМИН на объекте предназначен для проверки выполнения правил эксплуатации и технического состояния каждого технического средства и оценки соответствия текущего состояния защищенности объекта и зафиксированного при аттестационном контроле.

Эксплуатационный контроль состоит из двух частей: организационной и инструментальной. При выполнении организационной части эксплуатационного контроля необходимо:

– проверить наличие Аттестата соответствия, журнала учета проведения эксплуатационного контроля, перечня и плана размещения технических средств на объекте;

– уточнить места возможного ведения РПЭМИ и при необходимости внести изменения в план-схему контролируемой зоны;

– проверить поэкземплярно соответствие реального состава технических средств и состава, указанного в перечне технических средств на объекте;

– сверить соответствие действительного расположения технических средств и средств защиты расположению, приведенному в плане размещения технических средств на объекте;

– сверить соответствие сведений о степени секретности обрабатываемой информации и установленной категории объекта.

В инструментальной части эксплуатационного контроля необходимо:

– для средств защиты и технических средств произвести измерения параметров защищенности от РПЭМИ, которые были определены на этапе аттестационного контроля;

– для технических средств АСУ и ЭВТ измерить напряженность электрических и магнитных полей в реперных точках (точках с максимальным значением зоны R2) и результаты измерений сравнить с результатами аттестационного контроля;

– проверить работоспособность средств активной защиты.

В случае положительных результатов эксплуатационный контроль объекта считается завершенным, о чем составляется Акт проведения эксплуатационного контроля на объекте. При выявлении недостатков последние устраняются и контроль повторяется.

Функциями определения размеров зоны R2 технических средств, установленных на объекте, а также проверкой эффективности средств активной защиты обладают многие комплексы, но данные программные продукты являются дорогостоящими и зачастую работают с конкретной аппаратурой. Поэтому был создан универсальный и многофункциональный продукт, автоматизирующий процесс оценки защищенности от РПЭМИН. Основной задачей является расчет расстояний распространения информативных сигналов и значения допустимого пробега линий и коммуникаций до границы КЗ, а также составление соответствующих протоколов.

В программе предусмотрено два основных режима работы: без САЗ и с применением САЗ. В зависимости от данных режимов результатом выполнения программы может являться протокол оценки защищенности ОТСС от утечки конфиденциальной информации по каналу ПЭМИ и контроля защищенности информации, обрабатываемой ОТСС, от ее утечки за счет наводок информативного сигнала на линии и коммуникации или протокол контроля эффективности принятых мер защиты информации ОТСС от утечки конфиденциальной информации по каналу ПЭМИН соответственно.

Предоставляя оператору возможность выбора различных режимов и настроек, а также функций вывода готовых к дальнейшей обработке протоколов, данный программный продукт значительно упрощает процесс проведения контроля защищенности объектов от РПЭМИН.

ЛИТЕРАТУРА

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. Технические средства и методы защиты информации: Учеб. для вузов. М.: ООО «Издательство Машиностроение», 2009. 508 с.

2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учеб. пособие. М.: Горячая линия – Телеком, 2005. 416 с.

ПРИМЕНЕНИЕ СВЕРХРАЗРЕШЕНИЯ В ЗАДАЧЕ ПОВЫШЕНИЯ КАЧЕСТВА ВИДЕОИЗОБРАЖЕНИЯ ОБЪЕКТА НАБЛЮДЕНИЯ

А.А. Полетаев; Р.Т. Файзуллин, науч. рук., д.т.н., профессор, проректор ОмГТУ по информатизации

г. Омск, ОмГТУ, poletaev.andrew@gmail.com

В настоящее время существует необходимость получения качественного изображения объекта наблюдения (предмета обстановки, лица человека, номера машины) в более высоком разрешении. Повышение качества видеоизображения является важной и актуальной проблемой при проектировании систем видеонаблюдения, систем охранного телевидения, систем контроля и управления доступом [1]. Более качественное изображение объекта наблюдения позволит с большей вероятностью идентифицировать субъект доступа, предотвратить потенциально опасную ситуацию, получив чёткое изображение подозрительного предмета, или повысить эффективность системы видеонаблюдения в целом.

Сверхразрешение и его применение к видеоданным

Процесс восстановления изображения высокого разрешения из нескольких изображений одного и того же объекта называют сверхразрешением (Super Resolution) [2–4].

Целью сверхразрешения является поиск изображения высокого разрешения, удовлетворяющего представленной модели. Математически данную задачу можно сформулировать так: даны K изображений $\left\{X_L^{(n)}\right\}_{n=1}^{K}$ размера $M_1 \times M_2$, найти изображение X_H размера $N_1 \times N_2$ такое, что функция ошибки будет минимальной:

$$E(X_H) = \sum_{n=1}^{K} \left\| P_n(X_H) - X_L^{(n)} \right\|_2^2,$$

где $P_n(X_H)$ – проецирование изображения высокого разрешения X_H на плоскость изображений низкого разрешения $X_L^{(n)}$.

Обычно оно состоит из следующих шагов:

1) геометрическое преобразование;

2) изменение разрешения изображения (наличие этого этапа отличает алгоритмы сверхразрешения от алгоритмов восстановления изображений [5]);

3) размытие изображения (применение фильтров);

4) добавление шума.

В данной постановке задача не имеет устойчивого решения, поэтому зачастую добавляют дополнительные ограничения и предположения относительно X_H [2, 3]. При этом практическая реализация алгоритмов сверхразрешения сопряжена с решением множества технических проблем, одной из которых, исходя из описания модели, является следующая: изображения низкого разрешения должны незначительно отличаться друг от друга (в случае изображения одного объекта, не изменяющегося со временем, это условие почти всегда выполняется). Однако если рассмотреть возможность практического применения разработанных методов сверхразрешения в системах видеонаблюдения, становится очевидно, что видеоданные, как правило, отображают одновременное, не упорядоченное движение множества объектов и не пригодны для использования без предварительной обработки, позволяющей свести задачу получения изображения высокого разрешения из видеоданных к задаче получения изображения высокого разрешения из набора изображений более низкого разрешения (то есть к стандартной задаче сверхразрешения). Для этого предлагается использовать алгоритм поиска характеристических точек, а также алгоритм отслеживания движения между соседними кадрами.

В данной статье под объектом наблюдения будем понимать набор координат точек (пикселей), с набором которых будем ассоциировать объект наблюдения, указываемых пользователем (оператором) вручную на изображении объекта. Наиболее простым решением для этого является поиск так называемых характеристических точек или «углов Харриса» [6, 7] вблизи отмеченных пользователем координат.

Для получения фрагмента кадра, содержащего объект, воспользуемся следующим приёмом: построим окружность такую, что внутри неё лежат все характеристических точки, после этого вокруг окружности построим квадрат, центр которого совпадает с центром построенной окружности. Таким образом, мы получим фрагмент текущего кадра, содержащий только объект наблюдения.

В качестве основного метода для отслеживания движения далее будет рассмотрен метод Лукаса–Канаде [6, 8].

Для того чтобы повысить надёжность работы предложенного алгоритма и уменьшить количество ложных срабатываний, вызванных недостаточно качественным отслеживанием, а также изменениями самого объекта, необходимо ввести дополнительную процедуру проверки результата.

Например, пусть в качестве объекта выступает лицо человека, в качестве изменений объекта можно рассмотреть поворот головы. Данные изменения не вызовут остановку алгоритма отслеживания, так как

перемещение характеристических точек на соседних кадрах, скорее всего, не превзойдёт размер окна поиска (в методе Лукаса–Канаде данный параметр влияет на качество отслеживания: чем он выше, тем хуже результат, поэтому простое увеличение не решает проблему), однако получаемые изображения, очевидно, не будут соответствовать друг другу. Следовательно, целесообразно дополнить алгоритм проверкой соответствия текущего фрагмента эталонному образцу (фрагменту кадра, полученному при инициализации алгоритма), для этого удобно воспользоваться нормализованным коэффициентом корреляции [6].

Применение методов сверхразрешения – технически сложно выполнимая задача, в частности, в общем случае невозможно непосредственное применение методов восстановления изображения для видео.

В статье предложен алгоритм, позволяющий получить последовательности изображений объекта наблюдения из видеоданных. Была выполнена его программная реализация на языке высокого уровня Python с использованием свободно распространяемой библиотеки OpenCV [6].

Применение предложенного алгоритма совместно с методами восстановления изображений может быть полезным для решения актуальных проблем систем видеонаблюдения, систем охранного телевидения, систем контроля и управления доступом.

ЛИТЕРАТУРА

1. Насонов А.В., Крылов А.С., Ушмаев О.С. Развитие методов повышения качества изображений лиц в видеопотоке // Информатика и её применения. 2009. Т. 3, вып. 1.

2. Chaudhuri S., Joshi M.V. Motion-Free Super-Resolution. Berlin: Springer, 2005. 239 p.

3. Farsiu Sina, Robinson Dirk, Elad Michael, Milanfar Peyman. Fast and Robust Multi-Frame Super-Resolution // IEEE Trans. On Image Processing. 2004. Vol. 13, №. 10. October. P. 1327–1344.

4. Тихонов А.Н., Арсенин В.Я. Методы решения некорректных задач. М., 1979.

5. Теребиж В.Ю. Введение в статистическую теорию обратных задач. М.: ФИЗМАТЛИТ, 2005.

6. Bradski G., Kaehler A. Learning OpenCV. O'Reilly Media, Inc, 2008. 526 p.

7. Harris C. and Stephens M. A combined corner and edge detector // Proceedings of the 4th Alvey Vision Conference. 1988. P. 147–151.

8. Lucas B.D., Kanade T. An iterative image registration technique with an application to stereo vision // Proc. of Imaging understanding workshop. 1981. P. 121–130.

МЕРОПРИЯТИЯ ПО ПРИВЕДЕНИЮ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ В СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

А.А. Пузырев, студент 5-го курса; В.Д. Зыков, науч. рук., аспирант
г. Томск, ТУСУР, каф. КИБЭВС, alekseipyz@mail.ru

В настоящее время, на территории Российской Федерации осуществляется государственное регулирование в области обеспечения безопасности персональных данных. Правовое регулирование вопросов обработки персональных данных осуществляется в соответствии с Конституцией Российской Федерации и международными договорами Российской Федерации на основании вступившего в силу с 2007 г. Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» [1].

В силу требований Федерального закона «О персональных данных» все информационные системы персональных данных (ИСПДн), созданные до введения его в действие, должны быть приведены в соответствие установленным требованиям до 2011 г.

В соответствии с законом «О персональных данных» постановлением Правительства от 17.11.2007 г. №781 было утверждено «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» [2], которое устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПД). Согласно Положению ИСПД подлежат классификации. ИСПД, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных, относятся к специальным информационным системам [3]. Механизмы безопасности для специальных систем определяются на основании модели угроз.

Кроме того, все учреждения и организации системы здравоохранения, социальной сферы, труда и занятости обязаны обеспечивать защиту персональных данных в соответствии с требованиями Методических рекомендаций Минздравсоцразвития России.

В соответствии с требованиями вышеизложенных документов каждое учреждение – владелец медицинской информационной системы должно провести следующие мероприятия:

1. Разработать и утвердить внутри учреждения приказ о защите персональных данных и о подразделении по защите персональных данных.
2. Разработать и утвердить план мероприятий по защите персональных данных.
3. Назначить ответственных лиц за обработку персональных данных.
4. Разработать и утвердить внутри учреждения Концепцию информационной безопасности и Политику информационной безопасности.

5. Провести внутреннюю проверку.

6. Определить состав и категории обрабатываемых персональных данных.

7. Провести классификацию медицинской информационной системы.

8. Разработать и утвердить внутри учреждения Положение о разграничении прав доступа к обрабатываемым персональным данным.

9. Разработать модель угроз медицинской информационной системы.

10. Зарегистрироваться в Роскомнадзоре (уполномоченном органе по защите прав субъектов персональных данных) в качестве оператора персональных данных.

11. Разработать комплект организационных документов по защите персональных данных (инструкции, порядки, журналы и др.).

12. Провести необходимые технические мероприятия для обеспечения защиты персональных данных при их обработке в медицинских информационных системах.

13. Декларировать соответствие или провести аттестационные (сертификационные) испытания медицинской информационной системы [4, 5].

Основополагающим этапом при проведении мероприятий по защите персональных данных в медицинской информационной системе является внутренняя проверка. В одном из медицинских учреждений Томской области была проведена внутренняя проверка двух медицинских информационных систем. По результатам проверки были сформированы отчеты, в которых отражены следующие сведения:

1) состав и структура объектов защиты;

2) состав и структура обрабатываемых персональных данных;

3) конфигурация и структура медицинской информационной системы;

4) режим обработки персональных данных;

5) список лиц, допущенных к обработке персональных данных, уровень их доступа;

6) угрозы безопасности персональных данных;

7) существующие меры защиты персональных данных.

В ходе внутренней проверки также были сформированы перечень необходимых мер по защите персональных данных и план по их реализации в учреждении.

ЛИТЕРАТУРА

1. Федеральный закон №152-ФЗ от 27.07.2006 г. «О персональных данных».

2. Постановление Правительства от 17.11.2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

4. Нормативно-методический документ Минздравсоцразвития России «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» от 23 декабря 2009 г.

5. Нормативно-методический документ Минздравсоцразвития России «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости» от 23 декабря 2009 г.

ИСПОЛЬЗОВАНИЕ OPENSSL ДЛЯ ШИФРОВАНИЯ ДАННЫХ*

И.А. Рахманенко, студент 3-го курса;
Н.А. Новгородова, науч. рук., ст. преп.
г. Томск, ТУСУР, каф. КИБЭВС, mail_ivan@sibmail.com

В современном мире все большее значение приобретает информация. Владение информацией дает большие возможности. Соответственно первичным становится приоритет по ее защите.

Изначально было решено создать модуль для шифрования данных и дальнейшей передачи по небезопасным каналам связи в приложении, работающем с базами данных, однако в процессе выбора средств решения данной проблемы появилась возможность использования системы и в других приложениях. Для решения данной задачи был выбран пакет свободно распространяемых библиотек OpenSSL.

OpenSSL – криптографический пакет с открытым исходным кодом для работы с SSL/TLS. Он позволяет создавать ключи RSA, DH, DSA и сертификаты X.509, подписывать их, формировать CSR и CRT. Также имеется возможность шифрования данных и тестирования SSL/TLS-соединений.

Данный пакет библиотек работает с Microsoft Windows, большинством UNIX-подобных операционных систем (включая Solaris, Linux, Mac OS X), а также для OpenVMS. OpenSSL основана на библиотеке

* Выполнено в рамках проекта ГПО КИБЭВС-0902 – Инженерия баз данных.

SSLeay, написанной Эриком Янгом (Eric A. Young) и Тимом Хадсоном (Tim Hudson).

Протокол SSL (Secure Sockets Level – уровень защищённых сокетов) обеспечивает установление канала шифрованной связи между Web-клиентами и серверами. В последних версиях SSL, помимо этого, обеспечивается идентификация клиента: сервер знает, какие клиенты с ним работают, и наоборот. SSL также обеспечивает независимость от алгоритма шифрования, так что отпадает необходимость пользоваться одним и тем же алгоритмом RSA, основанным на применении открытых ключей.

Для данного проекта была выбрана технология OpenSSL не только из-за того, что код этой библиотеки свободно распространяемый, но и из-за работы с различными криптографическими алгоритмами. В новой версии OpenSSL, разрабатываемой на данный момент, будут добавлены российские сертифицированные алгоритмы шифрования, такие как: ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 – алгоритмы цифровой подписи, ГОСТ Р 34.11-94 – алгоритм вычисления хэш-функции, ГОСТ 28147-89 – симметричное шифрование с ключом 256 бит. Работоспособность данной библиотеки в различных операционных системах позволит облегчить перенос разрабатываемого приложения на различные операционные системы.

Протокол SSL расположен под протоколами уровня приложений (такими, как HTTP,NNTP, Telnet, FTP и т.п.) и над протоколом TCP/IP. Данная стратегия позволяет SSL работать независимо. С применением SSL, одновременно на сервере и клиенте сообщения передаются в зашифрованной форме, гарантирующей приватность.

В данный момент полученное приложение имеет возможность создавать пару открытый / закрытый ключ с помощью RSA, а также осуществлять шифрование/расшифровывание данных этим криптографическим алгоритмом. В дальнейшем планируется также осуществлять работу с приведенными выше алгоритмами ГОСТа, а также добавить возможность создания канала связи, использующего SSL-соединение.

К достоинствам разработанной программы можно отнести:

– возможность создания ключа максимально большой длины;

– высокую скорость шифрования данных;

– возможность шифровать/расшифровывать файлы любой длины.

К недостаткам можно отнести низкую скорость создания ключей большой длины и невысокую скорость расшифровывания данных.

Криптографическая защита информации должна осуществляться в процессе передачи и хранения данных. Так как информация является ценным ресурсом, то тема защиты передаваемых в Internet данных, а следовательно, и разработка данного программного модуля являются актуальными.

МЕТОДИКА ЗАЩИТЫ ЦИФРОВЫХ ВИДЕОДОКАЗАТЕЛЬСТВ ОТ ФАЛЬСИФИКАЦИИ ВСТРАИВАНИЕМ ЦИФРОВОГО ВОДЯНОГО ЗНАКА

П.А. Ренжин, аспирант; Р.Т. Файзуллин, науч. рук., д.т.н., профессор, проректор по информатизации ОмГТУ

г. Омск, Омский государственный технический университет, каф. комплексных систем защиты информации, par.81@mail.ru

В работе правоохранительных органов и судов доказательствами зачастую выступают видеозаписи. Это может быть съемка с места происшествия, запись, сделанная скрытой камерой в банкомате, или запись допроса. Авторы данной работы предлагают меры для предотвращения фальсификации такого рода доказательств.

Проведение следственных действий может сопровождаться съемкой видеокамерой. Фотографические негативы и снимки, киноленты, диапозитивы, фонограммы допроса, планы, схемы, слепки и оттиски следов, выполненные при производстве следственных действий, прилагаются к протоколу в момент его подписания (ст. 166 УПК РФ). К сожалению, как показывает опыт, условия хранения доказательств не совершенны. Невозможно полностью исключить доступ к доказательствам посторонних лиц, не говоря уже о злом умысле самих участников следственного действия. Видеозапись до представления в суде может быть изменена. Например, вырезана часть кадров или заменена другими, проведена коррекция с помощью графических редакторов. Допустим, на подлинной записи присутствует автомобиль, стоящий во дворе дома. Злоумышленник, желая, по каким-либо причинам скрыть присутствие данного автомобиля, переснимает место съемки в другое время и производит монтаж исходной записи. Либо с помощью графического редактора затеняет номер автомобиля, изменяет цвет.

Разумеется, существуют методики судебной экспертизы, позволяющие с большой точностью определить перерисовку кадров. С большой вероятностью можно также определить факт монтажа (по содержимому видеофайла, например, по изменениям освещенности). Достоинства предложенной в работе методики состоят, во-первых, в избегании сложных экспертных процедур, которые достаточно трудно проводить многократно. Во-вторых, одним из способов фальсификации является элементарная полная подмена контента, выявить которую гораздо сложнее. В-третьих, данная методика ввиду ее простоты может быть быстрым индикатором того, что необходимо провести экспертизу.

Для исключения фальсификации записи привлекается постороннее лицо, оказывающие услуги по защите видеоданных. Запрос на такие услуги может быть вызван любыми заинтересованными лицами, а

именно следствием, прокуратурой, стороной обвиняемого. После проведения видеозаписи в присутствии понятых в видеоданные встраивается цифровой водяной знак [1, 2].

В дальнейшем у заинтересованных лиц могут возникнуть сомнения в подлинности записи. Допустим, кто-то из участников следственного действия может сказать, что не помнит автомобиль, стоявший во дворе дома, или что процесс съемки происходил в другом месте.

В этом случае заинтересованные лица могут сделать запрос на установление подлинности цифровой видеозаписи. Если подлинность видеозаписи не удостоверяется, она исключается из рассмотрения в деле.

Соответственно, можно определить требования, которые должны быть предъявлены к цифровому водяному знаку. Это низкая робастность (разрушаемость при пережатии, перерисовке, незначительной яркостной коррекции) и защита от монтажа. Методики встраивания цифрового водяного знака, предложенные в работах [1, 2], удовлетворяют требованиям низкой робастности (как и многие другие алгоритмы [3]), но, в отличие от существовавших ранее, обладают защитой от монтажа.

Методики встраивания основаны на встраивании черно-белого изображения в младшие значащие биты случайными частями. Отличие данных методик от существовавших ранее заключается в добавлении аддитивного шума в младшие значащие биты и декодировании цифрового водяного знака с помощью суммирования и установки порога. Это обеспечивает ЦВЗ такие свойства, как низкая робастность и защита от монтажа. Разработана программа для встраивания для Widows XP на языке C++.

Разработана методика защиты цифровых видеодоказательств от фальсификации. Предложенная в работе концепция позволяет решать спорные вопросы в процессе ведения следствия и в суде.

ЛИТЕРАТУРА

1. Ренжин П.А. Способ внедрения стегосообщения в видеофайл случайными частями с помощью замены // Вопросы радиоэлектроники, сер. ОТ. 2008. Вып. 2. С. 153–157.

2. Renzhin P.A. Limits of application of randomized parts embedding of picture in a videodata by logical summation // Системы управления и информационные технологии. 2007. № 4.1 (30). С. 189–191.

3. Грибунин В.Г., Оков И.Н, Туринцев И.В. Стеганографическая защита речевых сигналов в каналах открытой телефонной связи // Методы и технические средства обеспечения безопасности информации: Сб. тезисов Российской НТК. СПб.: ГТУ, 2001. С. 83–84.

МЕТОДИКА ФОРМИРОВАНИЯ МОДЕЛИ ОТЛИЧИЙ АВТОРСКИХ СТИЛЕЙ

А.С. Романов, аспирант; А.А. Шелупанов, науч. рук., д.т.н., профессор, зав. каф. КИБЭВС, проректор по научной работе ТУСУР
г. Томск, ТУСУР, каф. КИБЭВС, alexx.romanov@gmail.com

Проблему идентификации автора текста при ограниченном наборе альтернатив сформулируем следующим образом. Имеется множество текстов $T=\{t_1,...,t_k\}$ и множество авторов $A=\{a_1,...,a_l\}$. Для некоторого подмножества текстов $T'=\{t_1,...,t_m\}\subseteq T$ авторы известны, т.е. существует множество пар «текст–автор» $D=\{(t_i,a_j)\}_{i=1}^{m}$. Необходимо установить, кто из множества А является истинным автором остальных текстов (анонимных или спорных) $T''=\{t_{m+1},...,t_k\}\subseteq T$.

В данной постановке задачу идентификации автора можно рассматривать как задачу классификации с несколькими классами [1]. В этом случае множество A составляет множество предопределенных классов и их меток, D – обучающие примеры, а множество T'' – классифицируемые объекты. Целью является построение классификатора, решающего данную задачу, т.е. нахождение некоторой целевой функции $F:T\times A\to[-1,1]$, относящей произвольный текст множества T к его истинному автору. Значения функции интерпретируется как степень принадлежности объекта классу: 1 соответствует полностью положительному решению, –1 – отрицательному. При этом каждый текст рассматривается как вектор признаков $X=\{x_1,...,x_n\}$.

Для определения отличий стилей авторов предлагается следующая последовательность действий:

1) Разбиение имеющегося множества текстов на две группы. Первая используется для обучения модели классификатора. Вторая – для проверки точности идентификации автора с помощью обученной модели.

2) Формирование модели текста путем выбора модели представления текстовой информации и выделения определенных информативных групп характеристик текста. Отличия в стилях авторов характеризуются главным образом употреблением и частотой встречаемости определенных признаков в тексте – вектором.

3) Приведение значений признаков в единый диапазон с помощью операций нормирования и шкалирования.

4) Корректировка параметров классификатора, позволяющих обеспечить высокую разделяющую способность исследуемых авторов, путем обучения классификатора на нормированных векторах признаков группы обучающих текстов и проверки точности обученного класси-

фикатора на векторах признаков тестовой группы текстов. Первоначальное обучение классификатора происходит с параметрами по умолчанию или при заданных параметрах.

5) Изменение перечня групп характеристик и/или признаков, составляющих группу, в случае если изменением параметров классификатора достичь требуемой точности не удается.

Итогом является обученная модель классификатора, веса связей которой настроены таким образом, чтобы классификатор был способен разделить стили авторов, на текстах которых он обучался при подаче на его входы подобранного набора признаков.

Итоговая модель, помимо информативности признаков текста, учитывающихся в статистических методах идентификации авторства, учитывает общую способность классификатора к разделению данных и его точность.

ЛИТЕРАТУРА

1. Шевелев О.Г. Методы автоматической классификации текстов на естественном языке: Учеб. пособие. Томск: ТМЛ-Пресс, 2007. 144 с.

К ВОПРОСУ О ФОРМАНТНОМ МЕТОДЕ ТЕКСТОЗАВИСИМОЙ ВЕРИФИКАЦИИ ДИКТОРА

А.Н. Ручай, аспирант;
А.А. Соловьев, науч. рук., д.ф.-м.н., зав. каф. КБиПА, профессор
г. Челябинск, ЧелГУ, каф. КБиПА, ruchai@pochta.ru

Последние исследования ученых в области голосовой биометрики были направлены на исследования формантного подхода верификации диктора [1, 4]. Но многие вопросы, связанные с этим подходом, не были затронуты, поэтому основной задачей исследования будет всестороннее изучение этого подхода в данной работе.

Проведенные исследования [5, 6] показали, что очень эффективной с точки зрения надежности работы систем верификации и идентификации диктора является самая простая метрика в l_1, поэтому ее и рекомендуется использовать при реализации систем идентификации и верификации диктора.

Было предложено вместо меры близости между распознаваемым объектом ω и классом Ω_g взять следующую меру сходства, которая в некотором смысле показывает вероятность сходства $S \in (0,1]$,

$$S(\omega,\{\omega_g\}) = e^{-d(\omega,\{\omega_g\})},$$

где $d(\omega,\{\omega_g\})$ – расстояние между распознаваемым объектом ω и классом Ω_g.

Мера S дает лучшую надежность, что было выяснено в ходе тестирования реализованных систем верификации и идентификации диктора.

При построении меры сходства в задаче идентификации и верификации диктора использовалась точечная оценка значений форманты как математическое ожидание амплитуды и частоты форманты, которое вычислялось по формуле

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i.$$

Данная оценка была естественным образом выдвинута из гипотезы о нормальном законе распределения формант [2], что было также подтверждено экспериментально с помощью статистических критериев проверки гипотезы на нормальность.

Данная оценка может быть модифицирована для случая выборок малого объема ($n \le 10$) [3]

$$\overline{x}^* = \sum_{i=1}^{n} \frac{x_i}{d_i \sum_{j=1}^{n} \frac{1}{d_j}}, \qquad d_j = \sum_{i=1}^{n} (x_i - x_j)^2.$$

Данная оценка значений амплитуды и частоты форманты дает хорошую надежность идентификации и верификации диктора, данную оценку рекомендуется использовать при реализации подобных систем.

Также в качестве точечной оценки можно воспользоваться робастной оценкой Ходжеса–Лемана по средним Уолша [3], которая устойчива к отклонениям от нормальности распределения и засоренности выборки аномальными значениями. Пусть $x_1,\ldots,x_n$ – выборка, $z_1,\ldots,z_m$ – средние Уолша, где $m = n(n+1)/2$ и $z_{ij} = (x_j + x_i)/2$ $(j \le i)$, тогда медиана ряда $z_1 \le \ldots \le z_m$ будет оценкой Ходжеса–Лемана.

Можно сделать еще один очень важный вывод, что в качестве оценки можно использовать не точечные оценки, а строить доверительные интервалы с определенным уровнем значимости. Для этого воспользуемся оценкой математического ожидания μ при неизвестной дисперсии

$$\overline{x} - t_\gamma \frac{s}{n} \le \mu \le \overline{x} + t_\gamma \frac{s}{n},$$

где t_γ – γ-квантиль распределения Стьюдента с $n-1$ степенями свободы; γ равно уровню значимости $(1+\alpha)/2$, $s^2=\frac{1}{n-1}\sum_{i=1}^{n}(x_i-\bar{x})^2$, $\bar{x}=\frac{1}{n}\sum_{i=1}^{n}x_i$. Для вычисления t_γ – квантили можно воспользоваться следующей аппроксимацией:

$$t_\gamma = u_\gamma\left(1-\frac{u_\gamma^2+1}{4n-4}\right), \qquad u_\gamma = 4{,}91\left(\gamma^{0{,}14}-(1-\gamma)^{0{,}14}\right).$$

Было экспериментально установлено, что при использовании доверительного интервала очень важно выбирать уровень значимости, но этот выбор не очевиден и может быть получен только в ходе тестирования надежности верификации и идентификации диктора.

В ходе тестирования надежности системы верификации диктора было установлено появление аномальных выбросов в выборке значений формант. В предположении о нормальном законе распределения формант данные выбросы должны быть обнаружены с помощью критерия Роснера [3, с. 557], который основан на последовательном применении критерия Граббса со следующей статистикой

$$\tau = \max\left(\frac{\bar{x}-x_1}{s}, \frac{\bar{x}-x_n}{s}\right).$$

По начальной выборке объема n вычисляеются значение статистики τ_1. Затем из выборки удаляется экстремальный член $x_{\min}(x_{\max})$ – в зависимости от того, какое значение более удалено от $\bar{x}$. Вычисление последовательных статистик ведется до тех пор, пока $\tau_{i+1}>\tau_i$, и пусть повторится k раз. Полученные значения статистик τ_i $(i=1,\ldots,k)$ каждый раз сравниваются с критическими значениями. Превышение критерием τ_i критического значения позволяет установить не только наличие выбросов, но и их количество.

С.А. Репалов впервые разработал и исследовал математический аппарат обработки формантных характеристик и на основе разработанного аппарата построил методы распознавания образов, использующие эти робастные характеристики речевого сигнала [4].

Форманту будем обозначать как $f=(w,a)$, где w – частота форманты, a – амплитуда форманты. Пусть множество $H\subset R^2$ будет пространством формант, тогда если $f=(w,a)\in H$, то $w>0$ и $a>0$. Введем метрику $h(f_1,f_2)$ в пространстве формант H, которая будет равна

$$\min\left(r(f_1,f_2),r(f_1,(w_1,0))+r(f_2,(w_2,0))\right),$$

где $$r^2(f_1,f_2)=c_w(w_1-w_2)^2+c_a(a_1-a_2)^2$$

является метрикой в R^2.

В теореме 2.1 из [6] было доказано, что $h(f_1,f_2)$ является метрикой в пространстве формант H.

Из сделанного вывода о том, что самая простая метрика в l_1 дает лучшую надежность, в качестве $r(f_1,f_2)$ нужно взять следующую метрику:

$$r'(f_1,f_2)=c_w|w_1-w_2|+c_a|a_1-a_2|.$$

Было доказано, что $h(f_1,f_2)$ с метрикой r' является метрикой в пространстве формант H.

Под формантным набором будем понимать набор формант

$F=\{f_i\}_{i=1}^n=\{(w_i,a_i)\}_{i=1}^n$, где $n\in N$ и $w_i\neq w_j$, если $i\neq j$.

Под пространством формантных наборов X будем понимать множество всех возможных формантных наборов. Введем метрику в пространстве формантных наборов X

$$d(F_1,F_2)=\min_B \sum_{i=1}^{\max(n1,n2)} h(f_{1,B_1(i)},f_{2,B_2(B(i))}),$$

где B – всевозможные перестановки на формантных наборах B_1 и B_2. В теореме 2.2 из [6] было доказано, что $d(F_1,F_2)$ является метрикой в пространстве формантных наборов X.

ЛИТЕРАТУРА

1. Аграновский А.В., Леднов Д.А. Теоретические аспекты алгоритмов обработки и классификации сигналов. М.: Радио и связь, 2004. 164 с.

2. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. М.: Радиотехника, 2004. 144 с.

3. Кобзарь А.И. Прикладная математическая статистика. Для инженеров и научных работников. М.: Физматлит, 2006. 816 с.

4. Репалов С.А. Разработка математических моделей и робастных алгоритмов идентификации дикторов по их речи: Дис. ... канд. физ.-мат. наук. Ростов. гос. ун-т, Ростов-н/Д: 2003. 140 с.

5. Ручай А.Н. Разработка текстозависимой системы идентификации диктора по голосу // Системная интеграция и безопасность: Сб. науч. сессии ТУСУР-2009. Томск: В-Спектр, 2009. С. 347–352.

6. Ручай А.Н. Реализация текстозависимой системы идентификации диктора по голосу // Проблемы теоретической и практической математики: труды 40-й Молодежной школы-конференции. Екатеринбург: УрО РАН, 2009. С. 316–320.

СИСТЕМА ЭЛЕКТРОННОГО ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА*

М.С. Саблин, Е.Ц. Чимитдоржиева, Б.В. Шефф, студенты 3-го курса; Н.А. Новгородова, науч. рук., ст. преп.
г. Томск, ТУСУР, каф. КИБЭВС, msvega@mail.ru

С развитием современного образовательного процесса множество крупных учебных заведений открывают филиалы в различных городах. Вследствие этого появляется необходимость централизованной передачи данных между элементами одной структуры. Рассмотрим данную проблему на примере ТУСУРа и его филиала в г. Сургуте. Одним из решений данной проблемы является электронная почта. По электронной почте электронный документ приходит к получателю в считанные минуты. Но с устранением одной проблемы появилась другая – защита информации, которую содержит электронный документ. В свете законов «О персональных данных» [1], «О коммерческой тайне» [2] и для коммерческих компаний, и для государственных организаций эта проблема приобретает особое значение.

Основной целью данной работы является построение системы электронного защищенного документооборота, в обязанности которого входят хранение, редактирование и накопление большого количества документов на примере ТУСУРа и его филиала в г. Сургуте. В ходе работы должно быть разработано Windows-приложение, выполненное по технологии «клиент-сервер».

Для обеспечения наиболее эффективного документооборота необходимо выделить следующие этапы:

– аутентификация пользователя в сети;

– контроль целостности документов, циркулирующих в автоматизированной системе;

– защиту документов от несанкционированного доступа в процессе их передачи;

– резервное копирование документов;

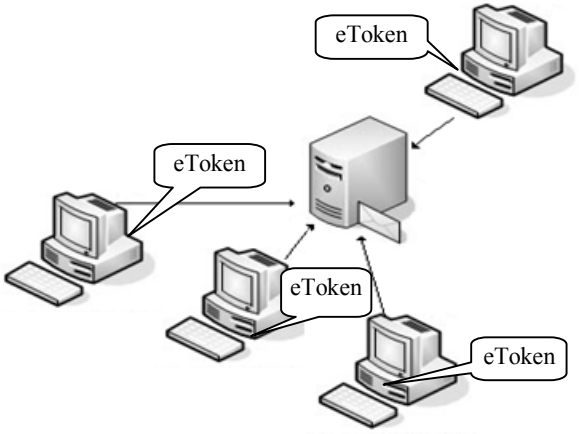
– ведение архива.

Первым и основополагающим этапом является выбор архитектуры (рис.). В данном случае была выбрана архитектура «клиент-сервер». Решение базируется на результатах эффективности работы данной структуры, хранения накопления и редактирования данных.

Аутентификация пользователей в сети производится с помощью eToken. Данный инструмент аутентификации является наиболее подходящим для данной архитектуры [3]. Также немаловажным является

* Выполнено в рамках проекта ГПО КИБЭВС-0902 – Инженерия баз данных.

контроль целостности документов, осуществляемый методом «контрольных сумм». В процессе передачи документов ведется мониторинг. Последним и немаловажным этапом разработки системы защищенного документооборота является резервное копирование данных. В представленной системе данный метод реализуется методом «теневого копирования».



Система защищенного документооборота

Таким образом, работа с документами в электронном виде позволяет быстро и удобно обрабатывать, хранить, передавать документы в информационной системе предприятия. От того, насколько полно в системе поддерживаются возможности обеспечения сохранности и конфиденциальности документов, во многом зависит общая безопасность документооборота предприятия.

ЛИТЕРАТУРА

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (в ред. Федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 N 363-ФЗ).

2. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» (в ред. Федеральных законов от 02.02.2006 № 19-ФЗ, от 18.12.2006 № 231-ФЗ 24.07.2007 № 214-ФЗ).

3. www.aladdin.ru

ПОДГОТОВКА К ВНЕДРЕНИЮ СЛУЖБЫ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ НА ПРЕДПРИЯТИЯХ НЕ ИТ-ПРОФИЛЯ

М.В. Савчук, аудитор Департамента внутреннего аудита по ИТ
г. Новокузнецк, ООО «ЕвразХолдинг», mikhail.v.savchuk@gmail.com

В настоящей статье рассмотрены особенности организации, а также возможные пути расширения функциональных обязанностей службы технической поддержки (Service Desk) на предприятиях не ИТ-профиля. Для предприятий, в основу бизнеса которых положены информационные технологии: операторов услуг сотовой связи, Интернет-провайдеров, разработчиков программного обеспечения, частично банков и т.д., роль ИТ-службы велика. Это связано с такими направлениями, как обеспечение непрерывности предоставляемых клиентам сервисов, качества функционирования внутренних систем, и многими другими. Однако основной целью любой коммерческой организации является получение прибыли, а для таких компаний характерна прямая зависимость прибыли от бесперебойного и качественного функционирования ИТ службы. То есть эффективность ИТ легко измерить, в т.ч. рентабельность вложенных в ИТ инвестиций.

Для предприятий не ИТ-профиля ситуация несколько иная. Например, эффективность отдела сбыта можно определить по объему продаж, юридического отдела – отсутствию потерь по судебным издержкам, необходимость наличия некоторых подразделений регламентируется внешними требованиями (в т.ч. бухгалтерской или экологической службы), а ИТ-отдел каким-то слабоизмеримым образом помогает остальным выполнять свои функции. Для наиболее реакционных отраслей промышленности ситуация усугубляется тем, что по сути ИТ-служба является придатком бухгалтерии, то есть обслуживающей структурой для другой обслуживающей структуры. Таким образом, ИТ в глазах руководства представляет собой некую черную дыру, которая поглощает финансовые средства, и зачастую немалые, без очевидного экономического эффекта.

В таких компаниях затраты на автоматизацию и её ценность определяются прежде всего личностью директора по ИТ. Это приводит либо к неэффективности или недооцененности ИТ в случае, если директор не обладает достаточным влиянием и компетенцией, либо к критической зависимости предприятия от одного сотрудника в обратном случае. Развитие обеих ситуаций неблагоприятно для компании в целом.

Внедрение Service Desk позволяет повысить управляемость ИТ-инфраструктуры, снизить уровень затрат, обеспечить более эффективное функционирование отделов эксплуатации и разработки, повысить уровень зрелости ИТ и т.д. Но помимо классических преимуществ ор-

ганизация службы поддержки пользователей является и своеобразной уловкой, позволяющей, с одной стороны, повысить прозрачность ИТ функции (включая обоснование операционных затрат на ИТ), с другой стороны, у директора по ИТ появляется возможность для построения платформы, обеспечивающей как повышение значимости ИТ [1], так и более существенной интеграции ИТ в деятельность предприятия (в т.ч. на участках, где смежные ИТ-функции, такие как сопровождение АСУТП систем или весового оборудования, переданы под руководство других подразделений). Проектируемая служба Service Desk представляет собой классический по структуре вариант, состоящий из следующих организационных элементов:

Первая линия поддержки – сотрудники, обеспечивающие прием и маршрутизацию заявок либо осуществляющие первичную консультацию сотрудников по общим вопросам, таким как собственно оформления заявки, либо в случае небольших организаций некоторые вопросы по эксплуатации информационных систем общего назначения: электронная почта, офисные пакеты и т.д.

Вторая линия поддержки – группа эксплуатации – обеспечивает настройку и сопровождение специализированного программного и аппаратного обеспечения: учетных, ERP, кадровых систем, клиент-банков, сетевого оборудования, систем резервного копирования, управляет подключением к информационным системам и т.д. Также принимает участие в тестировании нового программного обеспечения и разработке инструкций пользователей.

Третья линия поддержки – группа разработки – включает в себя наиболее квалифицированных технических специалистов, обрабатывающих запросы на существенные изменение либо разработку информационных систем.

В случае значительной интеграции ИТ в деятельность предприятия во вторую и третью линию поддержки могут включаться специалисты, занимающиеся обслуживанием АСУТП (в т.ч. SCADA) систем, обеспечивающим их настройку, замену датчиков, обучение обслуживающего персонала и т.д. [2].

Выбор технического решения по обеспечению Service Desk во многом определяет эффективность её функционирования. Выделим наиболее важные аспекты:

– Способность поддерживать качественное развитие, то есть позволять легко добавлять новые или улучшать существующие функциональные возможности. Сюда можно отнести такие элементы ITIL, как управление конфигурациями, проблемами, поддержка базы знаний, соглашений об уровне сервиса, развитая система отчетности и т.д.

– Способность масштабироваться, то есть иметь возможность поддерживать большее количество конечных пользователей и систем. Сюда можно включить поддержку нескольких организаций, развитую систему разделения полномочий между сотрудниками службы, широкие возможности по уведомлению, эскалацию инцидентов и т.д.

– Способность интегрироваться в существующие системы. То есть наличие хорошо документированного и структурированного интерфейса, позволяющего передавать данные между Service Desk и ERP, бухгалтерскими системами (например, в части управления запасами расходных материалов, закупа, контроля над их использованием), систем управления бизнес=процессами (будет рассмотрено в следующих статьях), систем автоматизированного мониторинга (также будет рассмотрено в отдельной статье).

Перечень требований, предъявляемых к развитой системе Service Desk, довольно широк. Поэтому для относительно небольших компаний, чьи потребности относительно невелики, имеет смысл внедрять систему Service Desk начального уровня либо собственной разработки.

Для крупных предприятий, в т.ч. холдингов, чья структура насчитывает тысячи компьютеров и десятки выделенных структурных подразделений, удаленных филиалов, внедрение крупной коммерческой системы более обосновано и дальновидно с точки зрения долговременного развития. Однако такой подход ввиду значительных затрат на внедрение требует серьезной обоснованной заинтересованности со стороны топ-менеджмента. В настоящий момент рынок предлагает большое количество готовых систем Service Desk, вопрос выбора сводится, прежде всего, к полноценному анализу структуры предприятия и его требований к ИТ.

Таким образом, уже в ходе рассмотрения всего лишь нескольких составляющих первых этапов подготовки становится очевидным, что внедрение технической службы на предприятии не ИТ-профиля является сложным процессом, однако последовательный комплексный подход к решению этой задачи позволит в полной мере получить преимущества Service Desk как в разрезе вложенных инвестиций, так и повышения эффективности предприятия в целом.

ЛИТЕРАТУРА

1. IT Assurance Guide – IT Governance Institute, 2007. 286 с.

2. Gerard Blokdijk, Ivanka Menken. Help Desk. Service Desk Best Practice Handbook. Emereo Pty Ltd, 2008. 192 с.

ПРОГРАММНЫЙ МОДУЛЬ ПРИНЯТИЯ РЕШЕНИЯ ПО РЕАГИРОВАНИЮ НА ОПАСНЫЕ СОБЫТИЯ В СЕТИ

И.Р. Сайфуллин, студент 5-го курса; Т.Х. Тухватшин, аспирант;
И.В. Машкина, науч. рук., д.т.н., профессор
г. Уфа, УГАТУ, каф. ВТиЗИ, ildar_sayfullin@mail.ru

В статье поднимается проблема выбора рационального варианта реагирования на опасные события в сети. Решение о выборе варианта реагирования принимается в зависимости от вероятности атаки, которая оценивается с использованием механизма нечеткого логического вывода, на основе оперативных данных о событиях безопасности от различных обнаружителей, что позволяет минимизировать ущерб. Поэтому данная тема является актуальным объектом исследований.

Задачей данной работы является разработка программного модуля принятия решения по реагированию на опасные события в сети. Программный модуль позволяет оперативно определять рациональный вариант реагирования на возможные угрозы для типовых путей распространения атак на основе модели противодействия угрозам нарушения информационной безопасности в сегменте корпоративной информационной системы.

Модели принятия решения, ставшие основой написания программного модуля, были предложены М.Б. Гузаировым, И.В. Машкиной, Т.Х. Тухватшиным в работах [1, 2].

Процесс выбора рационального варианта реагирования на опасные события описывается кортежем

$$\langle U_i, V_j, C(V_j), P_a, P(z_l), J, U*(P_a)\rangle,$$

где U_i – вариант реагирования; V_j – исход; C_j – оценка ущерба; z – параметр неопределенности состояния среды; $P(z_l)$ – вероятность состояния среды; J – целевая функция выбора; $U^*(P_a)$ – рациональный вариант реагирования; P_a – вероятность атаки.

Модель выбора рационального варианта формируется в виде графа связи вариантов реагирования на опасные события и исходов, а также с использованием функции реализации в табличной форме.

На рис. 1 показана блок-схема работы программного модуля принятия решения по реагированию на опасные события в сети.

На основе адаптированного для выбора рационального варианта реагирования метода принятия решений разрабатываются модели противодействия угрозам с учетом возможных путей их распространения:

- межсегментная атака;
- внешняя атака через беспроводную точку доступа;
- внешняя атака через периметр по высокоскоростному каналу.

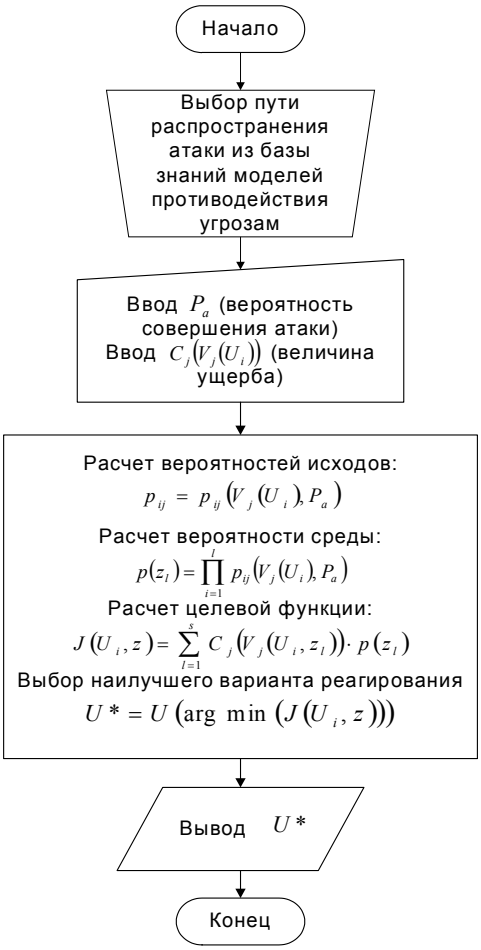


Рис. 1. Блок-схема работы программы

Модель противодействия угрозам в случае, к примеру, потенциально возможной межсегментной атаки представлена в виде графа и функции реализации, приведенных соответственно на рис. 2 и в таблице.

Варианты реагирования: U_1 – завершение сессии с атакующим узлом; U_2 – отсылка предупреждения пользователю или понижение приоритета пользователя.

Возможные исходы оцениваются по величине ущерба: $C(V_1)$ – ущерб отсутствует; $C(V_2)$ – ущерб пользователю (незначительный); $C(V_3)$ – ущерб системе (средний); $C(V_4)$ – ущерб от атаки (максимальный).

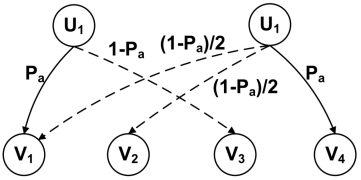


Рис. 2. Граф связей вариантов реагирования и исходов

Функция реализации

U	Z					
	$P(z_1)$	$P(z_2)$	$P(z_3)$	$P(z_4)$	$P(z_5)$	$P(z_6)$
U_1	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$
U_2	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$

Результатом данной работы является программный модуль, написанный на языке программирования Borland Delphi 7, позволяющий оперативно определять рациональный вариант реагирования на опасные события в сети.

ЛИТЕРАТУРА

1. Машкина И.В. Модели и метод принятия решений по оперативному управлению защитой информации // Системы управления и информационные технологии. Москва; Воронеж, 2008. №2(32). С. 98–104.

2. Гузаиров М.Б., Машкина И.В., Тухватшин Т.Х. Разработка моделей принятия решений по оперативному управлению защитой информации на основе численной оценки вероятности атаки // Известия Южного федерального университета. Технические науки. Ростов н/Д, 2008. №8. С. 18–24.

3. Гофман В.Э., Хомоненко А.Д. Delphi. Быстрый старт. СПб.: БХВ-Петербург, 2003. 288 с.

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ РАННЕЙ ДИАГНОСТИКИ ЗАБОЛЕВАНИЙ ТРОМБОЭМБОЛИЕЙ

Е.Ф. Щипунов, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, sef@security.tomsk.ru

В данной статье речь пойдет о наиболее трудно диагностируемом заболевании сердечно-сосудистой системы. Тромбоэмболия – так называют это заболевание, которое проявляется в виде закупорки ветвей легочной артерии тромбами, образовавшимися в большом круге кровообращения. Это заболевание трудно диагностировать, поскольку его появлению могут способствовать сразу несколько различных факторов. Основными факторами являются:

– повышенная вязкость крови;

– пониженная скорость тока крови;

– повреждение сосудов.

Смертность от тромбоэмболии составляет порядка 30%, однако адекватная тактика ведения пациента с точной диагностикой и своевременным назначением оптимального лечения позволяет снизить этот показатель до 2–8%. Тромбоэмболию далеко не всегда можно легко заподозрить и подтвердить, а надежные диагностические методы требуют финансовых затрат и определенное количество времени. Во многих случаях этого времени нет, поскольку тромбоэмболия развивается достаточно стремительно и зачастую становится причиной смерти многих больных [2].

Для решения данной проблемы требуется создать инструментальное средство, позволяющее диагностировать тромбоэмболию на ранней стадии развития болезни. Эту задачу можно решить, используя современные средства разработки программного обеспечения, алгоритмы и математические модели. Конечным результатом применения этих технологий является система поддержки принятия решений (СППР) для ранней диагностики заболеваний тромбоэмболией.

Работа данной системы основана на использовании сформированного регистра больных сердечно-сосудистыми заболеваниями, а также с помощью специальных математических методов, позволяющих оценить имеющиеся данные и вывести результирующее решение. В регистре должны содержаться данные о больных с подозрением на тромбоэмболию, а также имеющих другие заболевания сердечно-сосудистой системы. Случаи летальных исходов также должны содержаться в базе данных СППР со всеми сопутствующими параметрами. Помимо анализа данных, система должны выявлять закономерности между теми или иными параметрами болезни. То же самое относится и к возможности статистической обработки данных: построение графиков, диаграмм, гистограмм и иных форм визуализации; нахождение статистических закономерностей; получение результирующих соотношений по запрашиваемым параметрам.

На рисунке представлена структура системы поддержки принятия решений и введены следующие обозначения:

БЗ – база знаний, содержащая факты и правила вывода.

БД – база данных, содержащая все имеющиеся данные.

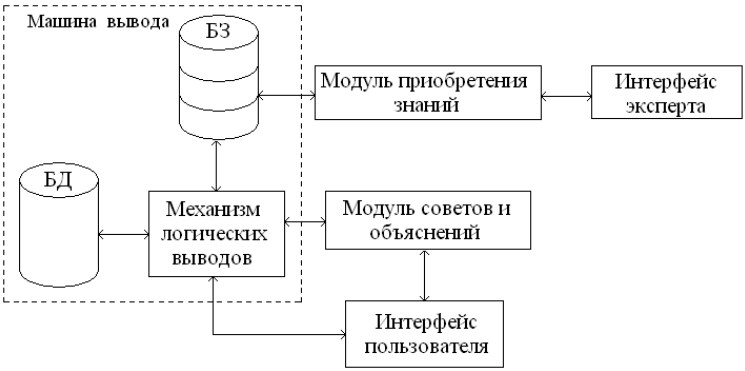
Модуль приобретения знаний – узел программы, отвечающий за ввод новых правил вывода.

Механизм логических выводов, позволяющий на основании данных, полученных от пользователя, и имеющихся правил вывода получить решение.

Модуль советов и объяснений – позволяет вывести логическую цепочку, с помощью которой было получено решение.

Интерфейс пользователя – система ввода-вывода запросов от пользователя и результатов работы программы.

Интерфейс эксперта, позволяющий эксперту работать с модулем приобретения знаний.



Структура системы поддержки принятия решений

В системе планируется продукционная модель представления данных. Эта модель эффективно применяется при создании систем поддержки принятия решений, а также при решении похожих задач [1].

Основным элементом в продукционной модели представления являются правила вывода. Правила вывода представляют собой импликацию или, по-другому, логическую цепочку вида: если <условие>, то <следствие>. Это называется ядром продукции [1].

В системе поддержки принятия решений планируется использовать недетерминированные ядра продукций: при актуализации посылки действие актуализируется в соответствии с фактором достоверности *F*.

В общем случае правило продукций имеет вид: если <*X*1, *X*2 ... *Xn*>, то <{*Y*1, *F*1}, ... {*Ym*, *Fm*}>.

– *X*1…*Xn* – набор условий;

– *Y*1…*Ym* – набор возможных исходов;

– *F*1…*Fm* – факторы достоверности, определяемые с помощью экспертных оценок.

Одним из вопросов, полагаемых для решения системой, является анализ выживаемости. Например, предложенная медиками задача – анализ выживаемости по следующим признакам:

– источник ТЭЛА;

– калибр пораженных сосудов;

– проводимость профилактических мероприятий;
– клинические признаки;
– давности ТЭЛА;
– наличие оперативного вмешательства.

Создание такой системы позволит значительно облегчить и улучшить возможности эксперта в вопросах диагностирования заболеваний тромбоэмболией на ранней стадии.

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Иванов А.С. Модель представления продукционных баз знаний на ЭВМ. Саратовский государственный университет. 2007. Т. 7, №1. С. 83–88.

2. Torbicki A. Konstantinides S. et al. Guidelines on the diagnosis and management of acute pulmonary embolism. The Task Force for the Diagnosis and Management of Acute Pulmonary Embolism of the European Society of Cardiology (ESC). Perrier A. // European Heart Journal. 2008. № 29 (18). P. 2276–2315.

СИСТЕМА ЭЛЕКТРОННОГО АРХИВА*

Б.В. Шефф, М.С. Саблин, Е.Ц. Чимитдоржиева, студенты 3-го курса; Н.А. Новгородова, науч. рук., ст .препод.

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

Быстрый рост объемов электронной информации, выполнение требований контролирующий органов и ограниченная емкость запоминающих устройств приводят к актуальности ведения электронных архивов. Использование электронных архивов в современных организациях обусловлено колоссальным объемом как текущего документооборота, так и еще более впечатляющими объемами архивных ресурсов. Необходимо сразу отметить, что архив электронных документов – это не просто отдельный сервер, компьютер или место для складирования носителей с информацией. Архив – это, прежде всего, технологии и производственные процессы, обеспечивающие весь цикл хранения документов от экспертизы ценности до их использования, через учет, описание, обеспечение сохранности и развитие научно-справочного аппарата и поисковых систем.

В качестве примера построения электронного архива возьмем Томский государственный университет систем управления и радиоэлектроники (ТУСУР). Весь процесс построения разбиваем на этапы:

* Выполнено в рамках проекта ГПО КИБЭВС-0902 – Инженерия баз данных.

– Описание электронных документов. На этом этапе подразумевается составление «библиотечной карточки», по данным которой можно узнать краткие сведения о документе. Эта «карта» должна содержать такие поля, как время поступления документа в архив, пользователя (автора), добавившего документ в архив, тип файла, дата последнего пользования, данные о последнем пользователе с документом, срок хранения, гриф секретности, сведения о оригинальности (целостности) документа, краткое описание содержимого документа, ключевые слова (из) документа.

– Обеспечение целостности информации. Простейшим методом контроля целостности документа является метод контрольных сумм. Однако наиболее приемлемым методом контроля целостности информации является использование хэш-функции, так как значение хэш-функции трудно подделать без знания ключа.

– Защита от несанкционированного доступа. Документы в архиве должны быть защищены от несанкционированного доступа средствами защиты информации для соответствующего уровня секретности / конфиденциальности.

– Резервное копирование данных, которое позволит не потерять документы при сбое системы.

Работа с электронным архивом дает следующие преимущества:

– длительное хранение без потери качества документов;

– быстрый и лёгкий поиск и доступ к документам;

– разграничение прав доступа к документам;

– работа с документами, учитывающими все последние обновления и исправления;

– выпуск документации высокого качества, независимо от срока хранения.

В заключение следует отметить, что организации архивного хранения электронных документов только начинает складываться. Здесь важен учет мнений и опыта всех заинтересованных сторон: архивистов (в архивах организаций и государственных архивах), делопроизводителей, ИТ-специалистов, управленцев, менеджеров, историков, других пользователей электронными информационными ресурсами. От этого зависит, что станет с накопленным информационным ресурсом организаций.

ЛИТЕРАТУРА

1. mosarchiv.mos.ru
2. www.reignvox.ru
3. www.alee-archive.ru

СТАТИСТИЧЕСКИЙ СТЕГОАНАЛИЗ МЕТОДОМ RS ДЛЯ ОБНАРУЖЕНИЯ LSB-СТЕГАНОГРАФИИ

Г.А. Шевчук, студент 4-го курса
г. Томск, ТУСУР, каф. КИБЭВС, vampiric@sibmail.com

Ежедневно в Интернете появляются миллионы мультимедийных файлов: графики, аудио- и видеоданные; публикуются текстовые посты и статьи. Вся информация копируется, пересылается большими объемами. Число доступных для использования программ по стеганографии постоянно увеличивается, многие программы реализуют одни и те же методы внедрения информации, значительно реже появляются новые, всё более изощренные. У простых пользователей появилась возможность скрытого обмена информацией.

Можно ли как-нибудь контролировать этот обмен?

Процесс стегоанализа требует значительных вычислительных ресурсов, отнимает много времени, помноженного на огромное количество файлов, и вообще не представляется возможным в крупных масштабах. В 2001 г. был проведен эксперимент. 2 млн картинок с сайта eBay, а также 1 млн картинок из архива USENET подверглись анализу на наличие стего. Исследование проходило в течение 5 дней, средняя скорость обработки около 7 изображений в секунду. В результате обнаружено 37 тысяч подозрительных картинок, но однозначно утверждать о наличии в них скрытых данных нельзя. Извлечь сообщения тем более не удалось. Для анализа использовалось около 200 машин, общая скорость которых грубо может быть приравнена к 72 машинам Pentium III 1200 МГц. Современные технологии позволяют выполнить такой анализ в разы быстрее. Очевидно, что проверки требуют как картинки, так и весь трафик, что существенно усложняет задачу.

Стегоанализ – новое направление в стеганографии, представляющее большой интерес. Найти информацию по этой теме очень сложно, новые разработки и достижения в области стеганографии не публикуются, делается это в целях борьбы с терроризмом. Однако встречаются отдельные выдержки из докладов, что-то публикуется, но объемлющей информации из них не получить.

Известно, что файлы графических форматов могут служить хорошим контейнером для стеганографической передачи данных, так как обладают необходимой информационной избыточностью. Одним из широко используемых методов стеганографии для изображений является LSB (least significant bits), который состоит в перезаписи младших бит изображения [1]. Одним из оригинальных методов статистического стегоанализа является метод RS, впервые опубликованный в 2001 г. коллективом ученых под руководством Дж. Фридриха [2, 3].

Суть метода заключается в разделении всего изображения на группы пикселей, для которых высчитываются статистические показатели (дисперсия, перепад значений), для этих же групп высчитывается функция флиппинга. Определяют две функции флиппинга – F1, соответствует инверсии младшего бита пикселя, и F2, представляющая собой инверсию с переносом в старший бит (прибавление единицы). Флиппинг преобразовывает группы пикселей. На основе сравнения статистических данных преобразованных и не преобразованных групп выделяют 3 класса: регулярные группы, сингулярные группы и неиспользуемые группы.

Метод основывается на статистическом предположении, что для естественного изображения, другими словами, незаполненного контейнера, соотношение между группами не должно существенно меняться. Значительное расхождение между значениями свидетельствует о применении LSB-стеганографии для младших бит изображения. Метод позволяет судить о количестве модифицированных бит и тем самым с приемлемой точностью (90–95%) определять длину сообщения. Для проведения исследований будет разработан программный комплекс, реализующий рассмотренный метод статистического стегоанализа.

Научный руководитель – Г.А. Праскурин, старший преподаватель каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-пресс. 2002.

2. Friedrich J., Miroslav G., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghampton: New York: SUNY, 2001.

3. Fridrich J., Du R., Meng L. Steganalysis of LSB Encoding in Color Image. New York City. ICME, 2000.

ОЦЕНКА КАЧЕСТВА РЕЧЕВОГО СИГНАЛА

П.С. Шорохов, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, rojja@mail2000.ru

Самым лучшим способом определения качества связи в сетях VoIP считается оценка его самими абонентами. Степень вредного воздействия шума, эха, задержек или помех от различных тоновых генераторов (warbling) на качество речевой связи определяется как интенсивностью этих факторов, так и тем, насколько они мешают разговаривать конкретным абонентам.

Кроме того, нужно иметь в виду, что оценка степени удовлетворенности абонентов IP-телефонии качеством связи – дело достаточно

сложное. В работе рассмотрены средства контроля качества речевой связи, позволяющие делать это достаточно эффективно в автоматическом режиме.

MOS-оценки. Официально рекомендуемым способом оценки качества IP- и других типов речевой связи является усредненная субъективная оценка MOS (Mean Opinion Score), алгоритм определения которой был разработана МСЭ-Т и последний раз корректировался в середине 90-х годов прошлого века. Алгоритм MOS, изложенный в спецификации МСЭ-Т P.800, основан на пятибалльной шкале – от единицы (самое плохое качество связи) до пяти (самое хорошее качество). В соответствии с этим алгоритмом группа людей оценивает качество звучания тестовых речевых шаблонов, передаваемых через сеть. Эти оценки, конечно, субъективны. Как правило, самый большой балл, который можно получить по данной методике, равен 4,5. Рейтинг в 4,0 балла и выше рассматривается как очень высокий, соответствующий качеству ТфОП (телефонные сети общего пользования). Цифровые сеансы связи часто получают даже более высокие оценки [1].

Попытки автоматизировать процесс получения оценок MOS делались еще задолго до широкого распространения технологии VoIP. Один из таких алгоритмов, известный как **PSQM** (Perceptual Speech Quality Measure), был закреплен МСЭ-Т в спецификации P.861. Однако PSQM, используемый в некоторых системах тестирования качества речевой связи, не слишком подходит для проверки VoIP-сетей, поскольку не учитывает, в частности, флуктуацию задержки (или джиттер), часто возникающую в IP-сетях. Между тем известно, что даже небольшая задержка между пакетами с речевой информацией вызывает изменения передаваемого речевого шаблона. В результате при сравнении отправленного и принятого шаблона может быть выставлена некорректная оценка качества речевой связи [1].

Современные программные средства, используемые для оценки качества речевой связи, выполняют свою работу максимально приближенно к тому, как это делает группа экспертов. Такие алгоритмы, как PSQM+, PESQ (Perceptual Evaluation of Speech Quality) и PAMS (Perceptual Analysis Measurement System), тоже предполагают передачу по VoIP-сети специальных речевых шаблонов и их последующий сравнительный анализ на приемной стороне сети. Алгоритм PESQ определен в стандарте МСЭ-Т P.862 [1].

Оценка качества связи PESQ. Алгоритм PESQ оценивает качество речи по стандартизированной в телекоммуникационной отрасли пятибалльной шкале – от 1 до 5 [МСЭ-Т P.800]. Однако оценка PESQ не превышает 4,5, поскольку обычно это максимальный показатель, получаемый путем субъективного тестирования по алгоритму MOS.

Оценка PESQ характеризует восприятие пользователями качества связи. Высшая оценка, равная 4,5, означает, что алгоритм не выявил никаких искажений. Чем больше искажений, тем хуже качество связи. Разработан ряд альтернативных оценок, которые получаются путем преобразования исходной оценки PESQ и лучше коррелируют с субъективными оценками MOS [2].

Алгоритм PSQM. Тест MOS, закрепленный в рекомендациях ITU P.800 и P.830, имеет один существенный недостаток: он требует значительных финансовых и временных ресурсов. Обойти его позволяют автоматические методы оценки качества. Хронологически первым из них стал алгоритм PSQM (Perceptual Speech Quality Measurement), закрепленный в рекомендации ITU-T P.861 (1996 г.). Он создавался для тестирования работы кодеков путем сравнения выходного речевого образа с входным и, строго говоря, применим только для этой цели. Между тем алгоритм PSQM нередко применяется для оценки сквозного качества голоса, хотя он нечувствителен к задержке передачи и ее флуктуациям, потерям, повторным передачам пакетов и т.д. В итоге оценки для сложной среды VoIP, выдаваемые PSQM, имеют мало общего с оценками MOS [3].

Алгоритм PAMS. PAMS является средством оценки качества речи разработанным компанией British Telecom. Тест выполняется путем передачи речи или речи-подобного сигнала в одном конце сети, и захвата этого же сигнала на другом конце. Оценка качества вычисляется с помощью математического сравнения исходного и полученного сигнала. Так же, как и в MOS, применяется 5-балльная система оценки качества голоса [3].

Заключение. При более детальном ознакомлении со средствами генерации оценок MOS нужно выяснить, какие проблемы они позволяют локализовать, в каком формате выдают информацию и как ее следует интерпретировать. Например, несмотря на то, что эти средства позволяют получить довольно точную оценку качества связи, они не всегда помогут выявить источник возникшей проблемы с качеством связи. Также нужно отдавать себе отчет, что выдаваемый некоторыми продуктами MOS-рейтинг представляет собой оценку качества некоторого среднего вызова, а качество конкретных сеансов связи может существенно отличаться от рейтинга MOS.

Научный руководитель – Р.В. Мещеряков, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Как измерить качество речевой связи: ООО «Сети и системы связи» [Электронный ресурс]. Режим доступа: http://www.ccc.ru/magazine/depot/05_08/read.html?0302.htm

2. Алгоритм PESQ: Компания SYRUS SYSTEMS [Электронный ресурс]. Режим доступа: http://www.pesq.ru/

3. Измерение качества голоса: scidom do blog [Электронный ресурс]. Режим доступа: http://scidom.blogspot.com/2008/07/blog-post.html

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ САЙТА С ЦЕЛЬЮ КРАЖИ ПОЛЬЗОВАТЕЛЬСКОЙ ИНФОРМАЦИИ ПРИ ПОМОЩИ XSS-АТАКИ

А.Ю. Сорокин, студент 4-го курса;
Р.В. Мещеряков., науч. рук., к.т.н., доцент
г. Томск, ТУСУР, каф. КИБЭВС, sasha15@bk.ru

Для просмотра информации, которая располагается в сети Интернет, пользователи компьютера чаще всего используют специальную программу – веб-браузер. Основная функция веб-браузера – отображение на экране веб-страницы, выполнение скриптов, обеспечивающих её динамичность и интерактивность. Если пользователь имеет возможность добавить на сайт произвольный интерпретируемый код (скрипт), исполняемый браузером, при этом не имея прямого доступа к сайту и серверу, то такой тип атаки можно характеризовать как XSS-атака.

XSS (англ. Cross Site Scripting) – тип уязвимости интерактивных информационных систем в сети Интернет. Специфика подобных атак заключается в том, что целью атаки является не сам сервер, а пользователь, который воспользуется сайтом, располагаемым на этом сервер. То есть сервер является посредником, средством атаки посетителя.

Основная причина возникновения уязвимости – недостаточная проверка данных, вводимых пользователем, которая позволяет вставить в обычный текст произвольные команды, интерпретируемые браузером как код.

По механизму исполнения XSS-атаки основными являются два типа:

− активная атака, когда вредоносный код хранится на сервере и выполняется веб-браузером жертвы при открытии им зараженной страницы. Такая атака активно используется в среде онлайн-дневников, социальных сетей;

− пассивная атака – вредоносный код не хранится на сервере и не может быть автоматически вызван. Для запуска такой атаки обычно требуется какое-либо воздействие со стороны пользователя.

Основная цель XSS-атак – получить доступ к пользовательской информации, хранимой в так называемых «Cookie» (HTTP Cookie).

Cookie – небольшой фрагмент данных, созданный веб-сервером и хранимый на компьютере пользователя в виде файла, который веб-браузер каждый раз пересылает веб-серверу при попытке открыть страницу соответствующего сайта. Cookie применяется для сохранения данных на стороне пользователя, а на практике обычно используется для:

- аутентификации пользователя;
- хранения персональных настроек пользователя;
- хранения данных о сессии доступа пользователя к сайту.

Если злоумышленник получит данные из Cookie, то он имеет возможность выдать себя от лица того человека, чьи данные он похитил, тем самым произведя несанкционированный доступ к системе.

Известный сайт http://vkontakte.ru ещё в начале своего развития хранил в Cookie такие данные пользователя, как E-mail и хэш пароля. Тем самым, если бы была произведена успешная активная XSS-атака, то злоумышленник смог бы получить базу данных E-mail адресов пользователей сайта, которую в последующем он мог бы продать прочим злоумышленникам. При использовании Rainbow-таблиц [1] существует возможность восстановить пароль из его хэша, тем самым произведя кражу пользовательского аккаунта.

Примеры атак:

- Отправка сообщения, содержащего вредоносный код. Например, злоумышленник написал в комментарии к статье текст «XSS-атака <script>alert(«XSS-attack exploit»);</script>». Теперь при открытии страницы с комментарием произойдет открытие окна, содержащего надпись «XSS-attack exploit».
- Кража Cookie. Пусть существует возможность отправить сообщение с текстом «<script>document.write(«<img src=http://example.com /image.php?cookie=«+document.cookie);</script>». Тем самым при загрузке страницы с сообщением произойдет обращение к сайту http://example.com к файлу image.php, которому в качестве входного параметра будет передано содержимое пользовательских Cookie.

Основные методы защиты:

- Запрет на использование html-тегов в сообщении, в частности тега <script>.
- Тщательная фильтрация данных, получаемых от пользователя.

ЛИТЕРАТУРА

1. Ferguson, Neils, Bruce Schneier. Practical Cryptography. Indianapolis: John Wiley & Sons, 2003. 432 p.

ГЕНЕРАЦИЯ КЛЮЧЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ОТПЕЧАТКОВ ПАЛЬЦЕВ

А.А. Суховей, студент 6-го курса МФТИ;
С.М. Гончаров, науч. рук., к.ф.-м.н., зав. каф. БИТС
г. Владивосток, МГУ им. адм. Г.И. Невельского, sumastal@mail.ru

Расширение области применения биометрии ставит ряд задач, которые не могут быть решены классическими биометрическими системами:

− хранимые данные должны быть преобразованы без возможности восстановления;

− в разных системах должны генерироваться различные уникальные данные.

Решение вышеописанных задач для современных биометрических систем является непреодолимым рубежом, упирающимся в сам принцип построения подобных комплексов – выделение биометрических образов, представляющих собой совокупность данных о физических характеристиках аутентификатора. В случае выделения из биометрических данных битовой последовательности появляется возможность решения поставленных задач, поскольку предполагается хранение в биометрической системе хэш-функции этой последовательности [1].

Первые шаги в этом направлении были сделаны в 2004 г., когда Е. Додис, Р. Островский, Л. Райцин и А. Смит предложили общие подходы к получению ключевой последовательности из нечетких данных при помощи процедуры «нечеткого извлечения» («fuzzy extractor»).

Нами предложены пути получения фиксированной последовательности на основе отпечатков пальцев.

Мы выделяем несколько ключевых этапов работы, приводящих к достижению поставленной цели:

− предварительная обработка отпечатка пальца;

− получение координат центра папиллярного узора;

− выделение ключевой биометрической последовательности.

Для выделения ключевой биометрической последовательности автором проведены исследования и предложены следующие этапы предварительной обработки:

• применение сглаживающего фильтра:

− полутоновое изображение T размером nxm подвергается преобразованию фильтрующей матрицей $W(i,j)=1/r^2; i,j\in(0,1,...,r)$ с размером r:

$$T(i,j)=\sum_{u=0}^{r}\sum_{v=0}^{r}W(u,v)*t(u,v),$$

где t – матрица размера rxr, полученная из изображения;

- бинаризация изображения:

– папиллярный рисунок делится на блоки B_i размером H, в которых каждому пикселю ставится в соответствие 0 или 1 в зависимости от его значения по отношению к математическому ожиданию M_i этого блока, т.е.:

$$B_i(m,n)=\begin{cases}1, B_i(m,n)\geq M_i * p,\\ 0, B_i(m,n)<M_i * p,\end{cases}$$

где p – корректирующий коэффициент, варьирующийся в зависимости от качества изображения от 0,98 до 1,02;

- скелетизация отпечатка пальца:

– проводится изменение толщины линий папиллярного узора до одного пикселя [2].

Определение координат отпечатка пальца включает следующие стадии:

– определение вероятных центров;
– фильтрация точек;
– определение координат точки O.

Нами предложен и реализован алгоритм, основанный на анализе линий папиллярного узора в локальной области с центром в точке O радиуса R, т.е. в нее попадают все точки изображения, удовлетворяющие условиям

$$|O_x - x| \leq R,$$
$$|O_y - y| \leq R.$$

Полученная область делится на сектора T_i шириной ω градусов, начиная с угла ω_0.

Для выделения ключевой биометрической последовательности в каждой области T_i производится преобразование F_1:

$$F_1 : T_i \rightarrow b_i \in N .$$

Учитывая использование помехоустойчивого кодирования, следует заметить, что число ошибок, определяемых при аутентификации, в секторе должно быть равно абсолютному значению разности b_i при регистрации пользователя и его идентификации. Использование значения b_i в ключевой биометрической последовательности не позволяет выполнить данное условие. По этой причине в алгоритм вносится преобразование F_2:

$$F_2 : b_i \to s_i \in \{0,1\}^l .$$

В результате выполнения алгоритма на выходе получаем вектор:

$$S' = (s_1, s_2, ..., s_n) ,$$

где n равно числу секторов в локальной области.

Приведенный алгоритм выделения ключевой биометрической последовательности является основой использования отпечатков пальцев в генераторе ключевой последовательности на основе нечетких данных (ГКПНД) [3]. Основываясь на нем, можно построить биометрическую систему, процедура регистрации в которой будет содержать следующие этапы:

− генерация случайной последовательности U, длина которой соответствует длине биометрической последовательности;

− вычисление открытой последовательности $V = S \oplus C_e(U)$;

− вычисление значения хэш-функции $H(U)$;

− вычисление ЭЦП $S(H(U), V)$ для исключения подмены данных.

Таким образом программно реализованы основные функциональные возможности описанной модели (в качестве помехоустойчивого кода использованы коды Рида-Соломона) и проведены эксперименты на базе данных из 521 отпечатка пальца, принадлежащего разным личностям.

Значение ошибок первого и второго рода оптимальны при способности помехоустойчивого кода исправлять от 10 до 12 ошибок.

Развитие ГКПНД может расширить рамки применения биометрических технологий в область криптографии, в частности, для генерации ключевых последовательностей для ЭЦП, а также систем аутентификации.

ЛИТЕРАТУРА

1. Jain K., Prabhakar S., Hong L., Pankanti S. Filterbank-Based Fingerprint Matching // IEEE Transactions on image processing. 2000. Vol. 9. P. 45–48. May.

2. Maltoni D., Maio D., Jain A.K., Prabhakar S. Handbook of fingerprint recognition. New York: Springer-Verlag, 2003. 408 p.

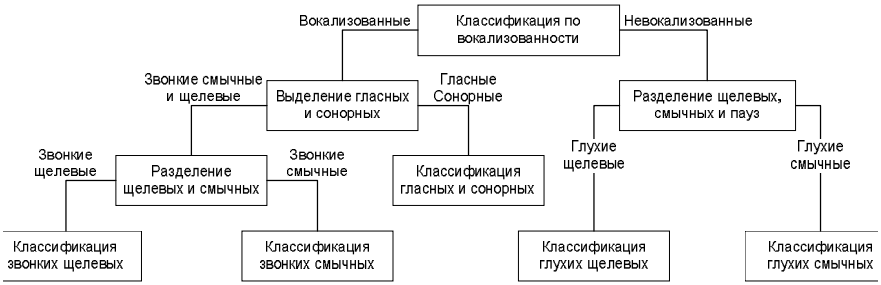
3. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. 2004.

ПАРАМЕТРИЧЕСКОЕ ОПИСАНИЕ ГЛАСНЫХ ЗВУКОВ В ПОТОКЕ РЕЧИ

С.Д. Тиунов, студент 5-го курса
г. Томск, ТУСУР, каф. КИБЭВС, t5d@ms.tusur.ru

Общепринятый подход к созданию систем автоматического распознавания речи связан с обучением под конкретный набор дикторов или конкретный набор распознаваемых слов. Такие системы являются весьма ограниченными в возможностях: они позволяют распознавать либо речь нескольких дикторов, либо ограниченный набор слов.

Подход к созданию системы, которая не обладает указанными недостатками, должен исключать обучение из способов создания конечной системы. Такой подход может быть основан, например, на иерархической классификации речевого сигнала, состоящей из нескольких алгоритмов, разделяющих речевой поток на сегменты одного класса (рисунок).



Иерархическая система классификации речевого сигнала

Автоматическая классификация гласных и сонорных является частью данной системы. В данной работе представлены исследования по получению необходимых статистических данных и созданию алгоритма для автоматической классификации гласных звуков.

Изначально для ограничения границ работы в класс исследуемых звуков входят только ударные гласные, так как:

– ударные гласные обладают наибольшей интенсивностью, длительностью и регулярностью;

– ударные гласные наиболее близки к основным оттенкам гласных, параметры которых давно исследованы и широко представлены в русской фонетической литературе.

Основные оттенки гласных различаются по трем различительным признакам: подъем, ряд и лабиализованность, которые определяются положением языка и губ при артикуляции гласного (таблица).

Система гласных фонем русского языка

Подъем	Передний ряд	Смешанный ряд	Задний ряд
Верхний	И	Ы	У
Средний	Э		О
Нижний		А	
	Нелабиализованные		Лабиализованные

Эти различительные признаки связаны с такими акустическими параметрами гласных, как частоты двух первых формант FI и FII [1]:

– подъем гласного влияет на частоту FI: чем выше подъем, тем ниже частота FI;

– ряд гласного влияет на частоту FII: чем более передний ряд, тем выше частота FII;

– лабиализованность гласного понижает частоты FI и FII.

В данной работе для определения частоты формант предлагается следующий подход: в каждой из областей значений формантных частот (200–800 Гц для FI и 800–2500 Гц для FII) измеряются частоты двух гармоник с максимальной интенсивностью. Таким образом, предлагаемые параметры:

– частота гармоники, максимальной по интенсивности в области частот 200–800 Гц;

– частота гармоники, второй по интенсивности в области частот 200–800 Гц;

– частота гармоники, максимальной по интенсивности в области частот 800–2500 Гц;

– частота гармоники, второй по интенсивности в области частот 800–2500 Гц.

Данные параметры в ходе исследований изменялись следующим образом:

– изменялись границы областей частот;

– изменялось количество учитываемых максимальных гармоник, попадающих в область частот;

– кроме того, учитывались соотношения между интенсивностями полученных гармоник: отношение интенсивности второй (третьей) гармоники к максимальной интенсивности.

Эксперименты сводились к получению статистики по ударным гласным на стационарном участке звучания, данная информация должна показывать:

– отражает ли данный тип параметров различия между гласными фонемами русского языка;

– в каких пределах лежат значения данных параметров для каждой из гласных фонем;

– позиции, в которых алгоритм, основанный на данных параметрах, может давать ошибки, а также оценку возможных ошибок;

– какова необходимая точность измерений (необходимое количество каналов фильтрации, необходимость вычисления частот гармоник) для приемлемой ошибки.

Характеристики исследуемого набора речевых сигналов:

– количество дикторов: не менее 10 (5 мужчин, 5 женщин);

– количество реализаций одной фонемы одного диктора одного оттенка: не менее 2;

– присутствующие фонемы: 6 гласных фонем (А, И, О, У, Ы, Э);

– присутствующие оттенки: обязательно должен присутствовать оттенок: ударный гласный между твердыми согласными.

В качестве инструментов для исследований использована система математического моделирования MATLAB. В данной системе предустановлена большая база математических алгоритмов, необходимых для цифровой обработки сигнала. Также в качестве инструмента для исследований использовалась система построения нейронных сетей для анализа речи, созданная в рамках проекта ГПО «Искусственный интеллект в задачах анализа и синтеза речи».

Научный руководитель – А.А. Конев, к.т.н., доцент каф. КИБЭВС.

ЛИТЕРАТУРА

1. Буланин Л.Л. Фонетика современного русского языка. М.: Высшая школа, 1970.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИИ И КОНТРОЛЯ ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ – ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ

Д.А. Толстунов, студент 5-го курса;
А.П. Зайцев, науч. рук., к.т.н., профессор
г. Томск, ТУСУР, каф. КИБЭВС, st.hate@list.ru

На сегодняшний момент инженерно-техническая защита информации переживает бурный рост. Многие организации заинтересованы в защите своих конфиденциальных данных и проводят мероприятия по предотвращению их утечки. Учитывая то, что в последнее время информация стала являться одним из самых ценных ресурсов предприятия, на рынке услуг по защите информации наблюдается ажиотажный спрос на проведение аттестации помещений для проведения совещаний и переговоров. Ведь, как известно, именно на закрытых совещаниях

циркулирует критически важная информация для предприятия, которая может потерять свою ценность ввиду известности третьим лицам.

Аттестация объекта информатизации по требованиям безопасности информации представляет собой комплекс организационно-технических мероприятий, в результате которых подтверждается, что на аттестационном объекте выполнены требования по безопасности информации, заданные в нормативно-технической документации, утвержденные государственными органами обеспечения безопасности информации и контролируемые при аттестации.

Комплекс специальных аттестационных мероприятий называется аттестационной проверкой и включает в себя контроль эффективности защиты.

Эксплуатационный контроль состояния акустической защищенности выделенного помещения проводится в целях документального подтверждения соответствия показателей эффективности принятых мер технической защиты установленным требованиям или нормам эффективности защиты информации.

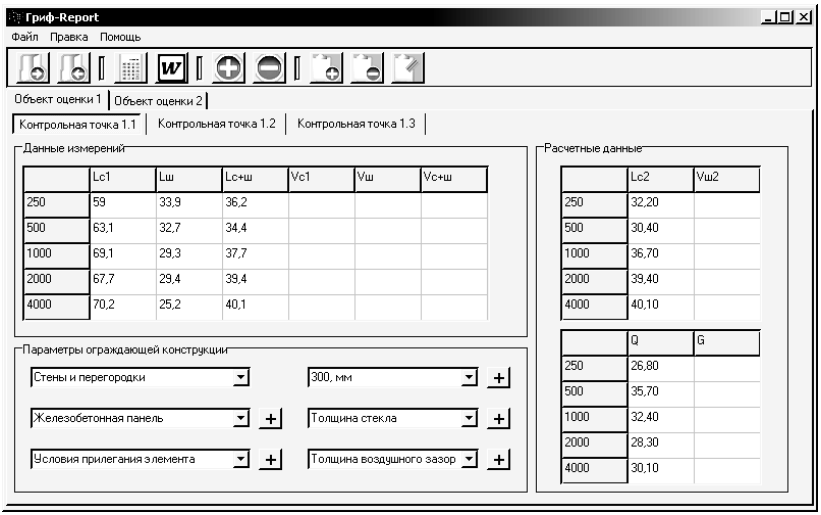
Эксплуатационный контроль состоит из двух частей: организационной и инструментальной.

Организационный контроль включает в себя проверку исходных данных об объекте, инженерно-технической документации, а также актов о проведении специальной проверки выделенных помещений и технических средств.

Методика инструментального контроля основывается на инструментально-расчетном способе определения отношений «речевой сигнал/акустический (вибрационный) шум» в контрольных точках в октавных полосах со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц. Далее происходит сравнением полученных результатов с установленными нормированными значениями. Методика ориентирована на использование контрольно-измерительной аппаратуры общего применения.

Результаты эксплуатационного контроля должны быть представлены в протоколе, а также сформулированы рекомендации и предложения по обеспечению выполнения норм защищенности.

Как видно, процесс аттестации и контроля защищаемых помещений является трудоемким, поэтому появилась необходимость автоматизировать этот процесс. Для этой цели был разработан программный продукт, основной задачей которого является расчет коэффициентов звуко- и виброизоляции, анализ результатов, а также составление протокола инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации. Внешний вид главного окна программы показан на рисунке.



Вид главного окна программы

Программа производит:

– расчет уровня акустического (вибрационного) сигнала в каждой контрольной точке для октавных полос со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;

– расчет коэффициентов звуко- и виброизоляции для каждой контрольной точки для октавных полос со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;

– анализирует результаты расчетов и выявляет контрольные точки, в которых не выполняются нормы защищенности;

– составляет протокол инструментально-расчетной оценки в формате MS Word. (В протоколе отображаются все результаты измерений и расчетов, а также указываются контрольные точки, в которых не выполняются нормы защищенности).

Программа позволяет:

– задавать количество контрольных точек и ограждающих конструкций с указанием типов и их параметров;

– хранить результаты измерений и расчетов в файлах;

– указывать информацию, которая должна быть отражена в протоколе.

Обладая удобным для оператора интерфейсом, автоматизируя процесс расчета показателей защищенности и анализа результатов, а также составления протокола, программный продукт значительно облегчает процесс аттестации и контроля защищенности помещения.

ЛИТЕРАТУРА

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учеб. пособие. М.: Горячая линия – Телеком, 2005. 416 с.

2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В, Скрыль С.В, Голубятников И.В. Технические средства и методы защиты информации: Учеб. для вузов. М.: ООО «Издательство Машиностроение», 2009. 508 с.

3. Положение по аттестации объектов информатизации по требованиям безопасности информации – Гостехкомиссия России, 1994.

СИСТЕМА УЧЕТА ОЦЕНОК СТУДЕНТОВ*

Р.В. Васин, студент 4-го курса

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

Цель работы: разработка автоматизированной информационной системы учета оценок студентов для филиалов ТУСУРа.

Задачи, поставленные для реализации:

− Учет списка студентов с возможностью добавления, редактирования и удаления записей о студентах.

− Учет списка преподавателей с возможностью добавления, редактирования и удаления записей о преподавателях.

− Учет оценок студентов с представлением наглядной информации о долгах студентов.

− Разграничение доступа к системе, возможность просмотра собственных оценок отдельными студентами.

− Возможность предоставления статистических данных: количество зачетов, экзаменов, курсовых из общего количества, средний балл и др.

− Реализация системы работы со штрих-кодами для эффективного предоставления информации об оценках.

Реализация системы

Для реализации системы выбрана среда программирования Microsoft Visual Studio. Для реализации базы данных – СУБД Firebird. Система поддерживает шифрование методом AES, которое используется для защиты информации в базе данных.

На данный момент в системе реализованы база данных, интерфейсы для работы со списком студентов, списком преподавателей, с оценками студента (рис. 1, 2). Сейчас идёт работа над внедрением системы штрих-кодов в программу.

* Выполнено в рамках проекта КИБЭВС-0842 – Инженерия баз данных.

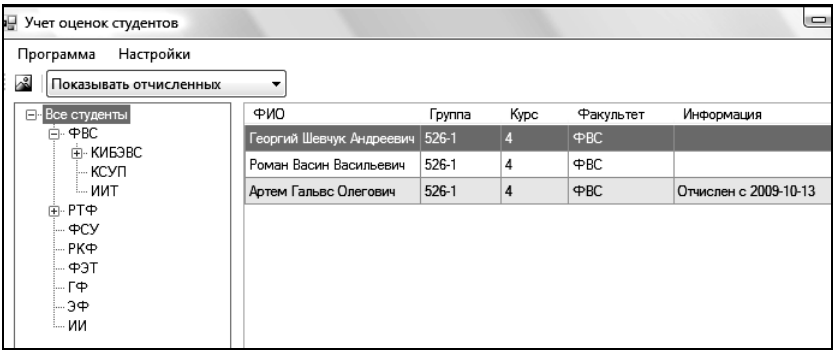


Рис. 1. Интерфейс редактирования списков студентов

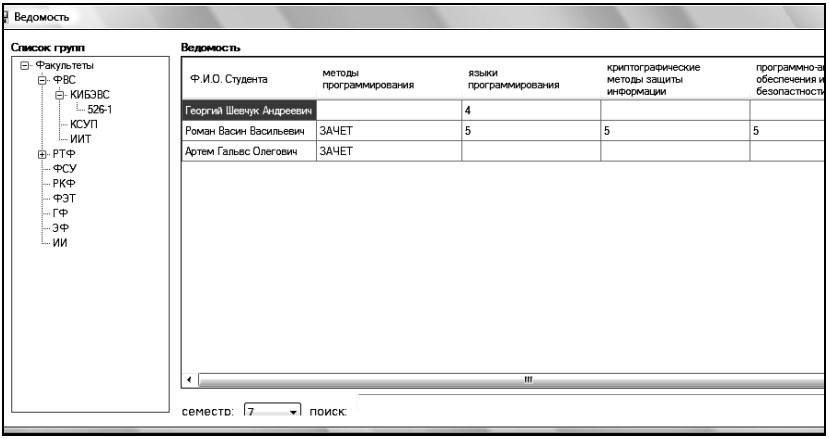


Рис. 2. Главная форма модуля «Ведомость»

Научный руководитель – Н.А. Новгородова, старший преподаватель каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1.Дейт К.Дж. Введение в системы баз данных. Introduction to Database Systems. 8-е изд. М.: Вильямс, 2006. 1328 с.

2.Кузнецов С. Д. Основы баз данных. 2-е изд. М.: Интернет-Университет информационных технологий; БИНОМ. Лаборатория знаний, 2007. 484 с.

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

4.Коннолли Т., Бегг К. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. Database Systems: A Practical Approach to Design, Implementation, and Management. 3-е изд. М.: Вильямс, 2003. 1436 с.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Н.А. Веретенникова, студентка 5-го курса;
А.А. Шелупанов, науч. рук., д.т.н., профессор, зав. каф. КИБЭВС, проректор по научной работе
г. Томск, ТУСУР, каф. КИБЭВС, azazel_n@sibmail.com

В настоящее время информационная безопасность (ИБ) – одна из важных проблем современного общества. Необходимым условием функционирования предприятия является обеспечение комплексной безопасности, которая заключается в системности проведения требуемых мероприятий, сбалансированности защиты, разработке организационно-технических мер и контроле их выполнения.

Комплекс мероприятий, необходимый для организации системы защиты, включает несколько этапов. На первом этапе планирования разрабатывается план, по которому проводится аудит безопасности и выявляется критически важная информация (уязвимости, каналы утечки и т.д.). По итогам аудита формируется полная и объективная оценка защищенности объекта, оценивается возможный ущерб, возникающий при утрате информации, составляются рекомендации, локализующие имеющиеся проблемы и содержащие в себе направление построения системы обеспечения информационной безопасности (ОИБ).

Следующим этапом является создание политики безопасности, в рамках которого разрабатываются технические, организационные, административные, юридические, физические меры, методы, средства, правила и инструкции, четко регламентирующие все вопросы ОИБ.

Таким образом, политику ИБ можно представить в виде многоуровневой системы документов, имеющих различное назначение и область применения. Наиболее эффективный метод выстраивания иерархии документов, составляющих политику ИБ, реализуется в использовании 4-уровневой модели, изображенной на рисунке.

Общая политика управления ИБ, или Концепция ИБ, находится на верхнем уровне и представляет собой нормативный документ, отражающий официально принятую организацией систему взглядов на проблему ОИБ, и является основой для создания всей структуры документов. Позволяет выработать комплекс мер нормативно-правового, технологического и организационно-технического характера с учетом современных тенденций развития информатизации.

К документам второго уровня относятся:

– частные политики ИБ, разрабатываемые под определенные области организаций. Могут содержать в себе требования по настройке механизмов ИБ в соответствии с рекомендациями производителей и

международных стандартов (ИСО/МЭК 17799, ИСО/МЭК 270001). Примерами частной политики безопасности являются политики криптографической или антивирусной защиты, резервного копирования, а также требования по ИБ в операционных системах, СУБД и прикладном программном обеспечении;

– корпоративные стандарты, регламентирующие требования к конкретным защитным механизмам и операциям. Их использование позволяет систематизировать процессы ИБ в совокупности с принципами ИБ, предыдущим опытом компании, отраслевыми стандартами и нормативами (ИСО/МЭК 9000, ИСО/МЭК 15408, ИСО/МЭК 13335) [1].

Иерархия документов политики ИБ

К третьему уровню иерархии относят процедуры и инструкции по ОИБ. Процедуры представляют собой описание процесса, относящегося к конкретной области ИБ, например, это может быть процедура предоставления доступа к сетевым ресурсам. Инструкции в свою очередь дополняют процедуры детальным описанием каждого шага по выполнению той или иной задачи. Целями разработки и применения являются оптимизация работы и сокращение времени выполнения до минимума, а также повышение уровня прозрачности и управляемости процессами ОИБ.

Документами самого нижнего уровня являются разного рода рабочие формы, журналы, заявки, протоколы и другие формы документов, используемые в рамках выполнения тех или иных процедур и являю-

щиеся отражением (и подтверждением) выполнения той или иной деятельности, например: форма заявки на предоставление доступа к сетевым ресурсам, форма журнала регистрации инцидентов ИБ и пр. Использование документов подобного типа применяется при возникновении инцидентов нарушения ИБ, служебных расследованиях и периодически проводящихся аудитах безопасности.

Политика безопасности является основой для понимания целей и задач ОИБ и главным механизмом системы управления информационной безопасностью (СУИБ). В СУИБ также должен быть включен циклический процесс взаимосвязанных непрерывных действий, акцентирующийся на поставленных целях и затрачиваемых ресурсах для их достижения. Данный процесс реализуется на применении PDCA-модели для всех процедур управления ИБ. PDCA-модель (или модель Шухарта–Деминга) определяет четыре этапа, которые последовательно должны выполняться для каждого процесса:

– plan (определение концепции ИБ, разработка политики безопасности по всем уровням);

– do (внедрение и функционирование политики ИБ);

– check (аудит безопасности, при отсутствии политики ИБ, является начальным);

– act (выполнение корректирующих и превентивных действий).

После того как все уровни политики ИБ пройдут хотя бы раз все этапы модели PDCA, СУИБ можно будет считать внедренной и оценить ее эффективность работы [2].

Разработка политики ИБ – достаточно трудоемкий процесс. Однако если работа по ОИБ будет комплексной и своевременной с применением рекомендации международных стандартов в области управления ИБ – ИСО/МЭК 27001:2005 и ИСО/МЭК 17799:2005, то процесс ОИБ достигнет необходимый уровень, а защита от угроз безопасности станет эффективной.

ЛИТЕРАТУРА

1. ГОСТ Р ИСО/МЭК 27001:2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования – http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=6&year=2008&search=27001&id=121123

2. Куканова Н. Практические аспекты применения международного стандарта безопасности информационных систем ISO 27001:2005 – http://dsec.ru/about/articles/practice_iso_27001/

ИНВЕНТАРИЗАЦИЯ ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.А. Вертинский, студент 5-го курса
г. Томск, ТУСУР, каф. КИБЭВС, dennis87@sibmail.com

Объектом исследования в данной работе является инвентаризация оборудования и программного обеспечения.

Под инвентаризацией в широком смысле понимается периодическая (чаще всего ежегодная) и регулярная проверка наличия и состояния материальных ценностей, принадлежащих организации, делается это посредством составления списков.

При инвентаризации компьютерной техники определяются:

– ее местоположение по рабочим местам/отделам;

– история перемещений;

– аппаратная конфигурация системных блоков;

– программная конфигурация системных блоков;

– производители комплектующих и программного обеспечения;

– гарантийные обязательства/лицензии на использование;

– сведения для бухгалтерского учета (поставщики техники, стоимость с учетом амортизации, накладные и счета-фактуры).

Вычислительная и оргтехника – это важный актив современной фирмы. Поэтому инвентаризация программных и аппаратных продуктов в течение всего жизненного цикла – одна из важнейших задач для любой компании.

Цели, которые преследует инвентаризация, – оптимизировать расходы на содержание парка компьютеров, периферийных устройств и покупку программного обеспечения; проверка программных продуктов на соответствие лицензионной политике (делается это, дабы избежать юридических исков за использование нелицензионного ПО); предоставление данных об основных средствах в налоговые органы (поскольку вычислительная техника приравнивается к средствам производства).

Традиционная сложность учета компьютерной техники состоит в том, что подобные объекты учета являются составными – компьютер как минимум имеет системный блок и монитор, а также устройства ввода-вывода (клавиатура, мышь, принтер, сканер и пр.). Естественно, возникает вопрос: как учитывать технику, если сама конфигурация компьютеров подвергается изменениям (модернизация, ремонт, списание, замещение)?

К тому же это довольно-таки трудоемкий процесс, требующий затрат большого количества времени.

Также с ростом количества компьютеров сложность процесса возрастает. Так, если для небольших фирм инвентаризацию возможно вы-

полнять вручную, то с ростом количества серверов и локальных станций это становится невозможным.

Основные задачи системы инвентаризации и управления аппаратным и программным обеспечением:

- предоставление сотрудникам компании необходимого программного обеспечения в нужном месте и в нужное время;
- уменьшение затрат на программное обеспечение благодаря наличию детальной информации об установленном программном обеспечении и его использовании.

Системы инвентаризации являются самостоятельным решением, функционал которых можно расширить за счет интеграции с системами регистрации и устранения неисправностей, мониторинга производительности ресурсов локальной сети, системам резервного копирования. Совокупность всех этих решений обеспечит эффективную работу и минимизирует простои в случае сбоя.

Научный руководитель – А.А. Конев, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Инвентаризация ПО: Microsoft Россия. URL: http://www.microsoft.com/rus/Licensemanagement/Implementing_InventorySoftware.mspx

О ПРОБЛЕМЕ ВЗЛОМА ПЕРЕБОРОМ И ПОТЕНЦИАЛЬНЫХ РЕШЕНИЯХ С ПОМОЩЬЮ СФЕРЫ РИМАНА И ВАРЬИРОВАНИЯ ЗАПЯТОЙ

А.А. Воробьев, студент

г. Комсомольск-на-Амуре, КнАГТУ, каф. ПМИ, zeromem@mail.ru

Симметричное шифрование, шифрование с открытым ключом, предложенные много десятилетий назад [5], имеют как ряд недостатков, так и преимуществ. Одним из недостатков является проблема bruteforce (англ. грубая сила), то есть взлома перебором «в лоб». Особенно остры споры вокруг DES (Data Encryption Standard, стандарт шифрования данных). В качестве преимуществ можно указать простоту основной идеи указанных алгоритмов.

В симметричных алгоритмах взлом «в лоб» заключается в переборе всевозможных ключей. В алгоритмах же с открытым ключом часто используются в качестве функции с секретом сложные математические задачи, требующие без знания секрета больших ресурсов для вычислений. Примером таких задач может служить задача о разложении доста-

точно больших чисел на множители или дискретное логарифмирование. Однако имеются проблемы.

Известно [2], что эти задачи являются сложными для решения, хотя это и не совсем верно. Практически их решать сложно. Но не доказано, что они действительно являются сложными, и отсутствие быстрого алгоритма решения не говорит о несуществовании такого [4].

Тенденция к нахождению все более быстрых алгоритмов, а также факт недоступности сегодня предсказания того, как быстро такие задачи смогут быть решены по временному периоду, можно увидеть в [6].

Далее условимся, что будем говорить только лишь о проблеме bruteforce. Исходя из текущего положения, логично задать вопрос: можно ли предоставить такое шифрование, которое бы совершенно не поддавалось bruteforce? Ответ на этот вопрос неоднозначный. Но главная идея [6] состоит в том, чтобы дискретное количество элементов представить элементами континуального множества. Тогда для перебора необходимо будет перебрать весь континуум, что невозможно.

Идея об отображении на сферу Римана

Пусть дано некоторое множество дискретных данных $I=\{a_i\}, i=1,2,\ldots,n.$ Предполагаем, что каждый элемент a_i является 8-битовым беззнаковым целым числом в диапазоне $[0,255]$.

Сопоставим ему некоторое равномощное множество $K=\{b_i\}$, т.е., другими словами, $|I|=|K|$. Из данного сопоставления получим некоторую совокупность упорядоченных пар $C=\{(a_i,b_i)\}, i=1,2,\ldots,n.$ Назовем шумовой функцией некоторую функцию $n(i)$ генерации элементов $b_i=n(i)$.

Тогда пары (a_i,b_i) можно считать некоторыми точками комплексных чисел z_i на комплексной плоскости φ (рис. 1).

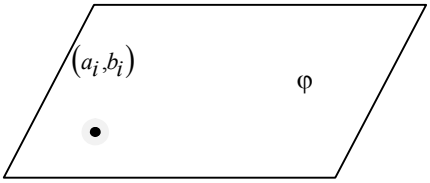


Рис. 1

Из теории функций комплексной переменной [3] известно, что эти пары могут быть биективно отражены на сферу Римана некоторого радиуса R с выколотой вершиной, т.к. предполагаем невозможность постановки точки в бесконечности.

В результате такого отображения совокупность упорядоченных пар перейдет в совокупность троек чисел

$$S=\{x(a_i,b_i),y(a_i,b_i),z(a_i,b_i)\}=\{x_i,y_i,z_i\}\ . \qquad (1)$$

Возможность данного отображения показана в [3]. Построим его.

Пусть дана декартова система координат, причем оси x и y лежат в заданной плоскости φ, и на плоскости имеем заданную точку $a(x_i,y_i)$. Также имеем сферу Римана радиусом R с выколотой верхней вершиной. Проведем некоторую прямую через эту выколотую вершину сферы $b(0,0,2R)$ и точку на плоскости. Имеем пересечение прямой со сферой в двух местах – в самой выколотой точке и в некоторой иной точке $\alpha(x,y,z)$ сферы. Поиск данной точки сводится из аналитической геометрии к решению системы:

$$\begin{cases} x^2+y^2+(z-R)^2=R^2, \\ \dfrac{x-x_i}{0-x_i}=\dfrac{y-y_i}{0-y_i}=\dfrac{z-0}{2R-0}. \end{cases} \qquad (2)$$

На самом деле, здесь присутствуют 4 уравнения, но нам нужны будут только 3 из них, причем решение $(x=0,y=0,z=2R)$ не удовлетворяет по условию. Второе решение имеет вид

$$x=\frac{4x_iR^2}{4R^2+y_i^2+x_i^2},\ \ y=\frac{4y_iR^2}{4R^2+y_i^2+x_i^2},\ \ z=2R-\frac{8R^3}{4R^2+y_i^2+x_i^2}\ .$$

Биективность данного отображения показана в [3].

При вычислении данных значений, вероятнее всего мы получим числа с плавающей точкой, соответственно, потери точности неизбежны и задача состоит в том, чтобы найти и исследовать параметры обратного преобразования для 100%-го возврата данных в первоначальное состояние, а также узнать и подобрать такие из них, чтобы невозможно было использовать переборные алгоритмы, работающие на перебор «в лоб».

Основная гипотеза состоит в том, что, варьируя бесконечно малые величины заданного порядка $\varepsilon>0$, действующие по неустойчивой схеме (т.е. небольшое изменение бесконечно малого влечет сильное искажение данных), невозможно будет использовать перебор всего отрезка действительных чисел, т.к. мощность любого бесконечно малого отрезка есть континуум.

Кроме того, добавление четвертого параметра к каждой тройке, а для определенности предположим, что это будет масса точки, можно определить некоторую механическую систему материальных точек, что при некоторых допущениях дает нам аппарат теоретической механики, изученный и разработанный столетиями.

Теперь попробуем произвести некоторый первичный анализ, исходя из полученных формул биективного отображения на сферу.

Каждая точка в пространстве получается некоторым отношением произведения координаты на радиус с суммой квадратов координат и учетверенного квадрата радиуса. Чтобы получить и произвести оценки погрешностей, рассмотрим различные случаи представления этих отношений. Для упрощения размышлений положим, что мы рассматриваем некоторое соотношение $\frac{x}{y}$, где $x>0, y>0$, т.к. полученные выводы можно легко расширить и для формул второго решения.

Логично, что при делении одного числа на другое мы можем получить ответ лишь с некоторой долей точности. Вспомним, что из теории погрешностей [1], зная относительную погрешность числа, можно восстановить некоторое количество значащих цифр. Очевидно, что для 100%-го восстановления информации нам необходимо определить, сколько в том или ином случае взять цифр, чтобы обратное преобразование дало ожидаемый результат.

Для соотношения $\frac{x}{y}$ основные варианты использования можно разделить на следующие группы:

$\frac{x}{y}=z_{\approx}+\sigma_z z_{\approx}$, где $z_{\approx}$ – приближенный результат дроби; σ_z – относительная погрешность результата дроби; $x\in N, y\in N$.

$\frac{x}{y}=z_{\approx}+\sigma_z z_{\approx}$, где $z_{\approx}$ – приближенный результат дроби; σ_z – относительная погрешность результата дроби; $x\in Q, y\in N, x>0$.

$\frac{x}{y}=z_{\approx}+\sigma_z z_{\approx}$, где $z_{\approx}$ – приближенный результат дроби; σ_z – относительная погрешность результата дроби; $x\in N, y\in Q, y>0$.

$\frac{x}{y}=z_{\approx}+\sigma_z z_{\approx}$, где $z_{\approx}$ – приближенный результат дроби; σ_z – относительная погрешность результата дроби; $x\in Q, y\in Q, x>0, y>0$.

Остальные расширения множества возможных чисел пока не рассматриваем.

Рассмотрим самый простой первый случай, когда числитель и знаменатель являются числами натуральными, тогда очевидно, что $x_i\in N, y_i\in N, R\in N$. Раз числа натуральные, значит, операция выполняется на числах без погрешностей. Но результат деления может оказаться как конечной десятичной дробью, так и бесконечной периодической.

Отсюда встает вопрос, с какой точностью передать значение другому объекту, чтобы:

− была возможность однозначно вернуть данные в начальный вид;

− осложнить процесс взлома.

Гипотетически точность, с которой нужно передавать число, можно определить по количеству значимых цифр. Но для данных рассуждений нам потребуется знать, сколько будет цифр в результате операции, если известно начальное количество знаков в каждом из операндов. Определить для операции сложения количество знаков не составляет труда. Поэтому рассмотрим операцию умножения. Для этого сформулируем и докажем теорему.

Теорема 1. Пусть x и y – целые, причем x состоит из $n>0$ цифр, а y состоит из $m>0$ цифр. Тогда $z=xy$ не превышает $m+n$ цифр. Числа x и y представлены в десятичной системе.

Доказательство в [6].

Из результатов оперирования числами с погрешностями [1] можно увидеть, что для восстановления достаточно взять значащие цифры и стандартными операциями округления привести значение к точному результату.

Но вопрос состоит еще в том, что операция восстановления, по логике вещей, должна будет производиться уже после передачи некоторых данных, т.е. во время расшифровки, а сколько в этом потоке необходимо передать цифр, чтобы восстановление всегда происходило успешно, – это вопрос. Теория погрешностей [1] говорит о минимуме значащих цифр. Но исходя из теоремы 1, очевидно, нет смысла брать более чем $n+m+1$.

По поводу осложнения процесса взлома можно использовать следующую простую схему. Представим, что данные в потоке передаются числами с плавающей точкой. Причем за 1 такт мы получаем лишь 1 цифру. В каком месте разделение разряда в числе – в потоке данных данная информация отсутствует. Отсюда получается, что для обратных преобразований, требующих достаточной точности числа, неизвестно, в каком месте числа поставить запятую (это особенно важно, когда небольшая погрешность в исходном значении дает сильное отклонение результата). Эту информацию можно представлять дополнительным ключом (назовем его степенным ключом), который и определяет, в каком месте необходимо поставить знак (варьирует запятую). Без необходимых данных о положении запятой сложность самого алгоритма перебора возрастет в число различных положений запятой. В случае когда информация о положении запятой известна, сложность остается прежней. Действительно, пусть сложность некоторого алгоритма шиф-

рования равна q. Дополняя свою схему отображением на сферу Римана переходом чисел к плавающей запятой, можно увеличить сложность решения задачи обратимости алгоритма в k раз, где k – возможные различные положения запятой. То есть по основной теореме умножения комбинаторики мы имеем максимально возможную сложность алгоритма kq, что и требовалось показать.

Из сказанного можно сделать следующие выводы:

1. Введение чисел с плавающей точкой дает возможность биективно, т.е. взаимно-однозначно перевести информацию в иную исследованную плоскость – плоскость теоретической механики, что открывает для использования огромный математический аппарат.

2. Показано, что отображение на сферу Римана точки зачастую дает рациональное значение.

3. Приведен базовый анализ, необходимый для работы криптографического алгоритма в условиях использования отображения на сферу Римана, а также возможность использования идеи о варьировании запятой в случае использования плавающей точки.

ЛИТЕРАТУРА

1. Демидович Б.П., Марон И.А., Шувалова Э.З. Численные методы анализа. Приближение функций, дифференциальные и интегральные уравнения. 3-е изд. М.: Наука, 1967. 368 с.

2. Новиков Ф.А. Дискретная математика для программистов. 2-е изд. СПб.: Питер, 2006. 364 с.

3. Свешников А.Г., Тихонов А.Н. Теория функций комплексной переменной. 5-е изд. М.: ФИЗМАТЛИТ, 2004. 336 с.

4. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.

5. Введение в криптографию / Под общ. ред. В.В. Ященко. М.: МЦНМО, ЧеРо, 1998. 271 с.

6. Воробьев А.А. О проблеме взлома перебором и потенциальных решениях с помощью чисел с плавающей точкой. Ч. 2 [Электронный ресурс]. Домашняя страница. Режим доступа: zeromem.narod.ru.

ВОЗМОЖНЫЕ КАНАЛЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О НАРУШЕНИЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.С. Яценко, студент 4-го курса

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

В наше время информационных технологий накоплено огромное количество различной информации. Большая часть является общедос-

тупной, но вот другая её часть принадлежит отдельным лицам, структурам, организациям или государствам. Речь идет о конфиденциальной информации, т.е. об информации, оглашение которой может принести её владельцам или хранителям финансовые или иные потери.

Поскольку данная информация является уникальной в своем роде, то желающих ею завладеть всегда немало. А значит, может случиться ситуация, что владелец или хранитель конфиденциальной информации может стать не единственным её обладателем или вовсе с ней распрощаться и понести потери. Для возмещения потерь владелец или хранитель конфиденциальной информации на основании Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации, но только в том случае, если владелец сможет доказать, что он принимал меры для соблюдения конфиденциальности и защиты тайны в соответствии с законодательством Российской Федерации и рекомендациями контролирующих органов. Следовательно, для того, чтобы иметь возможность обратиться за помощью в суд, исходя из данного закона, следует, что нужно фиксировать работу своей системы защиты информации.

Проанализировав данный вопрос, можно выделить программное обеспечение нескольких типов, используемых для реализации системы обеспечения информационной безопасности, в дальнейшем именуемые каналами получения информации о нарушениях информационной безопасности.

Одним из первых каналов, который можно использовать, – это антивирусы, установленные на серверах и локальных машинах сети. А поскольку в современных условиях редко можно встретить компьютер, на котором нет антивируса, то данный канал очень актуален. При своевременном обновлении сигнатур данный канал может дать довольно весомую часть интересующей нас информации. Примером могут служить антивирусы, сертифицированные ФСТЭКом РФ, такие как Doctor Web, Касперский и т.д.

Еще одним из актуальных каналов для операционных систем семейства Windows являются политики безопасности, а точнее журналы, которые используются при аудите во время действия политик безопасности. Поскольку посредством политик безопасности можно ограничить большое количество различных действий, то и журналы аудита будут содержать немало интересующей нас информации.

Актуальной также является информация, которую могут выдавать межсетевые экраны, установленные как на локальных машинах, так и

на серверах сети. В число сертифицированных ФСТЭКом входят: Cisco PIX Firewall, «Межсетевой экран Акер 3.10» и др.

Также для получения информации можно использовать программы, предназначенные для анализа сетевого трафика, т.е. снифферы. Например, WinDump, Kismet и т.д.

Еще один из актуальных каналов получения информации – это программы, производящие логирование действий пользователя и системы. Примером могут служить KGB Spy, Log4net и др.

Данные каналы были предложены не только из-за того, что они наиболее используемые, но и потому, что программы, которые реализуют данные каналы получения информации, ведут лог событий или по крайней мере предоставляют такую возможность, что существенно облегчает задачу. Но все же остается проблема сбора и хранения данных из вышеперечисленных каналов, т.к. непонятно, как именно её хранить и с какой частотой её собирать.

Для автоматизации данного процесса и решения проблем сбора и хранения информации видна необходимость в разработке многомодульной программной системы, решающей выше обозначенные задачи.

Данная система будет представлять собой клиент-серверное приложение.

Серверный вариант системы предполагает наличие модуля, принимающего данные из сети, базы данных для хранения данных, администраторское приложение для обзора записей и управления системой.

Клиентский вариант системы может содержать различные модули в зависимости от программного обеспечения, установленного на конкретном локальном компьютере, а именно различные модули, которые позволяют парсить файлы логов программ, представляющих собой каналы получения информации о нарушениях политики безопасности и атаках и модуль отправки данных по сети.

Таким образом, в будущем данная система позволит отслеживать работу системы защиты и поддерживать её в актуальном режиме, предоставлять лог работы системы в целом, в соответствующих случаях выявить слабые стороны системы защиты, позволит собрать статистический материал для построения новых моделей нарушителя.

Научный руководитель – Н.А. Новгородова, старший преподаватель каф. КИБЭВС ТУСУР.

ЛИТЕРАТУРА

1. Мещеряков Р.В. Основы информационной безопасности: Метод. указания. Томск: ТУСУР, 2001. 75 с.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

3. Государственный реестр сертифицированных средств защиты информации.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ*

В.С. Забавский, студент 4-го курса
г. Томск, ТУСУР, каф. КИБЭВС, tsk_tsr@sibmail.com

На кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) в рамках проекта ГПО № 0842 – Инженерия баз данных ведется разработка автоматизированной системы учета успеваемости студентов. Так как данная система предполагается не только как учебный проект, но и планируется ее дальнейшее внедрение и использование, то встал вопрос о необходимости проведения организационно-правовых мер. Так как данная система содержит персональные данные о студентах, не относящиеся к общедоступным данным, согласно Федеральному закону «О персональных данных» должна быть проведена классификация данной системы для определения необходимой степени защиты и на основании чего проведен комплекс организационных и технических мероприятий.

Согласно Федеральному закону «О персональных данных» персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

На основании «Порядка проведения классификации информационных систем персональных данных» была проведена классификация данной информационной системы.

Также были затронуты вопросы безопасности и составлен примерный минимальный список требований и мероприятий, которые необходимо провести при обработке персональных данных:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

* Работа выполнена в рамках проекта ГПО КИБЭВС-0842 – Инженерия баз данных.

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Мероприятия по обеспечению безопасности персональных данных:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

Заключительным этапом для внедрения данной системы с точки зрения организационно-правовых мер является разработка пакета документов, регламентирующих обработку персональных данных в информационных системах.

Научный руководитель – Н.А. Новгородова, старший преподаватель каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 27.12.2009) «О персональных данных» (принят ГД ФС РФ 08.07.2006).

2. Постановление Правительства РФ от 17.11.2007 N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Приказ ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

АНАЛИЗ И ОБРАБОТКА ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННЫХ БИБЛИОТЕЧНЫХ СИСТЕМ*

Н.Л. Загайнова, Н.О. Симанова, студентки 3-го курса, каф. РЗИ;
Д.П. Сапрыкина, студентка 3-го курса, каф. ТОР
г. Томск, ТУСУР, zagainova-n_1a7@sibmail.com

Библиотеки в своей деятельности используют автоматизированную библиотечную систему. Электронный каталог такой системы представляет собой общую поливидовую базу данных по многоотраслевой тематике. Она включает в себя сведения обо всей литературе, поступающей в библиотеку, – печатных и рукописных языковых материалах, нотах, видео- и звукозаписях, компьютерных файлах.

Электронный каталог такой системы может быть разбит на ряд отдельных баз данных, например по типу и виду литературы, тематике, виду описания, в хронологическом порядке или по любому другому принципу.

За основу формата представления данных в базах данных принят Международный коммуникативный формат UNIMARC — в части компоновки библиографических данных по полям и подполям и кодирования информации.

Язык форматирования (язык манипулирования данными) представляет собой средство, с помощью которого осуществляется разнообразное представление данных для многих операций и режимов системы, в частности для показа и печати документов, для создания словарей, для импорта/экспорта данных, для формально-логического контроля и т.д.

Язык форматирования включает в себя набор команд и функций. Совокупность команд и функций, записанных в соответствии с требованиями данного языка, называется форматом. В общем случае формат определяет некоторое подмножество данных из записи базы данных, которые затем могут использоваться системой для выполнения определенных функций.

Обрабатывая формат, система работает с тремя объектами: запись базы данных, собственно формат и рабочая область, в которой размещаются выходные данные. Команды выполняются последовательно в порядке их представления в формате. Одни из команд порождают выходные данные (например, значения полей данных), другие – инициируют некоторые действия (например, переход на другую строку, создание нескольких пустых строк и т.д.). Создаваемые данные запоминают-

* Выполнено в рамках проекта ГПО РЗИ-0906 – Анализ и безопасность данных пользователей автоматизированных библиотечных систем.

ся в рабочей области в виде текстовых строк, которые затем передаются для последующей обработки, например, для печати [1].

В автоматизированных библиотечных системах также ведется база данных читателей, которая содержит основные сведения о пользователях библиотек и взятых документах.

Из года в год в библиотеке изменяется состав читателей. Кто-то вырастает и их перестают удовлетворять эти ресурсы, кто-то вступает в тот возраст, когда необходимы ресурсы библиотеки. Чтобы фонд библиотеки был востребован современными читателями, необходимы его постоянные изменения. Для этого нужно знать текущее состояние состава читателей и изменение этого состава из года в год.

Таким образом, была поставлена задача анализа клиентской базы, в том числе изменений состава пользователей, для дальнейшего формирования библиотечного фонда и определения портрета среднестатистического должника библиотеки.

Решение указанной задачи состоит из следующих этапов:

1) изучение структуры автоматизированной библиотечной системы;

2) изучение языка запросов CDS/ISIS и формирования отчетов автоматизированной библиотечной системы;

3) исследование базы данных пользователей для разных библиотек и работающих в них точек обслуживания за последние два года по следующим категориям: пол, занятость, образование, возраст.

Особенность регистрации читателя заключается в том, что читатель регистрируется не во всех отделах (точках обслуживания библиотеки) одновременно, а в конкретном отделе в зависимости от его запроса. Поэтому один и тот же читатель может быть зарегистрирован в нескольких точках обслуживания библиотеки. Ежегодно читатели проходят перерегистрацию.

Исходными для анализа базами являются: база данных читателей библиотеки, её объём составляет 106000 пользователей; база данных должников; объём которой – 4996 пользователей.

Каждый статистический последовательный запрос для базы данных читателей обрабатывается 3–4 мин, а для решения поставленной задачи необходимо произвести 56 последовательных запросов.

Построение выражения последовательного запроса осложнялось тем, что период годового отсчета для перерегистрации читателя в библиотеке не с 1 января по 31 декабря, а с 1 декабря по 30 ноября следующего года. Каждый год читателей перерегистрируют.

Был проведен отбор данных и сформированы таблицы результатов запросов: «Изменения количественного состава читателей по категориям за 2008–2009 годы» и «База данных должников».

Предварительный анализ данных показал, что состав читателей за последние годы изменился. Например, в одной из библиотек процент мужчин уменьшился на 4. Число студентов уменьшилось на 20.

Анализ сведений о должниках показал, что среднестатистическими должниками являются ученики средней школы, преимущественно мальчики.

Изменения состава читателей позволяют выработать требования к изменению комплектования библиотек литературой, электронными, аудио- и видеодокументами.

Научный руководитель – А.С. Карауш, к.т.н., директор МИБС.

ЛИТЕРАТУРА

1. Система автоматизации библиотек ИРБИС. Общее описание системы. М.: ГПНТБ России, 2002. 260 с.

ИСПОЛЬЗОВАНИЕ ОДНОВРЕМЕННОЙ МАСКИРОВКИ ДЛЯ СЕГМЕНТАЦИИ РЕЧЕВОГО СИГНАЛА

С.В. Жевуров, студент 5-го курса

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

В речевых технологиях существует несколько направлений, напрямую связанных с информационной безопасностью (идентификация диктора и др.). Одним из основополагающих моментов в идентификации диктора по голосу и выделении ключевых слов в слитной речи является предварительная обработка речевых сигналов. К предварительной обработке относятся: фильтрация сигнала, его первичная сегментация и классификация.

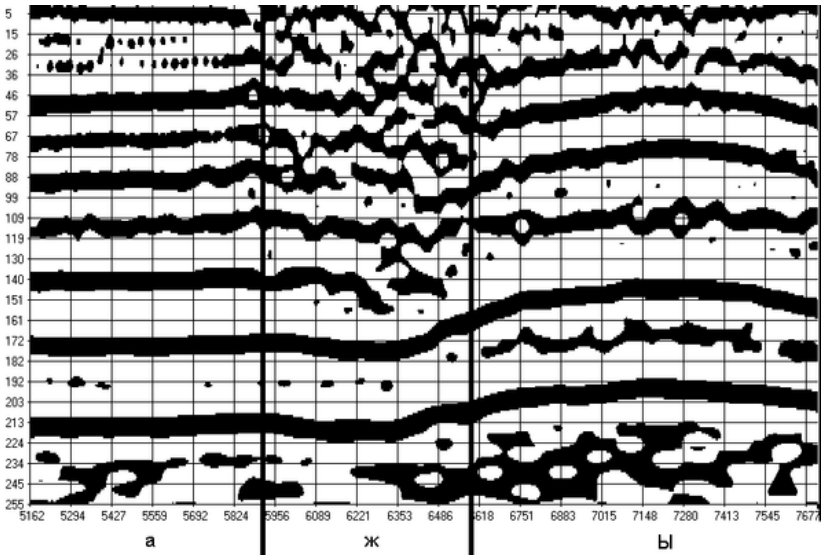
В теории речеобразования рассматриваются два типа источников речевого сигнала – голосовой и шумовой [1]. Голосовой источник генерирует квазипериодический сигнал, характеризующийся наличием гармонической структуры. В сигнале, генерируемом шумовым источником, гармоническая структура отсутствует либо является слабовыраженной.

Кроме сигналов, генерируемых только голосовым или только шумовым источником, речеобразующая система человека способна генерировать сигналы, в образовании которых могут участвовать одновременно оба типа источника.

В фонетике существует классификация звуков речи, учитывающая тип источника, сгенерировавшего звук [2]. В этой классификации к звукам, образованным с использованием только голосового источника,

относятся сонорные, с использованием только шумового – глухие согласные, с использованием обоих источников – звонкие согласные.

Используемая в исследованиях система фильтров основана на модели периферической части слуховой системы человека [3]. В данной модели учитывается эффект одновременной маскировки. После одновременной маскировки сигнал имеет структуру, представленную на рисунке. Подобная структура позволяет проводить автоматическую сегментацию сигнала на вокализованные (сонорные и звонкие согласные) и невокализованные (глухие согласные и паузы) участки.



Структура речевого сигнала после одновременной маскировки

Данная структура представляет собой набор бинарных данных. По оси абсцисс – время в дискретных отсчетах (частота дискретизации – 8 кГц), по оси ординат – номера частотных каналов фильтрации (0 канал – 2500 Гц, 255 – 50 Гц). Черным цветом выделены компоненты, которые представлены значением на частотном канале, равным единице. Эти компоненты воспринимаются слуховой системой человека. Белым цветом выделены компоненты, невоспринимаемые слуховой системой, которые представлены значением на частотном канале, равным нолю. На сегменте, соответствующем звуку «а», четко просматривается «полосатая» гармоническая структура сигнала. В «полосу» входят сама гармоника и прилегающие к ней незамаскированные частотные компоненты. Таким образом, «полоса» – непрерывный интервал единиц на одном временном отсчете.

Основной задачей работы является формирование статистики структуры речевого сигнала на участках звуков различных классов. Данная статистика необходима для выработки требований к алгоритму сегментации вокализованных участков сигнала на сонорные и звонкие согласные.

Научный руководитель – А.А. Конев, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Сапожков М.А. Речевой сигнал в кибернетике и связи. М.: Государственное издательство литературы по вопросам связи и радио, 1963. 450 с.

2. Буланин Л.Л. Фонетика современного русского языка. М.: Высшая школа, 1970.

3. Bondarenko V.P., Moor V.R., Chabanets A.N. The analysis of speech perception mechanisms on the models of auditory system // Proceedings XIth ICPhS. Tallinn, 1987. Vol. 2. P. 77–80.

ТЕСТИРОВАНИЕ МОДУЛЯ ШИФРОВАНИЯ В HASP

А.Е. Золотарёв, студент 5-го курса;
Ю.М. Филимонов, науч. рук., к.ф.-м.н., доцент
г. Томск, ТУСУР, каф. КИБЭВС, sever111@sibmail.com

Многие производители ключей внедряют возможность аппаратного шифрования/дешифрования в свои ключи. Многие современные шифры практически невозможно взломать методом грубой силы, а значит, программа будет надежно защищена при условии того, что шифр не будет взломан.

Как известно, существует множество бесплатных библиотек, реализующих различные алгоритмы шифрования, поэтому шифрование для нужд программы стоит производить посредством таких библиотек, а не с помощью ключа. Встроенный в ключ алгоритм шифрования нужен для того, чтобы защитить память ключа: как произовольные данные, записанные разработчиком в EEPROM, так и дескрипторы аппаратных функций.

У производителей по-разному реализовано получение ключа (пароля) для шифра. Если он будет зашит в тело программы, то методом reverse ingeneering не составит труда злоумышленнику заполучить его, пусть даже он будет зашифрован или замаскирован. Поэтому разумно получать ключ шифра из выхода хэш-функции: пропуская некоторые данные через аппаратную функцию, выход этой аппаратной функции будет ключом шифра. Такой метод более устойчив ко взлому.

Например, ключ HASP HL от Aladdin Software Security умеет шифровать и дешифровать данные по алгоритму AES, который выбран американским стандартом шифрования.

Аппаратная часть реализована в виде компактного USB-ключа (всего 38 мм). Аппаратно реализован публичный симметричный алгоритм шифрования AES/128 бит – для шифрования блоков кода защищаемых программ и данных. Ключи шифрования хранятся в защищенной памяти HASP HL и никогда не «выходят наружу».

До этого большинство аппаратных средств защиты использовали так называемые «секретные» алгоритмы, взлом которых приводил к появлению эмуляторов. Использование публичного алгоритма с известной стойкостью кардинально усложняет задачу взлома, клонирования или эмуляции.

Защищенная память объемом до 4096 байт может хранить параметры и настройки защищенных программ, режимы лицензирования и т.п. Эти данные могут быть зашифрованы с помощью AES/128, что обеспечивает их неизменность.

Стандарт FIPS 140-2 предусмотривает следующие требования безопасности для криптографических модулей.

Криптографический модуль должен выполнять самотестирование при включении питания, при выполнении некоторых условий (когда вызывается функция безопасности, для которой предусмотрено тестирование), а также по требованию оператора.

Необходимо, чтобы тесты покрывали все функции модуля (зашифрование, расшифрование, аутентификацию и т.д.). Для определения правильности прохождения тестов может применяться как сравнение с заранее известными, эталонными результатами, так и анализ согласованности результатов двух независимых реализаций одной и той же функции.

Специфицированы следующие виды проверок:

- тесты криптографических алгоритмов;
- тесты функций, критичных для безопасности модуля.

В число проверок, выполняемых по условию, входят:

- проверка взаимной согласованности парных ключей;
- контроль загружаемых программ;
- контроль ключей, вводимых вручную;
- тест генератора случайных чисел;
- тест режима обхода.

Меры доверия проектированию, заданные стандартом, распространяются на конфигурационное управление, процедуры безопасной установки, генерации и распространения, процесс разработки и документацию.

Известные криптографы, такие как Бенни Пинкас, Лео Дерондорф, подвергают сомнению криптостойкость современных программных средств криптографии, в связи с чем и будет проведено тестирование модуля шифрования HASP, чтобы удостовериться в его качестве.

Тестирование выглядит следующим образом. На вход модуля шифрования HASP подаётся текстовый файл, в котором может быть как обычный текст, так и сгенерированный при помощи программы определённым образом набор символов, в котором учитывается частота встречаемости символов, как в обычном тексте. Далее на вход тестирующей программы (алгоритм проверки взят из FIPS) подаётся зашифрованный файл, в котором проверяется последовательность бит на частоту встречаемости символов из исходного текста в полученном зашифрованном файле. Также проверяется равномерное распределение бит в зашифрованном файле.

ЛИТЕРАТУРА

1. FIPS 140-1. Security requirements for cryptographic modules.

2. HASP HL – краткое описание [Электронный ресурс]. Режим доступа: http://www.aladdin.kz/168.html.

3. Zvi Gutterman, Benny Pinkas. Cryptanalysis of the Random Number Generator of the Windows Operating System. 2007. 24 с.

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ЗАВИСИМОСТИ КРИПТОСТОЙКОСТИ ШИФРОВАНИЯ ПО АЛГОРИТМУ ГОСТ 28147–89 ОТ ВЫБРАННОЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ

В.Ю. Золотухин, студент 4-го курса, каф. БИТ;
Т.А. Чалкин, аспирант каф. МБ;
О.Н. Жданов, науч. рук., к.ф.-м.н., доцент каф. безопасности информационных технологий
г. Красноярск, СибГАУ им. академика М.Ф. Решетнева,
booroo@rambler.ru

В настоящей работе рассматривается подход к оценке зависимости криптостойкости шифрования по алгоритму ГОСТ 28147–89 от выбранных элементов ключевой информации – ключа и таблицы замен, использующий представление преобразований бит в рамках процедуры шифрования как наборов булевых функций. Разработанная методика позволит выбирать элементы ключевой информации, обеспечивающие устойчивость шифрования к наиболее распространенным методам криптоанализа, для использования в криптографических системах защиты несекретной информации.

Каждая операция преобразования n бит в рамках процедуры шифрования может быть представлена в виде набора из n булевых функций от n переменных. Результат зашифрования открытого текста задается композицией наборов булевых функций. Анализируя характеристики этих функций, можно судить об особенностях процесса шифрования при данных конкретных значениях ключевой информации, так как вид функций будет меняться в зависимости от ключа (и таблицы замен – в случае шифра ГОСТ 28147–89).

На сегодняшний день наиболее эффективными и хорошо изученными методами криптоанализа являются линейный и дифференциальный криптоанализ. Для достижения высокого уровня стойкости шифра к линейному и дифференциальному криптоанализу необходимо, чтобы булевы функции, составляющие преобразование бит, соответствующее процедуре шифрования, обладали высокими показателями нелинейности (то есть были далеки в смысле расстояния Хэмминга от множества аффинных булевых функций) и лавинного эффекта (для любого изменения значений входных переменных функции выходное значение должно меняться с вероятностью 1/2, причем «непредсказуемым» образом, если рассматривать функцию как «черный ящик»). Количественными характеристиками, отражающими устойчивость шифрования к линейному и дифференциальному методам криптоанализа, являются нелинейность и динамическое расстояние [1].

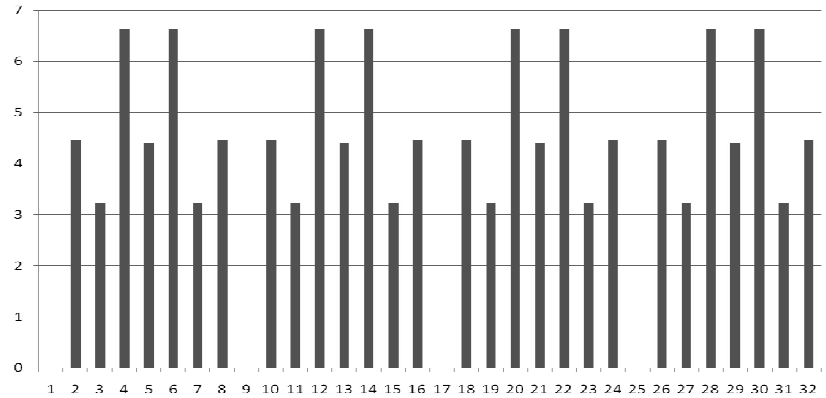
При рассмотрении раунда шифрования алгоритма ГОСТ 28147–89 очевидно, что нелинейность и лавинный эффект в процессе шифрования обеспечиваются операциями сложения полублока данных с подключом раунда и замены бит по таблице, поскольку операции циклического сдвига и побитового сложения с левым полублоком являются линейными и не несут лавинного эффекта.

В работе [2] описан алгоритм построения узлов замен алгоритма ГОСТ 28147–89, отвечающих требованиям устойчивости к линейному и дифференциальному криптоанализу, определяемой по значениям количественных характеристик нелинейности и динамического расстояния для отдельных узлов.

Так как нелинейность преобразования бит в раунде ГОСТ 28147–89 обеспечивается еще и операцией сложения с подключом раунда, то возникает задача оценки влияния используемого подключа на нелинейность раунда в целом. Для этого необходимо определить зависимость нелинейность операции сложения n-битного блока данных с числом из диапазона $[0\ldots2^n–1]$ по модулю 2^n от значения этого числа.

В случае ГОСТ 28147–89 $n = 32$. Однако вычисление нелинейности булевой функции столь большой разрядности – сложная вычислительная задача, поэтому на текущий момент исследования ведутся для

небольших значений n. На рисунке в виде гистограммы представлена зависимость нелинейности такой операции сложения при $n = 5$. При этом, вопреки классическому подходу, в данном случае нелинейность набора функций в целом определяется не как минимум нелинейностей функций из него и их линейных композиций (так как в этом случае всегда будет результат, равный 0), а как их среднее арифметическое.



Гистограмма значений нелинейности операции сложения по модулю 2^n при $n = 5$

Если анализировать раунд шифрования в целом, то еще одним важным для изучения вопросом является оценка взаимного влияния операций сложения полублока данных с подключом и замены бит по таблице. Поскольку в раунде эту пару преобразований можно представить одним преобразованием, являющимся их композицией, то задача стоит в определении соотношения между нелинейностью композиции преобразований бит и нелинейностью каждого из них в отдельности.

По причине, описанной выше, исследование данного вопроса было начато для небольших значений разрядности преобразований. Возможные соотношения нелинейностей операций сложения с подключом и замены бит по таблице, с нелинейностью их композиции, при длине полублока, равной 3, представлены в таблице. В данном случае нелинейность блока понимается в классическом смысле (как минимум нелинейностей функций и их композиций).

Возможные соотношения нелинейностей операций сложения с подключом (S1), замены бит (S2) и их композиции (S1○S2), при $n = 3$

NL(S1)	0	0	0	0
NL(S2)	0	0	2	2
NL(S1○S2)	0	1	0	1
Число	107520	129024	43008	43008

Таким образом, в зависимости от подключа нелинейность композиции преобразований может как увеличиваться, так и уменьшаться, что подтверждает практическую значимость исследования.

Таким образом, на текущий момент разработан программный комплекс исследования булевых функций и их наборов по значениям нелинейности и с его использованием получены эмпирические данные при малых значениях разрядности функций. Дальнейшее развитие исследований предполагает выявление и обоснование закономерностей, справедливых при больших значениях числа переменных.

ЛИТЕРАТУРА

1. Столлингс В. Криптография и защита сетей: принципы и практика. М.: Изд.дом «Вильямс», 2001. 672 с.

2. Чалкин Т.А., Волощук К.М. Алгоритм построения узлов замен алгоритма шифрования ГОСТ 28147–89 // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. Вып. 1 (22): В 2 ч. Ч. 2 / Под общ. ред. Г.П. Белякова; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2009. С. 46–50.

ТЕСТИРОВАНИЕ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ В RUTOKEN

А.Р. Звайгзне, студент 5-го курса

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

Генераторы случайных чисел (ГСЧ) – слабое место криптографических систем. Хорошие генераторы случайных чисел сложны в разработке, так как их надёжность часто зависит от особенностей аппаратного и программного обеспечения. Многие из программных продуктов используют плохие ГСЧ. Алгоритм шифрования может быть криптостойким, но если генератор случайных чисел выдаёт слабые ключи, то систему взломать гораздо проще. Другие продукты используют надёжные генераторы случайных чисел, но не используют достаточно случайности для обеспечения надёжной криптографии. Исследования показали, что генератор случайных чисел в операционной системе Windows 2000 дает неслучайную последовательность [1].

Для получения случайных чисел используются различные способы. В общем случае все методы генерирования случайных чисел можно разделить на аппаратные и программные. Устройства или алгоритмы получения случайных чисел называют генераторами случайных чисел (ГСЧ) или датчиками случайных чисел.

Аппаратные ГСЧ представляют собой устройства, преобразующие в цифровую форму какой-либо параметр окружающей среды или физического процесса. Параметр и процесс выбираются таким образом, что-

бы обеспечить хорошую «случайность» значений при считывании. Очень часто используются паразитные процессы в электронике (токи утечки, туннельный пробой диодов, цифровой шум видеокамеры, шумы на микрофонном входе звуковой карты и т.п.). Формируемая таким образом последовательность чисел, как правило, носит абсолютно случайный характер и не может быть воспроизведена заново по желанию пользователя.

К программным ГСЧ относятся различные алгоритмы генерирования последовательности чисел, которые по своим характеристикам напоминают случайную последовательность. Для формирования очередного числа последовательности используются различные алгебраические преобразования.

Любые программные ГСЧ, не использующие внешние «источники энтропии» и формирующие очередное число только алгебраическими преобразованиями, не дают чисто случайных чисел. Последовательность на выходе такого ГСЧ выглядит как случайная, но на самом деле подчиняется некоторому закону и, как правило, рано или поздно зацикливается. Такие числа называются псевдослучайными.

Последовательности случайных чисел, формируемых тем или иным ГСЧ, должны удовлетворять ряду требований. Во-первых, числа должны выбираться из определенного множества (чаще всего это действительные числа в интервале от 0 до 1 либо целые от 0 до N). Во-вторых, последовательность должна подчиняться определенному распределению на заданном множестве (чаще всего распределение равномерное). В-третьих, требование воспроизводимости последовательности. Если ГСЧ позволяет воспроизвести заново однажды сформированную последовательность, отладка программ с использованием такого ГСЧ значительно упрощается. Кроме того, требование воспроизводимости часто выдвигается при использовании ГСЧ в криптографии.

Поскольку псевдослучайные числа не являются действительно случайными, качество ГСЧ очень часто оценивается по «случайности» получаемых чисел. В эту оценку могут входить различные показатели, например: длина цикла (количество итераций, после которого ГСЧ зацикливается), взаимозависимости между соседними числами (могут выявляться с помощью различных методов теории вероятностей и математической статистики) и т.п.

Качество ГСЧ в значительной мере влияет на результаты работы программ, использующих случайные числа. Поэтому все применяемые генераторы случайных чисел должны пройти перед моделированием системы предварительное тестирование, которое представляет собой комплекс проверок по различным стохастическим критериям, включая в качестве основных тесты на равномерность, стохастичность и независимость (рассматриваются только ГСЧ с равномерным распределением).

Целью работы является тестирование генератора случайных чисел в изделии компании «Актив» Rutoken. Rutoken – это компактное устройство в виде USB-брелока, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных.

Для этого было написано программное обеспечение, с помощью которого было проведено тестирование ГСЧ Rutoken. В ходе тестирования были использованы тесты Diehard и FIPS.

Научный руководитель – Ю.М. Филимонов, к.ф.-м..н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Zvi Gutterman, Benny Pinkas. Cryptanalysis of the Random Number Generator of the Windows Operating System. 2007. 24 с.

2. FIPS 140-1. Security requirements for cryptographic modules.

3. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

КЛАССИФИКАЦИЯ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ С ТОЧКИ ЗРЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ МЕДИЦИНСКИХ ДАННЫХ

В.Д. Зыков, аспирант

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

В последние годы остро встал вопрос защиты персональных данных (ПДн) граждан, обрабатываемых в информационных системах персональных данных (ИСПДн). Этому способствует бурное развитие рынка самих ИСПДн, рост количества преступлений в сфере высоких технологий и требования законодательства [1].

Особое место среди систем этого класса занимают медицинские информационные системы (МИС), поскольку в них обрабатываются персональные медицинские данные (ПМДн) – сведения о состоянии здоровья граждан, которые относятся к врачебной тайне.

Для проведения классификации МИС на типы с точки зрения защиты ПМДн были определены общие для всех медицинских информационных систем свойства и критерии дальнейшей их классификации.

Руководствуясь порядком, утвержденным Приказом ФСТЭК РФ №55, ФСБ РФ №86, Мининформсвязи РФ №20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных» [2] и национальным стандартом Российской Федерации «Электронные истории болезни» [3], были определены

общие свойства для МИС и базовые критерии для дальнейшей их классификации.

Процесс классификации МИС по базовым критериям можно представить в виде ориентированного одностороннего графа $G(V,E)$, где $V=\{v_b,v_{1,1},v_{1,2}\ldots,v_{6,2},v_e\}$ – множество вершин графа G; E – множество дуг графа G-упорядоченных пар вершин $v\in V$ (рис. 1).

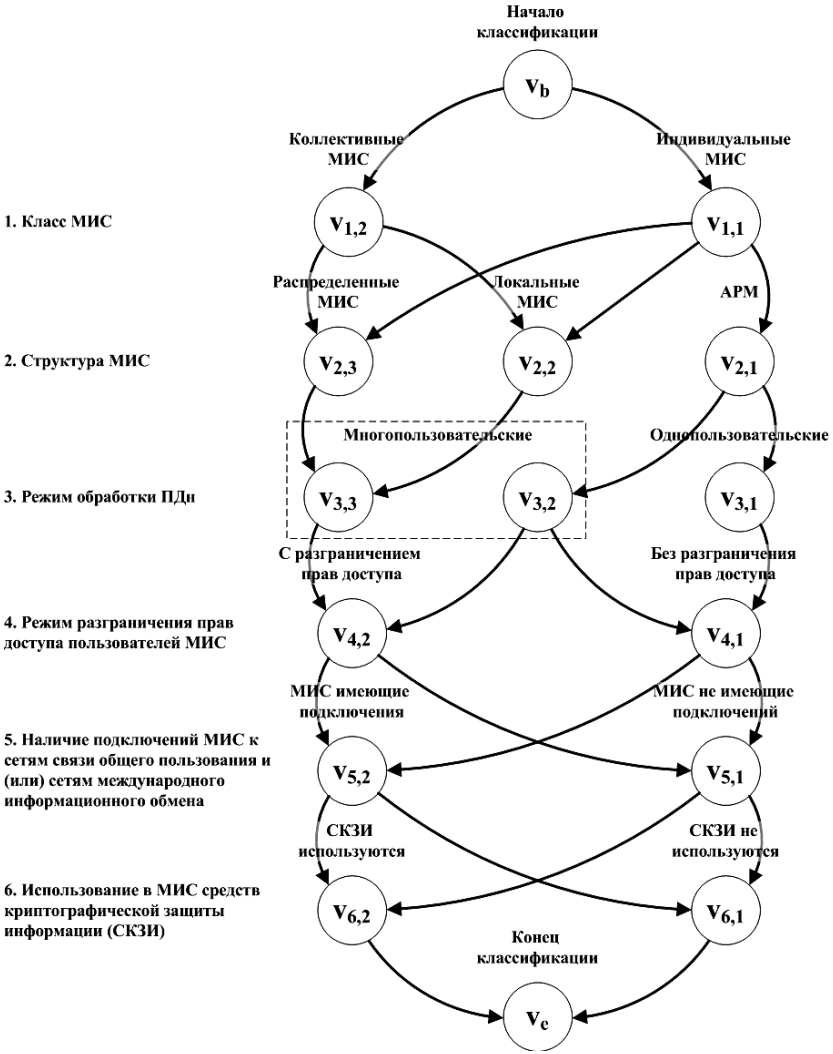


Рис. 1. Граф классификации МИС по базовым критериям

Как видно из рис. 1, свойства МИС критериев *1–4* имеют зависимости: коллективные МИС могут быть только локальными или распределенными, однопользовательские МИС не могут иметь разграничения прав доступа, а локальные и распределенные МИС могут быть только многопользовательскими с разграничением прав доступа.

Свойство МИС критериев *5* и *6* не имеют зависимостей и образует частные случаи МИС после классификации по критериям *1–4*. Таким образом, существует *7* базовых типов МИС:

1. Однопользовательское индивидуальное АРМ.
2. Многопользовательское индивидуальное АРМ без разграничения прав доступа.
3. Многопользовательское индивидуальное АРМ с разграничением прав доступа.
4. Многопользовательские индивидуальные локальные МИС с разграничением прав доступа.
5. Многопользовательские индивидуальные распределенные МИС с разграничением прав доступа.
6. Многопользовательские коллективные локальные МИС с разграничением прав доступа.
7. Многопользовательские коллективные распределенные МИС с разграничением прав доступа.

В 75 учреждениях системы здравоохранения Томской области имеется более 180 МИС, установленных на более чем 1000 рабочих местах. Количество типов МИС в Томской области представлено на рис. 2.

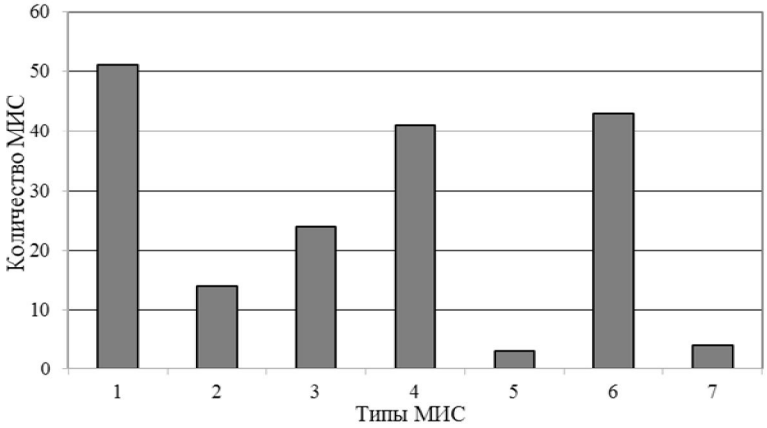


Рис. 2. Количество типов МИС в Томской области

ЛИТЕРАТУРА

1. Федеральный закон №152-ФЗ от 27.07.2006 г. «О персональных данных».

2. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

3. ГОСТ Р 52636–2006. Электронная история болезни. Общие положения. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии Российской Федерации от 27 декабря 2006 г. №407-ст.

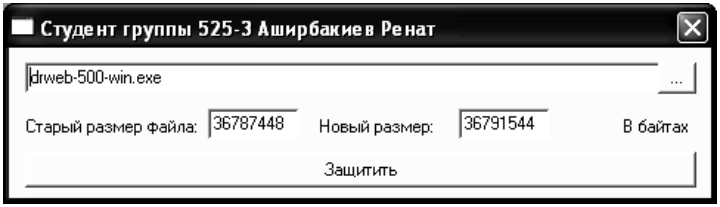
ЗАЩИТА СЕКЦИЙ КОДА В ФАЙЛАХ С PE-СТРУКТУРОЙ

Р.И. Аширбакиев, студент 5-го курса

г. Томск, ТУСУР, каф. КИБЭВС, renat.i.a7@gmail.com

В данной статье будет рассмотрена защита секции кода в файлах типа PE. Это необходимо для обеспечения защиты от взлома, исследования и декомпиляции программ. Класс программ, которые можно защищать моей программой, – коммерческое программное обеспечение.

Начнем реализацию с изучения структуры PE-файлов, после чего нужно приступить к реализации. Для этого в качестве языка программирования возьмем C++ от Microsoft'а, как средство, имеющее в своем составе уже созданные структуры для работы с PE-файлами, что позволяет более точно оперировать секциями, импортами, экспортами и другими частями структуры PE. Для защиты программы от взлома, во-первых, можно встроить различные антиотладочные фокусы, во-вторых, встроить запутывающий код или же иначе обфускацию, в-третьих, достаточно шифрования основной секции кода. Инновация состоит в том, что планируется сделать on-line версию продукта на Java + C++. Класс программ, которые можно защищать, используя программу: коммерческое ПО предназначенное для продажи, это могут быть игры и другие программы подлежащий продажи.



Защита секций кода

Для защиты программы достаточно нажать на кнопку обзор (на которой написано «…»), выбрать файл типа exe или dll и нажать кнопку «Защитить». Все готово: коммерческая программа drweb-500-win.exe защищена.

Научный руководитель – Е.М. Давыдова, к.т.н., доцент каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Научная сессия ТУСУР–2009: Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых. 12–15 мая 2009 г.: В 5 ч. Ч. 3. Системная интеграция и безопасность. Томск: В-Спектр, 2009. 392 с.

ПОДСИСТЕМА АВТОРИЗАЦИИ ДЛЯ ВИДЕОЧАТА

Ю.И. Конькова, студентка 5-го курса

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

Защита компьютерных систем от несанкционированного доступа (НСД) является одной из основных проблем защиты информации. Поэтому в большинство операционных систем и популярных пакетов программ встроены различные подсистемы защиты от НСД [1], например подсистема авторизации.

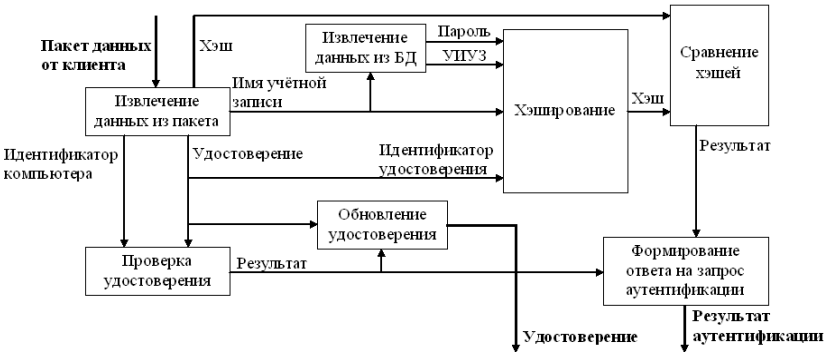
В данной статье речь пойдёт об авторизации в видеочате. Специфика программного обеспечения предполагает предоставление пользователю возможности сохранять аутентификационные данные на компьютере. В результате пользователь избавляется от необходимости вводить пароль вручную при каждом входе в систему, но возникает проблема кражи данных (паролей и серийных ключей) с компьютера пользователя. Таким образом, задача заключается в разработке подсистемы авторизации, позволяющей обнаружить попытки использования скопированных данных и выявить злоумышленника.

В ходе работы были проанализированы существующие механизмы аутентификации пользователя (многоразовые пароли, методы одноразовой аутентификации, протокол Kerberos, цифровые сертификаты) [2]. Был сделан вывод, что в разрабатываемой подсистеме должна применяться разновидность одноразовой аутентификации пользователя в сочетании с идентификацией компьютера.

В результате работы была спроектирована подсистема авторизации, основанная на удостоверениях пользователя. Удостоверение содержит идентификатор компьютера, счётчик входов в систему с данным удостоверением, серийный ключ (если пользователь прошёл про-

цедуру активации программы), номера учётных записей и IP-адреса, с которых осуществлялся вход в видеочат с данным удостоверением.

На рисунке показана упрощённая схема авторизации пользователя.



Упрощённая схема авторизации пользователя

Часть учётных записей и IP-адресов составляют контрольную группу – считается, что они гарантированно принадлежат законному пользователю. При расширении контрольной группы в неё включаются все учётные записи и IP-адреса, записанные в удостоверении. Для этого необходимо выполнение двух условий: ручной ввод пароля учётной записи, уже содержащейся в контрольной группе, и установленный пользователем флаг «Сохранить пароль». Выполнение второго условия означает уверенность пользователя в том, что данный компьютер не будет использован злоумышленником для входа в видеочат. В противном случае существовала бы возможность включения в контрольную группу учётной записи злоумышленника. Введение контрольной группы делает возможным выявление учётных записей и IP-адресов нарушителей.

Идентификатор компьютера вычисляется как функция от его параметров. В случае несовпадения вычисленного идентификатора с тем, что хранится в удостоверении, пользователю предлагается вручную ввести пароль учётной записи из контрольной группы. Если пользователь знает пароль, то информация в удостоверении обновляется.

Счётчик входов используется для обнаружения фактов авторизации с одинаковыми сертификатами (при удачном подделывании инсталляционного номера) с разных компьютеров. Ожидаемое значение счётчика хранится на сервере.

Удостоверение создаётся и проверяется на сервере и сохраняется на клиенте. После каждой проверки клиенту высылается обновлённое

удостоверение, которое заменяет старое. Удостоверение хранится в зашифрованном виде. Шифрование и расшифрование происходит на сервере с использованием уникального идентификатора учётной записи (УИУЗ), под которой было создано удостоверение.

Каждое удостоверение имеет уникальный идентификатор. Блок данных, включающий этот идентификатор, имя учётной записи, пароль и уникальный идентификатор учётной записи, хэшируется сервером. Хэш сохраняется на клиенте, если пользователь при аутентификации установил флаг «Сохранить пароль». Таким образом, хэш привязан к конкретному удостоверению и отдельно от него использоваться для аутентификации не может.

Разработанная система полностью удовлетворяет поставленной задаче. Дальнейшие исследования должны быть связаны с разработкой механизмов блокировки удостоверений, учётных записей и IP-адресов нарушителей.

Научный руководитель – А.А. Конев, к.т.н., доцент каф.КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004. 384 с.

2. Полянская О.Ю. Механизмы аутентификации [Электронный ресурс]: Инфраструктура открытых ключей. Режим доступа: http://www.intuit.ru/department/security/pki/2, свободный.

О ПРОБЛЕМАХ ЭФФЕКТИВНОЙ РЕАЛИЗАЦИИ ПАРАЛЛЕЛЬНОГО РО-МЕТОДА ПОЛЛАРДА

В.В. Перевощиков, А.А. Гриценко, студенты,
каф. компьютерной безопасности и прикладной алгебры
г. Калининград, РГУ им. И. Канта, roadrunner39@gmail.com

Данная работа посвящена проблемам разработки и реализации эффективного параллельного алгоритма дискретного логарифмирования в группе точек эллиптической кривой, основанного на ρ-методе Полларда, в модели вычислений SPMD. В основу разрабатываемого алгоритма заложены идеи параллельного поиска коллизии при случайных блужданиях, описанные в [1]. Авторы данной работы исследуют, при каком количестве центральных процессов и какой доле «особых» точек, на которых осуществляется этот поиск, ожидаемое время работы алгоритма будет оптимальным при ограничениях на доступную память.

Как было показано в [2], с помощью группового автоморфизма инверсии поиск коллизии может быть осуществлён на множестве мощности $0{,}5n$, где n – порядок данной подгруппы. Тогда, используя оценку ожидаемого время работы алгоритма, приведённую в [1], ожидаемое время работы составит

$$E[T]=\frac{\sqrt{\pi n}}{2m}+\frac{1}{\theta}, \qquad (1)$$

где m – количество генерирующих процессов; θ – доля особых точек.

Согласно [3] ожидаемое количество хранимых особых точек будет равно

$$E[S]=0{,}5\theta\sqrt{\pi n}+m. \qquad (2)$$

Пусть каждый центральный процесс может осуществлять хранение и обработку не более M точек; p – общее количество доступных процессов; x – количество центральных процессов; $A:=0{,}5\sqrt{\pi n}$, тогда, используя (1) и (2), получаем следующую задачу оптимизации:

$$\begin{aligned} &E[T](x,\theta)=\frac{A}{p-x}+\frac{1}{\theta}\to\min,\\ &0<A\theta\le x(M+1)-p,\\ &1\le x\le p-1. \end{aligned} \qquad (3)$$

Анализ данной задачи показывает, что если количество всех процессов меньше $\sqrt{M}$, то достаточно одного центрального процесса.

Оптимальное значение θ может быть найдено при выполнении равенства в правой части (3). Эффективность параллельного алгоритма равна примерно 99%.

Для реализации рассматриваемого алгоритма авторы рассматривали задачу дискретного логарифма на эллиптических кривых над полем $GF(2^n)$. С помощью языка программирования C++ и библиотек MPI (Message Passing Interface) был создан комплекс программ для решения поставленный задачи, эффективность работы которого была протестирована на суперкомпьютере РГУ им. Канта.

В результате авторам удалось решить задачу в группе порядка 2^{71} с использованием 100 процессов, на что потребовалось 50,2 ч, на каждом процессе было совершено $5{,}5\cdot10^5$ итераций. В предыдущей работе авторов [4] рассматривался вопрос об эффективной реализации непараллельного ρ-метода Полларда. Примерно за такое время удавалось решить задачу в группе порядка не более 53 бита.

В таблице представлены результаты тестирования комплекса программ в группе порядка 43 бита, осуществляемого на 48 процессах.

Зависимость среднего времени работы
и среднего количества требуемой памяти от θ

s	Кол-во итераций I	Кол-во памяти	Время T, с	I/T
2	$1{,}04\cdot10^5$	$1{,}45\cdot10^5$	8,76	$1{,}19\cdot10^4$
6	$3{,}94\cdot10^4$	$3{,}86\cdot10^4$	2,66	$1{,}48\cdot10^4$
10	$6{,}28\cdot10^4$	$3{,}95\cdot10^3$	0,85	$7{,}41\cdot10^4$
14	$5{,}43\cdot10^4$	$2{,}07\cdot10^2$	0,53	$1{,}02\cdot10^5$
18	$1{,}15\cdot10^5$	$2{,}73\cdot10^1$	1,1	$1{,}04\cdot10^5$
22	$1{,}84\cdot10^5$	2,67	1,72	$1{,}06\cdot10^5$
26	$5{,}72\cdot10^6$	2	52,8	$1{,}08\cdot10^5$

Для данной ситуации прогнозировалось, что оптимальным для ожидаемого времени работы было значение $s = 2$. Однако при таком большом значении параметра θ наблюдается как увеличение количества итераций, так и уменьшение производительности, связанное с необходимостью пересылок и обработки большого количества данных.

На рис. 1 представлена зависимость производительности алгоритма от количества отличительных бит s. На рис. 2 представлена зависимость времени работы программы от s. Видно, что при малых значениях параметра θ каждый из процессов способен генерировать почти максимальное количество точек, но максимуму производительности не соответствует оптимальное время работы программы.

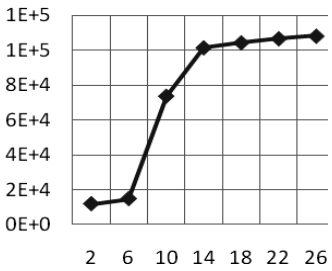


Рис. 1. Зависимость I/T от s

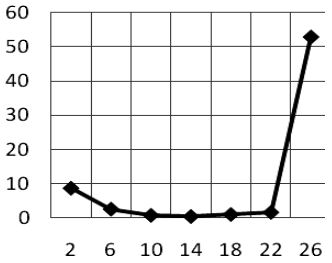


Рис. 2. Зависимость T от s

Данная работа может быть улучшена в направлении усложнения рассматриваемой модели. При расчёте ожидаемого времени работы программы стоит учитывать коммуникацию между процессами, чтобы рассчитывать оптимальную долю «особых точек». Как показали результаты экспериментов, большое количество генерированных точек отрицательно влияет на время работы программы. Также следует попытаться разработать более эффективный критерий проверки, является ли точка «особой», применимый к конкретной группе, в которой ищется решение задачи.

ЛИТЕРАТУРА

1. P. van Oorschot, Wiener M. Parallel collision search with cryptanalyticapplications // Journal of Cryptology. 1999. 12(1). January.

2. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. New-York, Inc.: Springer-Verlag. 2004.

3. Kuhn F. and Struik R. Random walks revisited: Extensions of Pollard's rho algorithm for computing multiple discrete logarithms // 8th Annual Workshop on Selected Areas in Cryprography (SAC), Toronto, Ontario, Canada, 2001.

4. Дональд Э. Кнут. Искусство программирования. Т. 3. Сортировка и поиск. 2-е изд. М.: Вильямс, 2008.

ПРОБЛЕМАТИКА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВУЗАХ

Н.А. Петрова, студентка 4-го курса;
М.А. Сопов, науч. рук., ассистент
г. Томск, ТУСУР, каф. КИБЭВС, pena_v3@mail.ru

В связи с принятием ФЗ №152 «О персональных данных» от 27.07.2006 возникло множество вопросов по выполнению его требований для системы высших учебных заведений. Речь идет об автоматизированной обработке персональных данных (ПДн) в информационных системах, т.к. технологии реализации требований безопасности ПДн вызывают больше всего вопросов.

Проанализировав закон, становится понятно, что вузы являются операторами ПДн и на них распространяется действие ФЗ №152. Значит возникает необходимость приведения информационных систем вуза в соответствие с требованиями закона и составления текста уведомления об обработке персональных данных, которое направляется государственному Регулятору, в Роскомнадзор. Необходимо отметить, что к моменту подготовки данного уведомления вуз уже должен точно определить, как фактически будет реализована система защиты в его ИСПДн.

Прежде всего необходимо определить, какие информационные системы ПДн (ИСПДн) есть и какого типа ПДн в них обрабатываются. Для этого проводится классификация ИСПДн. Она необходима для дальнейшего выбора методов и средств защиты ПДн, обрабатываемых в ИСПДн, поскольку в документах ФСТЭК и ФСБ каждому классу устанавливаются свои требования по защите ИСПДн. Система защиты персональных данных должна строиться только на основе сертифицированных ФСТЭК России и ФСБ России средствах защиты. Поэтому вуз обязан в установленном порядке получить лицензию ФСТЭК Рос-

сии на деятельность по технической защите конфиденциальной информации, а также иметь в своем штате сертифицированных специалистов по соответствующим техническим решениям, предназначенным для защиты персональных данных. Ясно, что это влечет за собой немалые денежные расходы.

Чтобы минимизировать затраты на реализацию мероприятий, регламентированных законодательством, необходимо провести ряд организационных и технических мероприятий, направленных на понижение класса ИСПДн. Достичь уменьшения класса можно двумя путями: понижением категории персональных данных и уменьшением количества записей ПДн. Если уменьшить количество записей достаточно сложно, то понижение категории вполне реально.

Одним из методов понижения категории ПДн является их обезличивание. Закон трактует обезличивание как «действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту». Однако методы, приводящие к такому состоянию, и то, какой набор считается достаточным для идентификации субъекта, в имеющихся на текущий момент документах не приводятся.

Существуют и другие методы.

Еще одним важным шагом является получение согласия субъекта персональных данных на обработку (закон тем самым предотвращает незаконный сбор и использование персональных данных).

Далее необходимо разработать положение, регламентирующее порядок хранения, обработки и защиты персональных данных.

Кроме того, необходимо оформить список лиц, допущенных к обработке ПДн, т.е. перечень тех (по должностям), кому доступ к ПДн необходим для выполнения служебных обязанностей. В первую очередь, это сотрудники кадровой службы, а также сотрудники бухгалтерии. Помимо того, доступ к этим сведениям могут получить руководители структурных подразделений. Однако все они вправе запрашивать не любые данные, а только те, которые необходимы для выполнения конкретных трудовых функций (например, чтобы рассчитать льготы по налогам, бухгалтерия получит не все сведения о работнике, а только данные о количестве его иждивенцев). Поэтому целесообразно прописать перечень информационных ресурсов, к которым пользователи допущены.

Мероприятия по защите информации трудоемки и могут привести к значительным финансовым затратам, что обусловлено необходимостью:

− получать (по необходимости) лицензию на деятельность по технической защите конфиденциальной информации ФСТЭК России;

− привлекать лицензиата ФСТЭК России для осуществления мероприятий по созданию системы защиты ИСПДн и/или ее аттестации по требованиям безопасности информации;

− отправлять сотрудников, ответственных за обеспечение безопасности информации, на курсы повышения квалификации по вопросам защиты информации и/или нанимать специалистов по защите информации;

− устанавливать сертифицированные по требованиям ФСТЭК средства защиты информации (СрЗИ), сертифицированные ФСБ средства криптографической защиты информации (СКЗИ) в зависимости от класса ИСПДн.

Конечно, надо иметь в виду, что при неисполнении требований по обеспечению безопасности ПДн оператор несет ответственность от дисциплинарной до уголовной.

ЛИТЕРАТУРА

1. ФЗ №152 «О персональных данных» от 27.07.2006 г.

2. Бурдаков М.В. Закон «О персональных данных» и вузы. М.: Статья, 2009. 12 с.

3. http://daily.sec.ru

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ЗАКОНА 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ» В БАНКОВСКОЙ СФЕРЕ

Д.А. Третьяков, студент 4-го курса;

М.А. Сопов, науч. рук., ассистент

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

Федеральный закон «О персональных данных» (ФЗ № 152 «О персональных данных») – является нормативно правовым актом, содержащим в себе основу нормативного регулирования обработки персональных данных. Он был принят 27 июля 2006 г. и вступил в законную силу 26 января 2007 г. Согласно изменениям, внесённым ФЗ-363 от 27.12.2009, операторы персональных данных должны привести свои системы обработки персональных данных, запущенные до 1 января 2010 г. в соответствие с законом до 1 января 2011 г. Основной причиной переноса, в пользу которого активно выступили российские банки, являются непрозрачность требований регуляторов и невозможность выполнить их за отведенное время. Выполнение требований закона для банковского сообщества является вовсе не тривиальной задачей. Здесь есть как организационные, так и технические сложности, ниже описаны основные из них:

– необходимость изменения сложившейся практики делового документооборота;

– необходимость выполнения новых функций, не приносящих дохода и требующих дополнительного привлечения значительных трудовых ресурсов;

– необходимость массового перезаключения договоров с клиентами;

– риски блокирования работы кредитной организации путем перегрузки ее запросами граждан – субъектов персональных данных;

– появление новых труднореализуемых и крайне трудоемких процессов, например уничтожение ПД в предусмотренных случаях и т.д.

Выполнение, в банковской сфере требований ФЗ-152 наталкивается на ряд серьезных ограничений и трудностей, что ставит под сомнение возможность практической реализации этих требований к установленному сроку. Это обусловлено несогласованностью норм ФЗ-152 с нормами действующего отраслевого законодательства, отсутствием должной нормативной базы подзаконного уровня, игнорированием ресурсных возможностей банков выполнить работы по защите персональных данных в условиях кризиса, а также неадекватной жесткостью некоторых норм ФЗ-152 и подзаконных актов регуляторов.

Кроме того, существует очевидный дисбаланс ФЗ-152 в сторону абсолютизации интересов субъекта персональных данных без учета реальных возможностей операторов, что не соответствует ратифицированной Россией конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных».

Требования по защите персональных данных, содержащиеся в подзаконных актах регуляторов, не учитывают условий (масштабов и характера работы), в которых находятся отдельные группы операторов персональных данных, в частности кредитные организации. Хотя, если сравнивать ситуацию в кредитно-финансовой сфере с положением дел в других отраслях, то можно сказать, что банки подготовлены значительно лучше, чем многие другие операторы персональных данных. Это связано, прежде всего, с тем, что финансовые организации, обслуживающие частных лиц, всегда серьезно относились к защите персональных данных своих клиентов, рассматривая такие данные, как банковская и/ или коммерческая тайна. То же относится и к защите персональных данных сотрудников.

Напомним, что особенностями российских банков являются огромное число субъектов ПД (десятки миллионов), большой объем и разнообразие ПД по одному субъекту, а также высокий уровень автоматической обработки.

Из вышеперечисленного, учитывая особенности банков как операторов персональных данных, вытекают следствия:

– необходимость отвлечения ресурсов в реализацию мер по выполнению требований Закона от более приоритетных проектов;

– сложности с развитием прогрессивных технологий;

– риск появления новых возможностей мошенничества субъектов;

– риски вмешательства субъектов ПД в текущую деятельность операторов;

– снижение операционной эффективности и технологичности бизнеса.

Подведем черту и отметим явные недостатки ФЗ-152:

– закон не учитывает особенности обработки ПД в различных областях бизнеса;

– закон не отвечает требованиям принципа соразмерности мер, размеру возможного ущерба;

– закон содержит ряд практически неисполнимых и избыточных требований.

Также следует отметить, что за неисполнение требований ФЗ «О персональных данных» каждая российская организация и каждый руководитель рискуют подвергнуться административному и уголовному преследованию вплоть до отзыва лицензии на основной вид деятельности.

ЛИТЕРАТУРА

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ О персональных данных // Российская газета. www.rg.ru/2006/07/29/personaljnye-dannye-doc.html

2. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных // www.fstec.ru

3. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных» // Российская газета, http://www.rg.ru/2008/04/12

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

А.Н. Уразаева, студентка 5-го курса; Н.А. Новгородова, ст. преп.

г. Томск, ТУСУР, каф. КИБЭВС, u.alina88@mail.ru, nna@keva.tusur.ru

В настоящее время возникла необходимость принимать развернутое, детализированное и достаточно жесткое законодательство по защите персональных данных (ПД). На фоне растущего числа угроз безопасности ПД каждая организация стремится защитить их от действий злоумышленников.

В соответствии с Федеральным законом Российской Федерации № 152-ФЗ «О персональных данных» от 27 июля 2006 г. персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Под обработкой ПД понимаются действия (операции) с ПД, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение [1].

Федеральный закон «О персональных данных» регулирует отношения, связанные с обработкой ПД государственными и муниципальными органами власти, юридическими и физическими лицами, с использованием средств автоматизации (а в некоторых случаях и без). Цель такого регулирования – обеспечение защиты прав и свобод человека при обработке его ПД, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В соответствии с ФЗ «О персональных данных» с защитой ПД связаны три органа государственной власти: ФСБ, ФСТЭК и Роскомнадзор Министерства связи и массовых коммуникаций. Область ответственности у каждого из них своя. ФСБ курирует вопросы защиты информации с использованием средств шифрования (криптографии). ФСТЭК России осуществляет контроль защиты информации с применением технических средств. Роскомнадзор является основным исполнительным и надзорным органом по защите прав физических лиц, чьи ПД обрабатываются. За неправомерное обращение с ПД установлена гражданско-правовая, уголовная, административная и дисциплинарная ответственность [1].

В большинстве случаев обработка ПД происходит с использованием средств автоматизации. Требования к обеспечению безопасности ПД при их обработке в информационных системах персональных данных (ИСПД) устанавливает Постановление Правительства Российской Федерации № 781 от 17 ноября 2007 г. об утверждении положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Положение описывает проведение классификации ИСПД, представляющих собой совокупность ПД, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПД с использованием средств автоматизации [2].

Выбор оптимальной стратегии защиты ПД – важная и сложная задача. Эта задача возлагается на оператора. В соответствии с ФЗ «О пер-

сональных данных» оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПД, а также определяющие цели и содержание обработки ПД [1].

Для решения задачи защиты ПД необходимо построить эффективную, соответствующую регуляторным требованиям ИСПД, которая должна сочетать в себе реализацию организационных и технических мер защиты.

Организационные меры предусматривают обязательное прохождение средствами защиты ПД процедур оценки соответствия (для некриптографических средств) и тематических исследований (для криптографических), т.е. сертификации в рамках существующей в стране системы.

Оператору необходимо определить угрозы безопасности ПД при их обработке и на основе этого сформировать модель угроз безопасности ПД в соответствии с типовой моделью, которую определяют регуляторы. После этого необходимо создать и описать систему защиты, обеспечивающую нейтрализацию угроз. Затем нужно произвести проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации, провести установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией.

Обязательнымм должны быть учет лиц, допущенных к работе с ПД в ИСПД, и их обучение с правилами работы. Организация доступа персонала к данным должна производиться на основании утвержденного руководителем организации списка.

Далее предусматриваются организация контроля над соблюдением условий использования средств защиты ПД, проведение разбирательств и составление заключений по фактам несоблюдения условий хранения носителей ПД и/или использования средств защиты ПД, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

Технические меры защиты должны быть направлены на предотвращение несанкционированного доступа к ПД в информационных системах и обнаружение попыток такого доступа, а также недопущение воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование.

Все указанные меры по обеспечению защиты обрабатываемых ПД должны выполняться в соответствии с классификацией таких систем. Классифицировать ИСПД должны операторы таких систем в зависимости от объема обрабатываемых ими ПД и угроз безопасности жизненно важным интересам личности, общества и государства. Для этого пред-

назначен совместный Приказ ФСТЭК, ФСБ и Мининформсвязи №55/86/20 от 13.02.2008 «Об утверждении порядка проведения классификации информационных систем персональных данных» [3].

В данной статье был приведен обзор необходимых мер защиты ПД, которые помогут оператору ПД быть юридически подготовленным и грамотно выполнять свои обязанности.

Научный руководитель – Н.А. Новгородова, старший преподаватель каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Федеральный закон «О персональных данных» №152-ФЗ от 27 июля 2006 г.

2. Постановление правительства Российской Федерации №781 от 17.11.2007 года «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

ПРАВОВАЯ СПРАВОЧНО-ИНФОРМАЦИОННАЯ СИСТЕМА ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

А.Н. Уразаева, студентка 5-го курса; Н.А. Новгородова, ст. преп.

г. Томск, ТУСУР, каф. КИБЭВС, u.alina88@mail.ru, nna@keva.tusur.ru

Законодательство сегодня – это огромная, постоянно меняющаяся информационная база. В нашей жизни постоянно требуется правовая информация: законы, кодексы, нормативная документация и многое другое. Необходимо постоянно быть в курсе происходящего, и без правовой базы данных, которая бы структурировала этот огромный объем информации, не обойтись [1].

Источником получения такой информации является правовая справочно-информационная система. В настоящее время существует немало таких систем, лидерами которых являются Гарант и Консультант Плюс. Однако все эти системы содержат в себе только общедоступную информацию и рассчитаны на широкий круг пользователей. В настоящее время особую актуальность приобретают проблемы в сфере предпринимательской деятельности, и необходимо создать систему защиты в рамках конкретной организации, учитывая все ее особенности. Поэтому для юридических лиц и индивидуальных предпринимателей была разработана правовая справочно-информационная система

(СИС) по защите конфиденциальной информации, а именно персональных данных и коммерческой тайны.

Главной целью разработки такой системы было создание информационно-правовой базы для организации, которая правильно проинформирует и поможет грамотно защитить конфиденциальную информацию, а также позволит быстро найти необходимые документы и обеспечит удобную работу с ними.

Данная СИС представляет собой программный комплекс в виде веб-приложения, состоящий из базы данных, которая позволяет хранить большое количество информации, и программных инструментов, позволяющих работать с этим массивом информации.

В СИС содержатся данные по правовым, организационным и техническим мерам защиты, которые информируют пользователей о том, почему и как правильно защищать, обрабатывать и хранить конфиденциальную информацию.

Важной особенностью СИС является возможность определения класса информационной системы персональных данных с учетом введенных данных пользователем (структура информационной системы, наличие подключений к сетям связи, режим обработки персональных данных в информационной системе, разграничение прав доступа пользователей информационной системы и др.). В соответствии с тем, какой класс присвоится информационной системе персональных данных, выводится список необходимой документации для обеспечения защиты этого класса.

В СИС предусмотрено ведение журнала учета разработанной в организации документации по защите персональных данных и режима коммерческой тайны.

СИС хранит в себе информацию разных уровней конфиденциальности, поэтому доступ к конфиденциальной информации открыт только тем пользователям, которые наделены соответствующими правами. Также фиксируются дата и время каждого посещения пользователей. Для обеспечения безопасности от несанкционированного доступа реализована система регистрации и аутентификации пользователей, сделана проверка на выполнение требований парольной защиты.

СИС имеет дружественный интерфейс и проста в использовании. В системе реализовано два вида поиска: по ключевым словам и по точным реквизитам документа. Названия разделов позволяют быстро сориентироваться и понять, какие документы в каком разделе находятся. Документы связаны между собой через гипертекстовые ссылки, позволяющие нажатием клавиши моментально перейти из одного текста в другой.

Данный программный комплекс является эффективным инструментом, который обеспечивает быстрый и удобный доступ к документации, необходимой для работы и защиты конфиденциальной информации. Грамотно подобранные методы защиты помогут руководителям сделать свою компанию надежной и юридически подготовленной.

Научный руководитель – Новгородова Н.А., старший преподаватель каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Справочно-правовые системы [Электронный ресурс] – Режим доступа: http://www.pravinfo.ru/consultantplus.shtml

ОСНОВНЫЕ ДОКУМЕНТЫ ПО РЕЖИМУ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ*

М.П. Чеплакова, студентка 4-го курса; С.С. Ерохин, инженер ЦТБ
г. Томск, ТУСУР, каф. КИБЭВС, milstar@inbox.ru

Информация – это ресурс, который, как и прочие бизнес-ресурсы, имеет ценность для организации и, следовательно, нуждается в должной защите.

Согласно Международному стандарту ISO/IEC 27002 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью» информационная безопасность – это обеспечение конфиденциальности, целостности и доступности информации. Она достигается внедрением подходящего набора механизмов контроля, включая политики, процессы, процедуры, организационные структуры, а также функции программного и аппаратного обеспечения. Эти механизмы должны быть установлены, внедрены, отслеживаться, пересматриваться и, в случае необходимости, совершенствоваться, в целях обеспечить достижение конкретных целей организации в области безопасности и в бизнесе.

Была поставлена задача подготовить пакет организационных документов для ЦТБ ТУСУРа, предусматривающих механизмы контроля по обеспечению информационной безопасности.

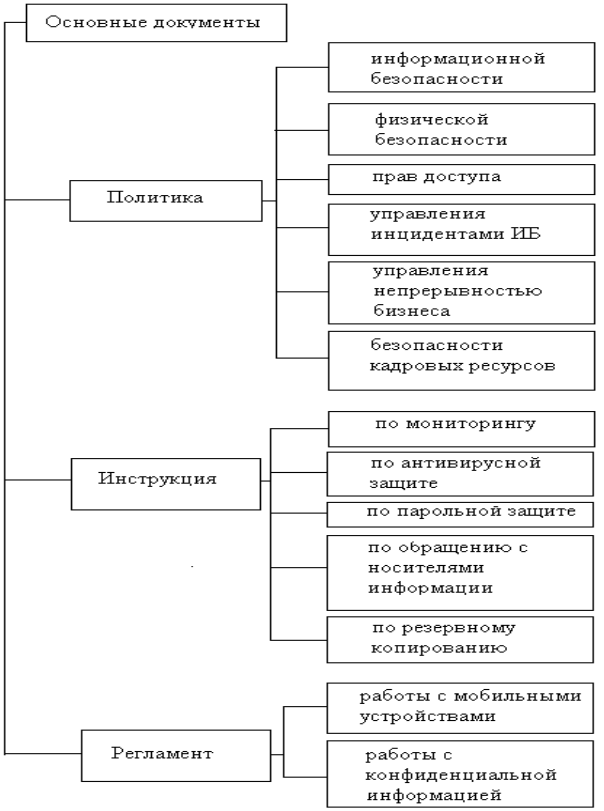
В данной работе был составлен список основных документов по режиму конфиденциальности информации в организации (рис.) и разработаны такие документы, как:

– инструкция по мониторингу;

* Выполнено в рамках проекта ГПО КИБЭВС-0842 – Инженерия баз данных.

– политика управления инцидентами информационной безопасности;
– инструкция по парольной системе защиты;
– инструкция по антивирусной защите;
– инструкция по обращению с носителями информации.

Механизм контроля документа «Инструкция по мониторингу» предназначен для обнаружения несанкционированных действий по обработке информации.



Основные документы по режиму конфиденциальности информации в ЦТБ ТУСУР

Документ «Инструкция по парольной системе защиты» предназначен для предотвращения несанкционированного доступа пользователей к операционным системам, а также компрометации или кражи информации.

Документ «Политика управления инцидентами информационной безопасности» предназначен для обмена информацией о событиях и

слабостях информационной безопасности, связанных с информационными системами, позволяющего своевременно предпринимать корректирующие меры, а также для обеспечения эффективного подхода к управлению инцидентами информационной безопасности.

Документ «Инструкция по антивирусной защите» предназначен для обеспечения защиты целостности информации и программного обеспечения.

Документ «Инструкция по обращению с носителями информации» предназначен для предотвращения несанкционированного раскрытия, модификации, удаления или разрушения ресурсов ЦТБ ТУСУРа, а также прерывания бизнес-деятельности.

Научный руководитель – Н.А. Новгородова, старший преподаватель каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Международный стандарт ISO/IEC 27002 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью» (Information technology – Security techniques – Code of practice for information security management), 2005. 160 с.

ОБУЧАЮЩАЯ СИСТЕМА ПО КУРСУ «ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»*

М.П. Чеплакова, студентка 4-го курса;
Н.А. Новгородова, ст. преп.
г. Томск, ТУСУР, каф. КИБЭВС, milstar@inbox.ru

Обучающие системы являются на сегодня одним из наиболее эффективных средств обучения.

С этой целью и было принято решение в рамках проекта ГПО «Инженерия баз данных», проводимого на кафедре КИБЭВС, создать обучающую систему по курсу «Правовое обеспечение информационной безопасности».

Учебно-методический комплекс (далее УМК), разработанный преподавателем по данному курсу, представляет собой документы разных форматов, таких как:

– выписку из ГОС по дисциплине;
– рабочую программу по курсу;
– методические указания к практическим занятиям;
– теоретический материал согласно разделам ГОСа.

* Выполнено в рамках проекта ГПО КИБЭВС-0842 – Инженерия баз данных.

Следовательно, задача состоит в том, чтобы структурировать полученный материал и представить УМК в системе через удобные интерфейс в едином формате и поиском необходимой пользователю системы информации. Теоретический материал необходимо также дополнять информацией.

Обучающая система, структура которой представлена на рисунке, состоит из трех частей:

– сведений УМК;
– обучающей;
– тестирующей.

Структура системы

Обучающая часть содержит теоретический материал, разбитый по тематическим разделам ГОС, и позволяет также пользователю системы просматривать примеры документов.

Тестирующая часть дает возможность пользователю самостоятельно проверить полученные знания.

Для реализации оболочки обучающей системы был выбран язык разметки HTML.

Данная система имеет следующие возможности:

– обучение конкретным знаниям;
– контроль ответов учащихся;
– возможность подсказки;
– удобство представления изучаемого материала.

Научный руководитель – Новогородова Н.А., старший преподаватель каф. КИБЭВС ТУСУРа.

ЛИТЕРАТУРА

1. Петюшкин А.В. HTML: Экспресс курс. СПб.: БХВ-Петербург, 2003. 256 с.

МЕТОДИКА ФОРМИРОВАНИЯ ШУМОВОЙ ЭЛЕКТРОМАГНИТНОЙ ПОМЕХИ СРЕДСТВОМ АКТИВНОЙ ЗАЩИТЫ

П.В. Урбанович, аспирант
г. Томск, ТУСУР, upaul@rambler.ru

При обработке конфиденциальных данных на компьютере или с помощью любого другого электронного средства возникают технические каналы утечки информации [1]. Одним из наиболее опасных каналов являются побочные электромагнитные излучения (ПЭМИ). Физика этого явления заключается в том, что при протекании переменного электрического тока по проводнику вокруг него создается электромагнитное поле. Вследствие этого каждый проводник информационного сигнала выступает в качестве антенной системы, и чем длиннее проводник, тем эффективнее данная система будет работать. Токи, протекающие по шлейфам и интерфейсным проводам компьютерных и других электронных и коммутационных систем, малы, но достаточны для того, чтобы перехватывать их информационные излучения на расстоянии до нескольких десятков метров.

Самым распространенным методом защиты является активный с использованием генераторов пространственного зашумления. Он не накладывает ограничения на конфигурацию используемого для обработки информации оборудования и имеет известную стоимость комплекса работ по поставке, установке генератора шума и оценке защищенности, что является основным фактором при планировании средств на защиту информации. Недостатком данного метода является создание повышенного электромагнитного поля, вызывающего помехи и сбои в работе электронных устройств, радиоприемной и радиопередающей аппаратуры, расположенной в непосредственной близости.

Основным приемом, направленным на уменьшение помех, является снижение интегрального уровня шума в достаточно широких полосах частот. Однако данные полосы частот могут включать в себя большое количество как полезных сигналов телевизионных или радиостанций, так и опасных сигналов ПЭМИ. В этом случае снижение интегрального шума, кроме уменьшения уровня помех, приведет к уменьшению показателей защищенности до значений, не соответствующих нормам. Это не позволяет в полной мере исключить создание помех генераторами шума на другие радиоэлектронные устройства.

Новый принцип по созданию активного средства защиты от утечки по каналам побочных электромагнитных излучений основан на методике формирования шумовой помехи, при которой учитываются особенности электромагнитной обстановки в конкретном месте эксплуата-

ции. В выходные цепи генератора шума включаются перестраиваемые полосно-заграждающие фильтры, которые вносят затухание на частотах полезных сигналов. Величина вносимого затухания и ширина полосы заграждения исследованы для всех групп радиосигналов, на которые могут создаваться помехи.

При установке средства активной защиты, реализованного с использованием нового принципа, в конкретном месте эксплуатации производится точная подстройка данных фильтров с учетом электромагнитной обстановки и частот вещания телевизионных и радиосигналов.

Данная методика формирования шумовой электромагнитной помехи средством активной защиты позволяет снизить уровень излучения генератора шума именно на тех частотах, на которых ранее создавались помехи, не снижая общего показателя защищенности. Это позволяет одновременно решить вопрос технической защиты информации и обеспечения бесперебойной работы радиооборудования, находящегося в непосредственной близости.

ЛИТЕРАТУРА

1. Хорев А.А. Способы и средства защиты информации. М.: 1998. 316 с.

РАЗРАБОТКА СРЕДСТВА АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

П.В. Урбанович, аспирант

г. Томск, ТУСУР, upaul@rambler.ru

Для защиты информации от утечки по техническим каналам чаще всего применяются средства активной защиты, к которым относятся генераторы пространственного зашумления. Основным недостатком данного метода является создание повышенного электромагнитного поля и, как следствие, электромагнитных помех на радиоприемное и радиопередающее оборудование, расположенное на расстоянии нескольких метров.

Использование перестраиваемых узких, полосно-заграждающих фильтров в выходных цепях генератора шума, позволяет вносить затухание в определенных полосах и уменьшать маскирующий шум на частотах полезных сигналов.

Для выявления полос частот полезных сигналов, на которые генераторами шума создаются помехи, проводится анализ нормативной документации по радиосвязи в Российской Федерации в части распределения полос частот между радиослужбами, по результатам которого

была составлена таблица сигналов, чувствительных к повышенному уровню электромагнитного поля, создаваемого генератором шума. Установлена численная зависимость между величиной превышения уровня сигнала над уровнем шума и степенью вызываемых помех. Исследованы полосы частот радиосигналов, на которых создаются существенные помехи при включенном режиме генерации шума. Выбраны аппроксимации активных фильтров, отвечающих условиям простоты реализации, простоты подстройки по частоте и добротности, возможности достижения больших значений добротности и невысокой чувствительности к отклонению значений элементов схемы от номиналов. Классические фильтры не удовлетворяют указанным условиям, однако исследования в области фильтрации позволили получить схемы, обладающие возможностью достижения средних и больших значений добротности и относительной простой реализацией. Одной из них является схема на основе конверторов полного сопротивления или гираторная схема [1]. Данное схемное решение удовлетворяет критериям проектирования и обладает следующими положительными качествами: возможность достижения средних значений добротности в пределах от 4 до 20–25 без чрезмерного расширения диапазона номиналов элементов; невысокая чувствительность к отклонениям значений элементов схемы от номиналов; относительная простота настройки схемы и всего два операционных усилителя.

Произведено математическое моделирование данной схемы, в результате которого установлено ее полное соответствие заданным условиям.

Произведен расчет необходимых полосно-заграждающих фильтров с использованием программного обеспечения.

Реализация данных фильтров в виде опытных образцов показала хорошие результаты. Эксперименты, проводимые в лаборатории ООО по защите информации «Секрет-Сервис» (г. Иркутск) показали, что включение опытных образцов в выходные цепи генератора шума позволяет исключить создание помех на полезные сигналы телевизионных и радиостанций, не снижая общих параметров защищенности. Перестройка фильтров по частоте дает возможность использовать их в любом месте эксплуатации.

ЛИТЕРАТУРА

1. Мориц Г., Хорн П. Проектирование активных фильтров: Пер. с англ. / Под ред. И.Н. Теплюка. М.: Мир, 1984. 318 с.

СОДЕРЖАНИЕ

СЕКЦИЯ 14

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Научное издание

Научная сессия ТУСУР-2010

Материалы
Всероссийской научно-технической конференции
студентов, аспирантов и молодых ученых
4–7 мая 2010 г., Томск, Россия
В пяти частях

Часть 3

Корректор – **В.Г. Лихачева**
Верстка **В.М. Бочкаревой**

Издательство «В-Спектр».
Сдано на верстку 01.04.2009. Подписано к печати 27.04.2010.
Формат 60×84 1/16. Печать трафаретная.
Печ. л. 17,75. Усл. печ. 16,7.
Тираж 200 экз. Заказ 22.

Тираж отпечатан в издательстве «В-Спектр».
ИНН/КПП 7017129340/701701001, ОГРН 1057002637768
634055, г. Томск, пр. Академический, 13-24, т. 49-09-91.
E-mail: bmwm@list.ru